FATF • GAFI

FINANCIAL ACTION TASK FORCE

Mutual Evaluation Report

Anti-Money Laundering and Combating the Financing of Terrorism

THE NETHERLANDS

25 February 2011

The Netherlands is a member of the Financial Action Task Force (FATF). This evaluation was conducted by the International Monetary Fund and was adopted by the FATF at its Plenary in Paris on 25 February 2011.

TABLE OF CONTENTS

Tables

ACRONYMS

AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
BL	Banking Law
BCP	Basel Core Principles
CC	Criminal Code
CDD	Customer Due Diligence
CPC	Criminal Procedure Code
CSP	Company Service Provider
DNFBP	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FI	Financial institution
FIU	Financial Intelligence Unit
FSAP	Financial Sector Assessment Program
FSRB	FATF-style Regional Body
FT	Financing of terrorism
IAIS	International Association of Insurance Supervisors
KYC	Know your customer/client
LEG	Legal Department of the IMF
MEF	Ministry of Economy and Finance
MFA	Ministry of Foreign Affairs
MOU	Memorandum of Understanding
ML	Money laundering
MLA	Mutual legal assistance
NPO	Nonprofit organization
PEP	Politically-exposed person
ROSC	Report on Observance of Standards and Codes
SRO	Self-regulatory organization
STR	Suspicious Transaction Report
UN	United Nations Organization
UNSCR	United Nations Security Council Resolution

EXECUTIVE SUMMARY

Background information

1. This report summarizes the anti-money laundering and counter-terrorist financing measures (AML/CFT) that were in place in the Netherlands at the time of the on-site visit (June 28–July 13 2010) and immediately thereafter. It describes and analyses these measures and offers recommendations on how to strengthen certain aspects of the system. It also assesses the Netherlands's level of compliance with the *40+9 Recommendations* of the Financial Action Task Force (FATF) (see the attached table on the *Ratings of Compliance with the FATF Recommendations*).

Key Findings

2. Indicators suggest that the Netherlands is susceptible to ML, including because of its large financial center, openness to trade and the size of criminal proceeds. The 16th economy in the world by nominal GDP, it ranks 7th in terms of the systemic importance of its financial sector. It has an excellent communications network, convenient transportation infrastructure, and Rotterdam is one of the world's busiest ports. Estimates indicate that substantial proceeds of crime are generated in the country, mostly stemming from fraud (including tax fraud) and illicit narcotics. Presently the proceeds of domestic crime are estimated at approximately USD14 billion, or 1.8 percent of the GDP. In addition, work done by academics suggests a significant amount of criminal proceeds originating from foreign countries flows into The Netherlands for laundering. The authorities have developed novel and advanced research investigating the links between business and crime.

3. There is a terrorism and TF risk but it appears limited based on available information. The country has experience dealing with a variety of terrorist organizations, at present the main threat seems to come from international Islamists extremists, but the risk is currently deemed to be limited.

4. The Netherlands have criminalized ML fully in line with the requirements under the Vienna and Palermo Conventions. The Criminal Code does not provide for an autonomous offense of "terrorism financing" but criminalizes such conduct based on the offense of "preparation to commit a serious crime" and "participation in a terrorist organization".

5. The Netherlands have a long-standing FIU which is one the founding members of the Egmont Group and enjoys high trust for its professionalism, both domestically and internationally. The delays in the completion of its reorganization as FIU-Netherlands have eroded its operational independence and affected its effectiveness.

6. Financial investigations have been pursued through aggressive and effective approaches, as shown by the relatively high number of prosecutions for ML or ML and other offences. However, it has not been demonstrated that the analytical work of the FIU has significantly contributed to investigations and prosecutions of ML cases.

7. The Netherlands have a long-standing system of preventive measures and while the legal framework is modern and comprehensive for both financial and non-financial institutions, it falls short of the international standard in some areas, such as in the case of the verification of beneficial owners and simplified due diligence.

8. Supervision of AML/CFT obligations is based on broadly comprehensive powers and is well regarded by most sections of the regulated financial sector but some gaps in the legal framework need to be filled.

9. The AML/CFT Law has to be amended to improve the reporting regime, including by requiring that suspicious transactions are reported promptly. Measures should be taken to ensure quality reporting by all financial and non-financial institutions. In light of the risks identified in relation to corporate lawyers' activities, authorities are recommended to address legal issues preventing effective implementation of preventive measures and supervision.

10. The Criminal Procedure Code (CPC) should be revised to enable the Netherlands to grant any foreign country assistance in searching and seizing evidence in ML cases, and to make ML an extraditable offense, regardless of the predicate offense involved. Statistics should be maintained in a number of important areas to demonstrate that the AML/CFT legal framework is implemented effectively.

Legal Systems and Related Institutional Measures

11. The Netherlands have criminalized ML fully in line with the requirements under the Vienna and Palermo Conventions. The Dutch ML provisions cover all FATF designated predicate offenses, extend to any type of property as defined in the FATF standard and also apply to persons who commit the predicate offense. Appropriate ancillary offenses are provided for. Although a significant number of investigations, prosecutions and convictions has been carried out, due to the lack of information on the types of predicate offenses involved it could not be determined that the ML provisions are applied in a fully effective manner.

12. The Dutch legal system does not provide for an autonomous offense of "terrorism financing" but criminalizes such conduct based on the offenses of "preparation to commit a serious crime" and "participation in a terrorist organization". A number of serious shortcomings have been identified in this regard.[1] Most notably, the current legal framework criminalizes the "collection" of funds to commit a terrorist act only if the perpetrator has acquired or actual possession of the funds; the criminal provisions do not sufficiently apply to the financing of conduct covered by the offenses set forth in the nine Conventions and Protocols listed in the Annex to the FT Convention; and the financing of an individual terrorist is criminalized only in relation to persons designated under UNSCR 1267 or 1373, or the EC or Dutch Sanctions Regulations. In discussions with a number of different law enforcement authorities it was indicated that the absence of an autonomous FT offense has a negative impact on the effective investigation of terrorism financing activities.

13. The Netherlands have in place a strong and comprehensive legal framework for the seizing and confiscation of proceeds of crime, the application of which has yielded some positive results. However, in the absence of complete and more detailed statistics it was not possible for the assessors to determine that the seizing and confiscation measures are applied in a fully effective manner with respect to ML, FT and predicate offenses.

14. The Netherlands have a strong and comprehensive framework in place to implement its obligations under UN Security Council Resolutions 1267 and 1373 and in a number of cases have effectively applied this framework to freeze the funds and assets of designated terrorists and terrorist organizations. The most important financial sectors are effectively supervised for compliance with their obligations under the EC and Sanctions Regulations. Only a few technical deficiencies were identified. Concerns remain as to whether in practice the authorities make use of the possibility to

1 A clear ministerial commitment to pursue the criminalization of terrorist financing (TF) in line with FATF Special Recommendation II (SR II) has been communicated by the Dutch authorities.

circumvent the time delay on European level and freeze without delay the funds and assets of individuals, entities and organizations designated under UN Resolutions 1267 and 1373.

15. The Netherlands have a long standing financial intelligence unit (FIU) responsible for receiving, analyzing and disseminating information concerning ML or FT, which enjoys the trust of the financial community and law enforcement authorities (LEAs) alike. The FIU, first established in 1994, underwent a restructuring process in 2006, but the legal framework governing the FIU is not yet fully complete. Moreover, the completion of the reorganization of the FIU has been delayed, which has hampered its effectiveness and eroded the operational independence. A new governance model was agreed in September 2010, but it is rather complex and should be streamlined by reducing the number of institutions to which the FIU is accountable and simplifying the reporting lines.

16. The FIU has the potential for producing high-quality financial analysis but it should reconsider the manner in which financial information is disseminated to LEAs, and place more emphasis on a case-by-case dissemination. The number of ML criminal investigations that is triggered by disseminated financial information could not be confirmed, but appears to be rather low. Analysis of financial information would also benefit from greater prioritization and pursuit of a red flag-based approach. The authorities should also ensure that the FIU has timely and full access to all the information that is necessary to properly undertake its functions.

17. Financial investigations have been pursued through aggressive and effective approaches, as demonstrated by the relatively high number of prosecutions for ML or ML and other offences. The Dutch authorities encourage LEAs to prosecute ML and deprive offenders of the proceeds of crime for each case, even when the proceeds are low. LEAs have most powers necessary to carry out their investigations and are generally effective. The only caveat is the scope of legal privilege, which hinders the ability for law enforcement authorities to locate and trace assets and property, and may also negatively impact mutual legal assistance, freezing, seizure and confiscation.

Preventive Measures—Financial Institutions

18. The Netherlands have a long-standing legal framework concerning AML/CFT preventive measures, which dates back to 1993. The latest Money Laundering and Terrorist Financing Prevention Act (WWFT), adopted in 2008, establishes CDD, record keeping and reporting requirements for a broad range of financial institutions and DNFBPs. The scope of the WWFT covers all financial activities covered by the FATF definition of “financial institutions”.

19. The legal framework for CDD is generally adequate; however a number of provisions are problematic. These include: issues with the definition of the beneficial owner which, inter alia, does not include the person that can exercise ultimate effective control over a legal arrangement; the very broad exemptions allowed for specified low-risk customers; the treatment of all the EU/European Economic Area (EEA) members states and jurisdictions as well as certain other countries as a single risk category when determining certain low risk scenarios; the transitional regime envisaged by the WWFT in the case of existing customers, which relies on a de jure presumption of compliance with the CDD requirements and the limited scope and enforceability of countermeasures in the case of countries that do not or insufficiently apply the FATF Recommendations. Of particular concern is the requirement to verify the identity of the beneficial owner, which, along with the obligation to understand the ownership and control structure of the customer, is only applicable in high risk scenarios. Furthermore, there is no obligation for financial institutions to determine whether a beneficial owner of a customer is a politically exposed person.

20. The Dutch system of preventive measures emphasizes the risk-based approach, complemented by a principles-based approach. The latter relies on the financial institutions’ capacity

and expertise to implement a particular obligation envisaged by the law, without prescribing in detail how the relevant obligation should be met, and it is aimed at providing financial institutions with the possibility to develop an individualized approach to CDD.

21. The principles-based approach should be better supported with guidance for financial institutions. Implementation of the principles-based approach was in some cases uneven, particularly in challenging areas such as identifying and verifying the identity of the beneficial owner of legal persons and PEP accounts. Despite limited guidance, the level of implementation of CDD measures is good overall, with larger, multinational banks best placed to meet the higher standard set out in the WWFT, and smaller, newly formed banks finding it challenging to do so.

22. Although most elements of the STR reporting requirements are in place, the reporting regime has one minor legal shortcoming and raises effectiveness concerns. The 14-day period to report after a transaction has been established suspicious is not consistent with the standard's call for prompt reporting and raises an effectiveness issue in relation to the recovery of criminal assets. Reporting by insurance agents, life insurance companies and bureau de change is particularly low, which raises concerns regarding the effectiveness of the reporting regime. Both the protection for reporting and the prohibition from tipping off also present shortcomings.

23. The requirements for internal controls in the financial sector are found in the Act on Financial Supervision (Wft) and cover most of what is required by the standard but leave some gaps. Although the assessors accept that the Wft can be interpreted as imposing an obligation on financial enterprises to have internal controls that implement the WWFT obligations, the legal position would be more robust if this obligation were made explicit, as it is in the Wgt Regulation. Even so, the internal control requirement does not apply to all categories of financial enterprise. The WWFT and Wgt requirements relating to employee training are limited and should be broadened. The obligations relating to the role and seniority of compliance officers also need strengthening. Record-keeping requirements in the tax law (AWR) and Civil Code (BW) are comprehensive.

24. The WWFT obliges institutions to apply Dutch standards on customer due diligence to branches and subsidiaries in foreign countries but the requirement does not extend beyond CDD to other AML/CFT measures and does not apply to branches and subsidiaries in EU Member States.

25. The supervisors generally have the powers and resources they require to ensure effective implementation of AML/CFT obligations but the supervisory approach may not be equally effective in all sectors. The Netherlands operates a "twin peaks" supervisory system, with the Dutch Central Bank (DNB) responsible for prudential supervision and the Authority for the Financial Markets (AFM) responsible for conduct of business. Both have responsibility for enforcing AML/CFT measures. Some institutions such as money transfer offices and small banks have found the DNB to be most helpful and effective. In other areas, such as insurance and the securities sector, there are some doubts about effectiveness, arising from the experience of specific institutions and the statements by the supervisors. Guidance to financial enterprises needs to be brought up to date and broadened to include monitoring obligations as well as CDD. There is scope for strengthening the training given as a matter of routine to supervisory staff. These weaknesses should be addressed but, nevertheless, the maturity and sophistication of the Netherlands' risk-based supervisory approach is largely effective in implementing the AML/CFT obligations.

Preventive Measures—Designated Non-Financial Businesses and Professions

26. The preventive measures for DNFBPs mirror those for financial institutions, except for trust and company service providers (TCSPs) where they are more comprehensive. The authorities

have clearly put a lot of resources and political commitment in relation to DNFBPs and the regime in place is relatively comprehensive. The legal framework for TCSPs has only minor shortcomings and appears effectively implemented, but their STR reporting level is low in relation to both the importance of financial flows and risks. Regarding other DNFBPs, there are a few shortcomings in the scope of the customer due diligence requirements for real estate agents, lawyers and notaries. The reporting system appears quite effective for notaries and accountants, and recent positive developments have been noted regarding real estate agents. However, reporting by precious metals dealers and lawyers is still very low, while significant risks are acknowledged by the authorities for the latter. In relation to supervision, the main shortcoming is that secrecy issues prevent the exercise of supervision of lawyers by the designated supervisor. Effectiveness issues have been identified in relation to the monitoring of precious metals dealers and accountants, but are likely to be addressed by the recent implementation of a risk-based supervisory framework.

Legal Persons and Arrangements & Non-Profit Organizations

27. The Netherlands have a number of measures in place that contribute to the availability of beneficial ownership information in relation to legal entities and arrangements. Amongst these measures are the obligation to register legal entities with the Chamber of Commerce, to involve licensed and thus supervised notaries and trust service providers in the establishment and/or management of certain legal entities, as well as the obligation under Dutch tax law to file annual returns. However, some gaps remain in relation to information on the ultimate beneficial owners of legal persons and legal arrangements and as such information may thus not be available, accessible and/or up-to-date in all cases.

28. At the time of the assessment, Dutch law still permitted the issuance and free transfer of bearer shares. A dematerialization process has been put in place but will not be completed and thus fully effective until 2013. Based on estimates provided by the authorities, it seems that bearer shares are no longer widely used in the Netherlands.

29. The measures in place in the Netherlands in relation to NPOs ensure a high level of transparency. Information available with respect to NPOs is generally comprehensive, in particular with respect to NPOs within the Central Bureau for Fundraising (CBF) seal mechanism.[2] Information sharing and cooperation mechanisms between competent authorities are in place but do not comprise the CBF, which is a private organization. This poses a limitation in that the CBF maintains detailed information on a significant share of the sector.

National and International Co-operation

30. The Netherlands has no overarching law dealing with Mutual Legal Assistance but cooperates internationally based on the provisions of the Criminal Procedure Code. The authorities may provide a wide range of assistance in relation to ML and FT cases and the granting of such assistance is not subject to any unduly restrictive or unreasonable conditions. In relation to a large number of countries, however, assistance in searching and seizing of evidence can, with few exceptions, be provided only in ML cases involving corruption or transnational organized crime but not any other types of predicate offenses. In cases where dual criminality is required, the shortcomings identified in relation to the provisions criminalizing terrorist financing limit the Netherlands ability to provide MLA. Furthermore, the scope of legal privilege may unduly hinder the possibility for law enforcement authorities to access information and documents held by notaries, lawyers and tax accountants, including upon foreign request. Due to the lack of relevant statistics, the Netherlands did not establish that they effectively seize and confiscate funds based on foreign requests.

2 NPOs, to enhance their credibility and improve their fund raising opportunities, may apply to the CBF for a "seal of approval," which subjects such NPOs to a relatively close supervision by the CBF.

31. ML is an extraditable offense in relation to Council of Europe Member States and countries with which the Netherlands has entered into a bilateral or multilateral extradition treaty. In relation to all other countries, only ML cases involving transnational organized crime or corruption but not any other types of crimes are extraditable offenses. FT is an extraditable offense but based on the dual criminality requirement, the shortcomings identified under Special Recommendation II may limit the Netherlands' ability to extradite in certain FT cases.

PREFACE

INFORMATION AND METHODOLOGY USED FOR THE EVALUATION OF THE NETHERLANDS

32. This assessment of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of The Netherlands is based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT assessment Methodology 2004, as last updated in February 2009. The assessment team considered all the materials supplied by the authorities, the information obtained on site during their mission from June 28 to July 13, 2010, and other verifiable information subsequently provided by the authorities. During the mission, the assessment team met with officials and representatives of all relevant government agencies and the private sector. A list of the bodies met is set out in Annex 1 to the detailed assessment report.

33. The assessment was conducted by a team of assessors composed of staff of the International Monetary Fund (IMF) and three expert(s) acting under the supervision of the IMF. The evaluation team consisted of: Richard Lalonde (LEG, team leader); Giuseppe Lombardo (LEG, deputy team leader), Emmanuel Mathias (LEG, financial sector expert); Gabriele Dunker (legal expert), Richard Pratt (financial sector expert) and Sarah Runge (U.S. Department of the Treasury, financial sector expert). The assessors reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter and punish money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBP). The assessors also examined the capacity, implementation, and effectiveness of all these systems.

34. This report provides a summary of the AML/CFT measures in place in The Netherlands at the time of the mission or shortly thereafter. It describes and analyzes those measures, sets out The Netherlands' levels of compliance with the FATF 40+9 Recommendations (see Table 1) and provides recommendations on how certain aspects of the system could be strengthened (see Table 2). The report was produced by the IMF as part of the Financial Sector Assessment Program (FSAP) of The Netherlands. It was also presented to the FATF and adopted by this organization at its plenary meeting of February 2011.

35. The assessors would like to express their gratitude to the authorities of The Netherlands for their cooperation and hospitality throughout the assessment mission.

1. GENERAL

1.1 General Information on The Netherlands and Its Economy

Overview

36. The Netherlands is a parliamentary democratic constitutional monarchy. It borders the North Sea to the north and west, across which are Norway, Denmark, and the United Kingdom. It shares land borders with Belgium (450 km.) to the south, and Germany (577 km.) to the east. The capital is Amsterdam and the seat of government is in The Hague. The Netherlands is densely populated. The 2009 estimate is that 16 554 448 people live on 41 562 km. It is a geographically low-lying country, with about 27 percent of its area and 60 percent of its population located below sea level. Significant areas have been gained through land reclamation and preserved through an elaborate system of polders and dikes. The Netherlands was a founding member of the UN, NATO, the European Communities (now the European Union), the International Monetary Fund, the World Bank, and the Western European Union.

Dutch economy

37. The Dutch economy is a private free-market system. The main impact of the government on the economy is through regulation and taxation. Currently, almost two-thirds of the economy is based on foreign trade. In terms of exports the country ranks seventh in the world. The country has been one of the main proponents of international free trade and the reduction of duties and tariffs on goods and services. As a member of the European Union (EU), the Netherlands uses the Euro since January 1, 2002, a common currency used by 16 EU countries.[3] The Netherlands is also a party to the Schengen Agreement.[4]

38. The Netherlands is home to some of the world's largest corporations, including Royal Dutch Shell and Unilever. Despite its small size, the Netherlands ranks number seven in the world in total value of its corporations. The 2009 GDP was 572 billion Euros, after reaching 596 billion in 2008.[5] This makes the Dutch economy the 16th largest worldwide.[6] After the recent recession (4.0 percent real GDP decrease in 2009), the economy looks set to grow again on the back of a recovery in world trade, fiscal stimulus and easier monetary conditions. The latest estimate of the CPB (*Centraal Planbureau*), the Netherlands Bureau for Economic Policy Analysis, is that real GDP will increase by 1¼ percent in 2010 en 1¾ percent in 2011.[7] The IMF estimates that GDP will increase modestly by ¾ percent in 2010.[8]

System of government

3 The 16 countries that use the Euro are: Austria, Belgium, Cyprus, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Malta, the Netherlands, Portugal, Slovakia, Slovenia, and Spain.

4 The 25 member countries are: Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, and Switzerland.

5 Source: CBS (Statistics Netherlands, the Dutch national bureau for statistics, http://www.cbs.nl) and CPB (Netherlands Bureau for Economic Policy Analysis, http://www.cpb.nl). Source: IMF World Economic Outlook (WEO) Database, October 2010 (updated October 6, 2010).

6 Source: IMF World Economic Outlook (WEO) Database, October 2010 (updated October 6, 2010).

7 See newsletter of the CPB at: http:/www.cpb.nl/eng/news/2010_31.htlm

8 See February 2010 IMF Article IV Report (IMF Country Report No. 10/34).

39. The Netherlands has been a constitutional monarchy since 1848. The Constitution (*Grondwet*) states that the government, *i.e.* the ministers, is responsible for government policy, rather than the Monarch. The Queen enjoys immunity. The Netherlands is a parliamentary democracy. The State is ruled by the government under the supervision of parliament. The government consists of the Ministers under the leadership of the Prime Minister (minister-president). Parliament consists of an Upper House (*Eerste Kamer*) and a Lower House (*Tweede Kamer*).

40. The 150 members of the Lower House (*Tweede Kamer*) are elected directly by the citizens of the Netherlands. In principle, there are elections every four years. The main task of the Lower House is to supervise the government's actions. The Lower House has several powers to achieve this objective. One of the most important is the right of amendment, *i.e.* the right to change bills proposed by the Cabinet, which is led by the Prime Minister and consists of the Ministers and State Secretaries. The Minister responsible for the proposed bill can adopt such an amendment, submit it to a vote in the Lower House, or can reject it outright. If this is the case the Lower House may table a motion of 'no confidence' against the Minister or the Cabinet. This can ultimately lead to the resignation of the Minister or the entire Cabinet. The Lower House also has the right of initiative, *i.e.* the right to propose bills, the right of interpellation, the right to demand clarification from a Minister, the right of inquiry, and the right of budget.

41. The Netherlands has three administrative layers: the State, the provinces (*provincies*), and the municipalities (*gemeenten*). Elections are held every four years for the Provincial Councils (the second administrative layer) and the municipalities.

42. Delegates from the Provincial Councils elect the membership of the Upper House (*Eerste Kamer*). The Upper House is a co-legislator and monitors government policy. All bills which have been passed in the Lower House must also be approved by the Upper House. The Upper House can only adopt or reject a bill. It cannot propose or amend bills. Furthermore, the members of the Upper House have the same rights as the members of the Lower House.

43. At the time of the mission, the Netherlands had 13 Ministries. With a new government in place since October 14, 2010, there are now 11 Ministries.[9] Each Ministry is headed by a Minister who bears political responsibility for the policy pursued by that Ministry. He or she is supported in this task by one or occasionally two State Secretaries (*staatssecretaris(sen)*). The civil servants in each Ministry assist the Minister and State Secretary or Secretaries in their work. They maintain an apolitical stance (loyalty principle). After elections, the civil servants continue to work at the same Ministry for the newly-appointed Ministers and State Secretaries.

Judicial system

44. The Netherlands is divided into 19 districts, each with its own court (*rechtbank*). Appeals against judgments passed by the district court in civil and criminal law cases can be lodged at the competent Court of Appeal (*Gerechtshof*). There are five Courts of Appeal in total. Appeals against administrative law judgments go to the competent specialized administrative law tribunal–the Administrative Jurisdiction Division of the Council of State (*Raad van State, Afdeling Bestuursrechtspraak*), the Central Appeals Tribunal (*Centrale Raad van Beroep*) or the Trade and Industry Appeals Tribunal (*College van Beroep voor het Bedrijfsleven*), also known as Administrative High Court for Trade and Industry, depending on the type of case. Appeals in civil, criminal and tax law cases are lodged at the Supreme Court of the Netherlands (*Hoge Raad der Nederlanden*, HR).

9 In the new government the Minister of Justice is now called the Minister of Security and Justice. The Minister of Security and Justice has overall responsibility for the Dutch police. Before October 14, 2010 the Minister of Interior and Kingdom Relations was responsible for overseeing the Dutch police.

45. The Council for the Judiciary (*Raad voor de Rechtspraak*) is part of the judiciary system, but does not administer justice itself. It has taken over responsibility over a number of tasks from the Minister of Justice. These tasks are operational in nature and include the allocation of budgets, supervision of financial management, personnel policy, ICT and housing. The Council supports the courts in executing their tasks in these areas. Another central task of the Council is to promote quality within the judiciary system and provide advice on new legislation which has implications for the administration of justice. The Council also acts as a spokesperson for the judiciary on both national and international levels.

Constitutional reform of the Kingdom of the Netherlands

46. The Netherlands is part of the Kingdom of the Netherlands, a political union made up of three constituent countries: the Netherlands in Western Europe, and Aruba and the Netherlands Antilles (consisting of the islands Curaçao, Sint Maarten, Bonaire, Sint Eustatius and Saba) in the Caribbean. All three countries are distinct jurisdictions and participate on a basis of equality as partners in the Kingdom.

47. At the time of the mission, it was foreseen that the Netherlands would be enlarged with three islands that formed part of the Netherlands Antilles: Bonaire, Sint Eustatius and Saba. These were to become 'special municipalities' of the Netherlands. The remaining islands of the Netherlands Antilles, Curaçao and Sint Maarten would then each acquire the status of independent country within the Kingdom of the Netherlands. This constitutional reform took place in October 2010.

Anti-Money Laundering and Combating the Financing of Terrorism framework

48. The Dutch legislation on the prevention of money laundering and the financing of terrorism originates in the 40+9 Recommendations of the Financial Action Task Force (FATF). These Recommendations constitute the basis for the directives of the European Communities (Council Directive 91/308/EEC of June 10, 1991 on prevention of the use of the financial system for the purpose of money laundering (OJEC L 166/77), amended by Directive 2001/97/EC of the European Parliament and of the Council of December 4, 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for money laundering (OJEC L 344) and Directive 2005/60/EC of the European Parliament and of the Council of October 26, 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJEC L 309, hereinafter: the Third Money Laundering Directive).

49. EU Directives 91/308/EEC and 2001/97/EC were implemented in the Identification (Financial Services) Act 1993 (later amended to Identification (Provision of Services) Act) and the Disclosure of Unusual Transactions (Financial Services) Act. These Acts entered into force on February 1, 1994. The purpose of the Identification (Provision of Services) Act 1993 (*Wet identificatie bij dienstverlening 1993*, hereinafter: WID) and the Disclosure of Unusual Transactions (Financial Services) Act (*Wet Melding ongebruikelijke transacties*, hereafter: WMOT) was to combat the laundering of criminal proceeds and the financing of terrorism. To this end, the WID imposed the obligations of customer identification and customer due diligence, while the WMOT made it compulsory to disclose unusual transactions. Together, the two Acts aimed to prevent the financial system from being used for money laundering and terrorist financing. When the new provisions of the Third Money Laundering Directive needed to be implemented in Dutch legislation, it was decided to simultaneously integrate the WID and the WMOT. The two Acts were fused in the Money Laundering and Terrorist Financing Prevention Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*, hereinafter: WWFT. This Act came into force on August 1, 2008.

50. Besides the WWFT there are several other laws that make up the AML/CFT framework in the Netherlands:

- **Act on financial supervision** (*Wet op het financieel toezicht*, **Wft**). The Wft came into force in January 2007. This law consolidated the law on the supervision on banks (*Wet toezicht kredietwezen*, Wtk), the law on the supervision on insurance companies (*Wet toezicht verzekeringsbedrijf*, Wtv), and some other supervisory laws for financial institutions. The Decree on Prudential Rules pursuant to the Act on Financial Supervision (*Besluit prudentiële regels Wet op het financieel toezicht*, BPR Wft) and the Decree on the Supervision of the Conduct of Financial Enterprises pursuant to the Act on Financial Supervision (*Besluit Gedragstoezicht financiële ondernemingen Wet op het financieel toezicht*, BGFO Wft) provide for further rules, including rules regarding measures to safeguard integrity. Such integrity measures have to be taken by financial institutions to mitigate, among other things, the risk of money laundering and the risk of the financing of terrorism.

- **Sanctions Act 1977** (*Sanctiewet 1977*). The Sanctions Act 1977 provides the basis for national freezing measures and other sanctions, and for supervision of compliance with sanction regulations.

- **Money Transfer Offices Act** (*Wet inzake de Geldtransactiekantoren*, **Wgt**). The Wgt entered into force on June 27, 2002. As of November 1, 2009, the EU Payment Services Directive (2007/64/EG, PSD) was implemented in Dutch legislation (in the Wft). Thus every payment service provider which is not a credit institution needs a license to be able to operate as a payment institution. Money transaction offices that provide payment services as defined in the Wft (i.e. money remittance services) will be regulated under the Wft instead of, as hitherto, under the Wgt. The Act provides for summary transitory legislation in respect of existing payment institutions.

- **The Trust Offices Act** (*Wet toezicht trustkantoren*, **Wtt**). The Wtt entered into force on March 1, 2004. Under the Wtt it is prohibited to carry on the business of a trust office from a Netherlands-based establishment without a license. Trust offices are subject to requirements concerning operations and organization, and the trustworthiness and expertise of the persons who operate it.

51. The Netherlands follows a threshold approach in defining predicate offenses for ML. Articles 420 bis and 420 quater of the Penal Code are applicable to objects that were obtained through the commission of “a criminal offense” but not to objects that stem from misdemeanors. Under the Dutch Penal Code (*Wetboek van Strafrecht*, hereinafter: WvSr), the public prosecutor needs to prove that the proceeds originate from criminal activity. The specific predicate offense itself and the exact origin of the laundered proceeds do not have to be proven. The general criminal origin as well as the knowledge of the perpetrator may be deduced from objective circumstances. The maximum sentence for “offenses” ranges between imprisonment for six months to imprisonment for life. “The maximum imprisonment sanction available for misdemeanours generally does not exceed six months.”

52. Dutch law does not provide for a separate terrorist financing offense but terrorist financing activities could be prosecuted based on either Article 46 WvSr (preparation of a criminal offense punishable with imprisonment for four years or more), or Article 140 (4) in conjunction with Article 140a WvSr (participation in a criminal/terrorist organization). At the time of the assessment, there have been no prosecutions or convictions for terrorist financing in the Netherlands.

1.2 General Situation of Money Laundering and Financing of Terrorism

1.2.1 Predicate Offenses

53. According to the WODC's and CBS's statistics, theft is the most prevalent criminal offense, in particular burglary, followed by traffic offenses, and assaults.

54. As shown by the table below, the country has fewer murders, drug offenses, police and prisoners than the average country, but slightly more assaults, many more burglaries, and a lower conviction rate.

Selected Crime Statistics (2003)		
Crime Related Statistic	*Average of countries*	*The Netherlands*
Criminal offenses per 100 000 population	3 400	8 530
Drug offenses per 100 000 population	191.1	96
Murders per 100 000 population	10	1.4
Assaults per 100 000 population	250	330
Burglaries per 100 000 population	510	2 958
Police per 100 000 population	300	227
Prisoners per 100 000 population	148	100
Conviction success rate (offenders/convictions)	60%	36%

Source: Ministry of Justice (WODC), Central Bureau of Statistics (CBS), United Nations

55. Over the years the Dutch authorities have taken the initiative to study predicate offenses and proceeds of crimes, and how they impact society. This includes novel and advanced research investigating the links between business and crime.

Corruption

56. Domestic corruption appears to be low. The Netherlands has consistently scored very well in transparency and anti-corruption rankings, including those published by Transparency International (TI), and the World Bank (see below).

Control of Corruption and Rule of Law Scores						
Measure	**2005**		**2006**		**2007**	
	% Rank	**Score**	**% Rank**	**Score**	**% Rank**	**Score**
Control of Corruption	96	1.99	96	2.06	97	2.25
Rule of Law	94	1.72	93	1.74	93	1.76
Scores range from -2.5 to 2.5, where -2.5 is worst and is 2.5 best						

Source: "Governance Matters VII: Aggregate and Individual Governance Indicators, 1996-2007," Kaufmann, Kraay & Mastruzzi (World Bank Policy Research Working Paper No. 4654, June 24, 2008).

57. In addition, in its most recent GRECO report,[10] the conclusion is that "overall, the Dutch legal framework for the criminalization of corruption complies with the standards of the Criminal Law Convention on Corruption (ETS 173) and its Additional Protocol (ETS 191)." And that "[…] the legal provisions seem to be broadly interpreted by prosecutors and judges alike and the case-law built up underscores the broad scope of the provisions under evaluation."

Drugs

58. The exact amount of drugs moving to and through the Netherlands is hard to estimate, but there are some indications. A November 2010 article in *Justitiële verkenningen*, a magazine published by the Ministry of Justice's WODC, entitled "The Share of the Drug Sector in the National Income"[11] estimates that the total contribution of production and trade in drugs to the national income rose from EUR1 300 million in 1995 to EUR1 800 million in 1998, and then dropped to EUR1 200 million in 2008.[12]

59. As far as cocaine is concerned, the primary countries used to move the product from source countries to the European market are the Netherlands and Spain, mostly by sea.[13] UNODC estimates that a total of 212 metric tons of cocaine were sent to Europe to satisfy an annual consumption[14] of 124 metric tons. The Dutch National Threat Assessment 2008[15] cites a 2004 study estimating that the annual use in the Netherlands is between 4 and 5.4 tons. According to the UNODC's 2010 World Drug Report, 12% of those arrested in France for trafficking cocaine were Dutch nationals,[16] illustrating the importance of the Netherlands as a transit country for illicit substances.

60. The Netherlands does appear to have taken action in response to this threat. Cocaine seizures have dropped markedly in recent years, presumably as a result of increased controls, especially in the Antilles and at Schiphol airport, and proactive enforcement.[17]

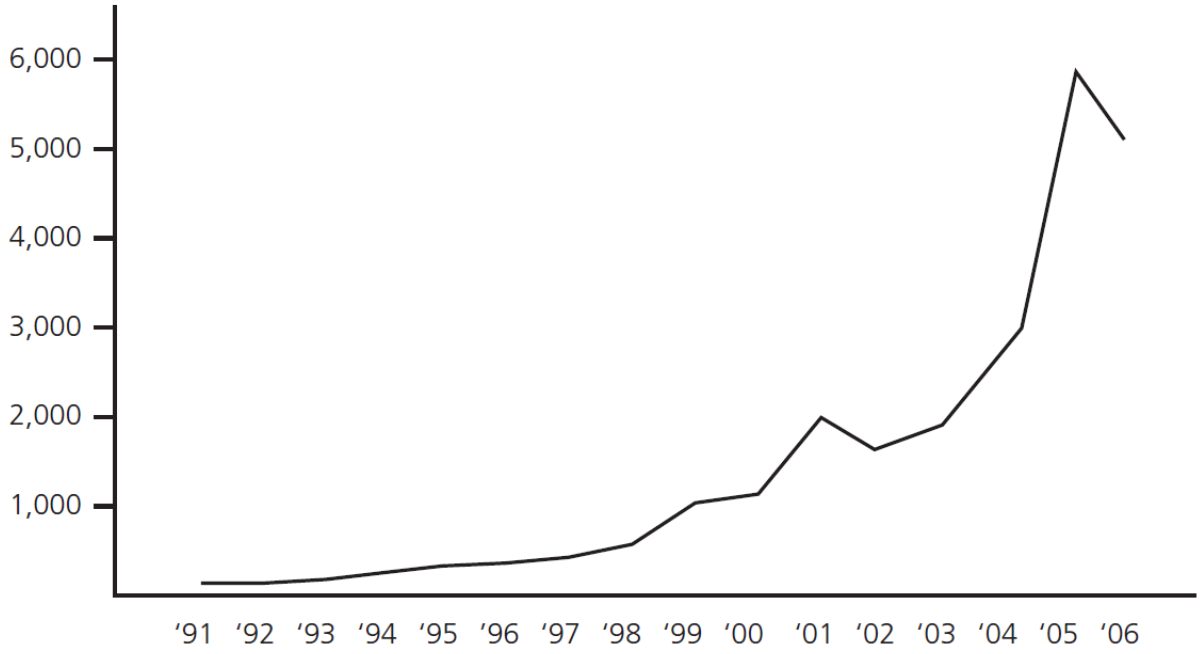
61. Heroin routes lead from the east to the U.K. and the Netherlands.[18] According to the report, "[t]he Netherlands is a hub for heroin trafficking to France, the United Kingdom, Belgium, as well as Germany. In the Netherlands, the total number of arrests made by customs authorities is limited."[19]

62. Indoor growth of cannabis has spread from the Netherlands and the drug is exported. Production estimates vary between 36 tons in 1995 to 766 tons in 2006. The NTA 2008 estimated that between 10% and 74% of the cannabis produced in the Netherlands is destined for export.[20] Which means that between 7 and 104 tons were smuggled out of the country in 2006. The authorities admit that they do not know the scale of the exports.

10 Council of Europe, Group of States against Corruption (GRECO), Third Evaluation Round "Evaluation Report on the Netherlands on 'Incriminations (ETS 173 and 191, GPC 2' (Theme I) (Greco Eval III Rep (2007) 8E, Theme I).
11 "Het aandeel van de drugssector in het nationaal inkomen," p. 25-42 (Justitiële verkenningen, jrg. 36, nr. 7, 2010 – Informele economie, uitbuiting en illegaliteit).
12 The authors of the article indicate that the numbers depend on the estimation of the chance of confiscation of imported drugs, and discovery of cannabis farms and XTC labs, requiring the estimations to be interpreted with some caution (*ibid*, p. 40).
13 United Nations Office of Drugs and Crime, World Drug Report 2010, p. 19.
14 UNODC, World Drug Report 2010, p. 18 (estimated consumption in 2008).
15 By KLPD-IPOL, p. 33.
16 UNODC, World Drug Report 2010, fig. 56, p. 90.
17 UNODC, World Drug Report 2010, p. 85.
18 UNODC, World Drug Report 2010, pp. 22 and 54.
19 UNODC, World Drug Report 2010, p. 57.
20 NTA 2008, p. 59.

63. The number of nurseries, where cannabis plants are grown, has continued to rise since the early 1990s, as illustrated in the chart below. In 1991 only 54 nurseries were dismantled, by 2005 this number had increased to almost 6 000.[21] If they produce between 61 and 142 tons per year, at a wholesale price of EUR3 000 per kilogram, the value of cannabis at the retail level is estimated to lie somewhere between EUR182 and EUR424 million per year.[22] If we take the high end of the estimate, this is slightly more than one third of the estimated total POC figure for drugs (see table with Average POC estimates per crime category below) and must be laundered. In addition, news reports indicate that there is often a link between real estate and cannabis growers, in that the owner of a particular building or piece of land sometimes allows, or even seeks, for his property to be used for the production of cannabis.

Figure 1. Number of dismantled nurseries between 1991 and 2006



Note: Graph taken from the National Threat Assessment–Organised Crime 2008 (KLPD – IPOL), p. 58.
Source: Netherlands Police Agency, Department of International Police Information (IPOL).

Links between Businesses and Crime

64. In the early 2000s the demise of a number of companies utilizing Dutch offshore services revealed the vulnerability of the Dutch financial system to large scale international fraud schemes and was a strong signal of the relationship between business and crime. In 2006 the Dutch Central Bank issued new rules because of concerns, expressed in a report, that "[trust] offices could be used by people with an interest in remaining anonymous, for reasons that cannot bear the light of day. This would impair the integrity of the financial system."[23]

65. In October 2008 a Working Group of the Dutch House of Representatives produced a report on the interconnectedness between the upper and the underworld.[24] In its conclusions the Working Group

21 "Het Groene Goud," p. 54.
22 "Het Groene Goud," p. 61.
23 Shaken Trust: The Netherlands Rethinks an Offshore Industry (The New York Times, February 19, 2004).
24 "Verwevenheid van de bovenwereld met de onderwereld – Rapport van de parlementaire werkgroep verwevenheid onderwereld/bovenwereld" (Joldersma, Teeven, de Wit, Heerts, Anker, de Roon, October 2008).

describes a grey zone between legal and illegal behaviour, especially in the real estate sector. Its conclusions were three-pronged. First, more research is needed into the possibilities for, and restrictions on, information exchange between various authorities and databases. Second, it requested the Justice Commission to organize a hearing regarding the abuse of professional privilege and the duty of secrecy by notaries and lawyers. Finally, with regard to the real estate sector, the Working Group proposed to take the following measures in the short term: a better protection of the profession of appraiser, to extend the Public Administration (Probity Screening) Act (*Wet bevordering integriteitsbeoordelingen door het openbaar bestuur*, Wet BIBOB) to the real estate sector, to improve MOT-reporting, to increase information exchange.

66. According to the NTA 2008, IPOL linked the database of names on the EU list of criminal organizations and Dutch Chambers of Commerce to check if and to what extent criminal suspects were linked to businesses. The NTA notes that: "Of every four suspects on the list for 2006, one is registered as a stakeholder in a company" and "the number of registered criminal organisations that can influence or that control companies through (core) members […] is 74.3%." The table below lists the sectors in which these companies are involved.

67. A number of caveats should be considered in relation to this IPOL research, which is still at a preliminary stage: The definition of financial institutions is broader than the FATF definition; the names in the database are suspected criminals not convicted criminals; there is a selection bias in the study, since it looks in particular at the persons that own a company; it is unclear if the companies are used for criminal activities, and; the nature and impact of alleged criminal's presence in these companies is unclear. This said, this innovative and forward-thinking initiative is an interesting attempt to better understand the links between businesses and crime.

Companies with a link to suspected criminal groups, by sector

Sector	Number
Financial institutions (except insurance companies and pension funds)	220
Other commercial services	136
Wholesalers and brokers (not involving cars or motorbikes)	94
Provision of accommodation, meals and drinks (catering establishments)	71
Leasing of and trading in property	71
Trading in and repairing cars and motorbikes; petrol service stations	66
Stock exchanges, stockbrokers, insurance brokers, etc.	61
Employer, employee and professional organizations; ideological and political organizations	54
Retail trade and repair of consumer articles	50
Culture, sport and recreation	49
Construction	48
Other	139
Not known (no code)	77
Total	**1 136**

Cited in: National Threat Assessment 2008, p. 204.
Source: KLPD, IPOL, EU list of criminal organizations 2006; Chambers of Commerce.

Misuse of companies in 2000, 2002 and 2004 (absolute numbers)			
	2000	2002	2004
Company liquidations discharged	3 758	3 948	5 939
of which: Criminal damage	380	340	359
of which: Shell companies, dubious activities	114	88	133

Cited in: National Threat Assessment 2008, p. 100.
Source: CBS (Statistics Netherlands), Statline.

1.2.2 Money Laundering

A Major Financial Center

68. The country's excellent communications network, convenient transportation infrastructure, highly developed financial services industry, and the fact that Rotterdam is one of the world's busiest ports, make it an interesting target for money launderers. The country has been described as a transit country for crime by academics.[25]

69. In August 2010 the IMF identified a list of 25 jurisdictions with the most systemically important financial sectors, in the context of the integration of the Financial Sector Assessment Program (FSAP) assessments into Article IV surveillance.[26] The list considers the size and the interconnectedness of jurisdictions' financial sectors.[27] Out of 25 countries,[28] the Netherlands ranks in seventh place overall, in ninth place in terms of size, and in sixth place as far as interconnectedness is concerned.

70. The figure below is based on Fund staff estimates.[29] It shows the U.K. to be more or less in the center of the global banking system. The Netherlands is very close to the center of the system, much closer than, for example, the United States. Due to the level of development of the Dutch financial system, notably the variety of products offered by the sector and the interconnectedness to the international financial system, the country has characteristics attractive to money launderers.

25 "The Amount and Effects of Money Laundering," University of Utrecht and Australian National University, 2006, p. 8.
26 IMF Board Executive Board Paper "Integrating Stability Assessments Under the Financial Sector Assessment Program into Article IV Surveillance" and "Background Material" (SM/10/235 & Supplement 1, August 31, 2010).
27 "Interconnectedness" is defined as "the extent of linkages of a particular financial sector with financial sectors in other jurisdictions. Interconnectedness captures the potential for systemic risk that can arise through direct and indirect interlinkages, so that an individual failure or malfunction has repercussions around the financial system, leading to a reduction in the aggregate amount of services." (SM/10/235, Supplement 1, par. 6, p. 4).
28 The 25 countries are: Australia, Austria, Belgium, Brazil, Canada, China, France, Germany, Hong Kong SAR, India, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Russia, Singapore, South Korea, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States.
29 Figure taken from IMF document SM/10/235, Supplement, 1, p. 14.

Figure 2. Position of the 25 jurisdictions with systemically important financial sectors in the global banking network.

Note: Lines between jurisdictions reflect the connections between their respective banking systems. For simplicity, only the connections between each of the 25 jurisdictions and the rest of the global network are shown.

Proceeds of Crime

71. In 2006, the Utrecht School of Economics published a study funded by the Dutch Ministry of Finance, on "The Amounts and Effects of Money Laundering." On a macro level the academics calculated that about EUR18 billion are laundered in or through the Netherlands each year. Although the estimate received a lot of criticism, it nevertheless provides an indication. This study estimated the money generated in the Netherlands which is laundered in the Netherlands itself at EUR3.8 billion, and the flow to the Netherlands from abroad at EUR14 billion.[30] According to this study, most of the money generated for laundering comes from drugs and fraud[31]. Real estate was seen as a very important method to launder money. Other forms of money laundering that the report mentions are bank transactions, back-to-back loans, money transfers, money exchange offices, trust offices, casinos, underground banking, cash smuggling and special purpose entities.

72. In order to account for criticism and to integrate more recent information, we calculate estimates of proceeds of crime generated in the Netherlands (see table below).[32] The main sources of criminal proceeds in the Netherlands appear to be fraud, including tax fraud, and illicit narcotics.[33] The total in billion US$ as brought to 2009 currency is approximately $14.6 billion, equivalent to 1.84 percent of the

30 See p. 61 of the report at: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2006/02/16/onderzoeksrapport-the-amounts-and-the-effects-of-money-laundering/witwassen-in-nederland-onderzoek-naar-criminele-geldstromen.pdf

31See p. 48 of the report at: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2006/02/16/onderzoeksrapport-the-amounts-and-the-effects-of-money-laundering/witwassen-in-nederland-onderzoek-naar-criminele-geldstromen.pdf

32 The proceeds of crime can vary over time. Due to e.g. price fluctuations of raw materials, market conditions, and law enforcement actions profitability can increase or decrease. Because of this, the POC numbers could therefore be biased in that the numbers are not always available for every year, leading to a possible over or underestimation of the POC.

33 The main sources for the table are Unger's study and Dutch governmental organizations.

Dutch GDP. Approximately $11.2 billion was related to fraud (including tax fraud), and another $2 billion to drug offenses.

NL Average POC estimates for offenses for which there was data available				
Crime Category[1]	**NL POC Average Annual Estimate 2001-2009 (in 2009 USD)**	**% of NL GDP**	**% of G8 GDP**	**% of WGDP**
Counterfeiting and piracy of products[2]	$145 964 472	0.02%	0.00%	0.00%
Environmental crime[3]	$1 828 890	0.00%	0.00%	0.00%
Fraud, including tax fraud[4]	$11 298 521 656	1.42%	0.04%	0.02%
Illegal gambling[5]	$227 055 846	0.03%	0.00%	0.00%
Illicit trafficking in narcotic drugs and psychotropic substances[6]	$1 629 373 854	0.20%	0.00%	0.00%
Illicit trafficking in stolen and other goods	$81 091 373	0.01%	0.00%	0.00%
Robbery or theft[7]	$620 507 915	0.08%	0.00%	0.00%
Sexual exploitation, including sexual exploitation of children[8]	$267 601 532	0.03%	0.00%	0.00%
TOTAL ML	**$14 271 945 538**	**1.79%**	**0.04%**	**0.02%**

Note: According to the April 2010 IMF World Economic Outlook, NL GDP: $794 777 000 000, G8 GDP: $32 220 515 000 000, World GDP: $57 937 460 000 000.

[1] This table does not list all of the FATF's designated categories of offenses since reliable figures cannot always be found. The most notable omission is corruption, which is generally considered among the crimes generating the most proceeds. However, the country occupies the seventh place in Transparency International's 2010 Corruption Perceptions Index, indicating a low level of corruption.

[2] De illegale economie in Nederland, Verbruggen & Smekens (Centraal Bureau voor de Statistiek, Webmagazine, September 20, 2004).

[3] National Threat Assessment 2008, p. 117.

[4] See above.

[5] Smekens, M. and Verbruggen, M. (2004). "De Illegale Economie in Nederland." Centraal Bureau voor de Statistiek, 20 September, 2004; cited in Unger *et al*. (2006, p. 48).

[6] Smekens, M. and Verbruggen, M.; Centraal Bureau voor de Statistiek, Webmagazine, (September 20, 2004); National Threat Assessment 2008.

[7] Criminaliteit en rechtshandhaving 2001, WODC, 2003, p. 60; taken from NIPO 2002; cited in Unger *et al*. (2006, p. 47); National Threat Assessment 2008.

[8] Smekens, M. and Verbruggen, M. (2004). "De Illegale Economie in Nederland." Centraal Bureau voor de Statistiek, 20 September 2004; cited in Unger *et al*. (2006, p. 48); "Amsterdam Closing Red Light District," 13 February 2008, Digital Journal.

73. The table only comprises proceeds of crimes committed in the Netherlands and laundered in the Netherlands. Not all proceeds of crimes generated in the country are laundered in the country, and some of the laundered proceeds originate in foreign countries. In this respect we must note the role of Dutch TCSPs. In the above mentioned report from the University of Utrecht, interviewees indicated that they suspected that approximately 1% of the money transiting through Dutch TCSPs from abroad is related to money laundering. Research indicates the size of the Dutch trust industry in 2006 to be approximately EUR4 500 billion,[34] equivalent of about 5.6% of the Dutch GDP.

34 Quarterly Bulletin DNB, March 2007, p. 62 cited in "Tax haven and development partner – Incoherence in Dutch government policies?" Weyzig & van Dijk, SOMO, Amsterdam, June 2007; "The Dutch Trust Industry – Facts and Figures," p. 27, SEO Economic Research, Amsterdam, April 2008.

Investigations, Prosecutions, and Seizures

74. The table below shows that the number of criminal investigations has steadily increased since 2004. As of 2008, the last year for which complete statistics are available, there were four times more pure or mixed ML investigations than four years earlier, showing a steady increase of the use of AML provisions in the law.

Number of Criminal Investigations in the Netherlands for pure or mixed ML investigations brought to the Public Prosecutor (provided by the Ministry of Justice)	
Year	**Criminal investigation – pure/mixed ML**
2004	332
2005	365
2006	861
2007	1 174
2008	1 170
2009 (1/1-30/6)	770
Total	**4 672**

75. According to prosecution data in the table below, the most prosecuted proceeds generating crimes in the Netherlands are drug related offenses, human trafficking, and criminal organizations. This is broadly in agreement with the proceeds of crime (POC) estimates table above. For each of the three offenses listed in the table below there is an increased use of AML provisions over the latter part of the decade.

ML prosecutions combined with certain other offenses (provided by the Ministry of Justice)			
Year	**ML & human trafficking**	**ML & drug related offense**	**ML & criminal organisation**
2004	6	111	62
2005	1	107	71
2006	3	254	189
2007	16	356	223
2008	29	325	152
2009 (1/1-30/6)	13	150	77

76. The table below sets out the outcomes of prosecutions of pure and mixed money laundering offenses.[35]

Results from prosecutions for pure and mixed ML prosecutions (provided by the Ministry of Justice)				
year	**Conviction**	**Merge**	**Acquittal**	**Other**
2004	128	7	17	
2005	184	7	23	1

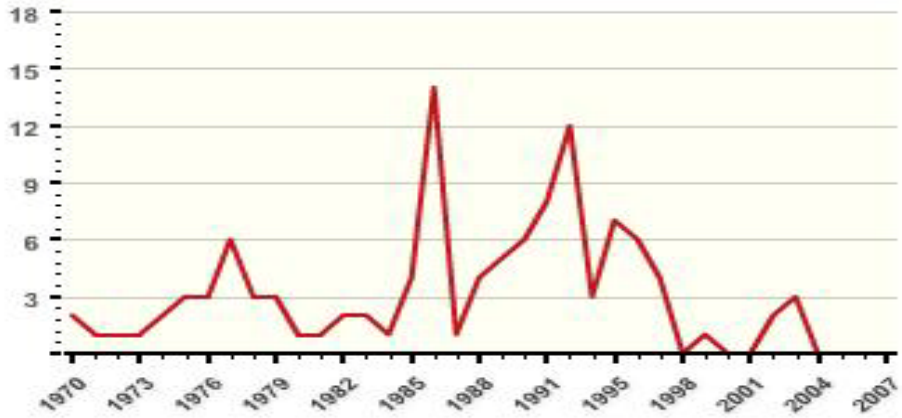
35 "Merge" refers to cases where one court proceeding was later merged with another court proceeding against the same person. "Other" means any decision other than a conviction, merger, or acquittal, e.g. invalidity of the subpoena, incompetency of the court, stay of prosecution, etc.

Results from prosecutions for pure and mixed ML prosecutions (provided by the Ministry of Justice)				
2006	302	5	36	8
2007	487	26	54	6
2008	647	25	81	8
2009 (1/1-30/6)	348	7	57	3

77. The number of seizures has also increased. In August 2009, the public prosecutor in Maastricht, province of Limburg, seized 134 buildings and lots belonging to a person suspected of laundering proceeds of crime, tax fraud, and growing marihuana.[36] People operating a business involved in real estate, mortgages and insurance were also suspected.[37] A notary and two banks were also scrutinized by the authorities. This indicates ties between illegal enterprises and seemingly legitimate businesses.

1.2.3 Terrorism and terrorist financing

78. The National Consortium for the Study of Terrorism and Responses to Terror (START)[38], based at the University of Maryland in the United States, Global terrorism database, contains data about terrorist incidents in the Netherlands since 1970 with the following profile:



79.

80. The country has experienced 115 terrorist incidents since 1970, their number peaking in 1986 and 1992. According to the database, terrorist organizations that are currently active or have been active in the Netherlands are: Actiefront Nationalistisch Nederland, Al-Qaeda, Armenian Red Army, Community Revolutionaries in Europe, Free South Moluccan Youths, Pan-Turkish Organization, South Maluku Republic (RMS), South Moluccan Suicide Commando, Stop Huntington Animal Cruelty (SHAC), and Takfir wa Hijra.

81. This shows that the country has had experience dealing with a variety of terrorist organizations, ranging from discontented Moluccans, over Palestinians and extreme left wing organizations, to, most

36 Operatie Schone Handen (Elsevier, March 6, 2010).
37 "Ondernemers Vast in Zaak Joep J." (http://www.strafrechtadvocaten.nl, 22 April 2010).
38 This database is used as a source of information as it is one of only a few to offer a comprehensive listing of terrorist incidents across the world. Not all incidents recorded in this database are recognized by all nations as "terrorist incidents."

recently, fundamentalist Islamic organizations. At present, the main threat to the Netherlands seems to come from international Islamist extremists.[39]

82. The Islamist extremist threat in the Netherlands is currently deemed to be limited.[40] According to the NCTB[41] this would mean that the likelihood of the country experiencing a terrorist attack cannot be ruled out entirely, but the probability is deemed to be low. As the Twelfth Counterterrorism Progress Report[42] was released the press release indicated that "Dutch interests abroad are more vulnerable to the risk [of] terrorist attack" and that "the threat against the Netherlands itself still mainly comes from transnational networks that could mainly manifest themselves via Dutch or European jihadists returning from training camps or areas of conflict." At the same time the report stated that "[l]ocal networks in the Netherlands remain, for the time being, weak and leaderless." And that "[t]o the extent that Dutch jihadists are indeed developing activities, it appears they mainly wish to focus on participation in the jihad in Afghanistan, Pakistan and Somalia."

83. In April 2010 several members of the Liberation Tigers of Tamil Eelam (LTTE) were charged with terrorism. Seven people were arrested and EUR40 000 in cash was seized, among other things. The DNR investigated with the help of the Fiscal Intelligence and Investigation Service - Economic Investigation Service (*Fiscale Inlichtingen- en Opsporingsdienst – Economische Controledienst*; hereafter: FIOD-ECD) after a tip from the General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst*; hereafter: AIVD). The suspects were presumably involved in gathering funds through collections, fundraisers, sale of DVDs and calendars, and the organization of illegal lotteries. These activities appear to have continued after the LTTE's military defeat in 2009.

1.3 Overview of the Financial Sector

84. The Netherlands has a modern and developed financial sector which contributes 6-7 percent to the overall GDP. The largest sectors of the financial services industry are banking, insurance, and pension funds and are represented by some of the largest banks and insurers in the world. The private fund management sector is one of the most sophisticated in Europe, as is venture capital.

85. The Netherlands financial services regulatory system is structured according to the "Twin Peaks" model. The Dutch Central Bank (*De Nederlandsche Bank*; hereafter: DNB) focuses on the prudential objective of promoting the soundness of financial institutions, while the Netherlands Auhority for the Financial Markets (*Autoriteit Financiële Markten*; hereafter: AFM) focuses on the conduct of business objective of enhancing orderly and fair market practices. Integrity supervision including AML/CFT supervision is performed by both. The institutions under the purview of DNB for integrity supervision are banks, insurance companies, pension funds, bureaux de change, and money transfer offices. AFM supervises approximately 14 000 financial institutions; the majority of them are financial service providers, approxmiately 10 000, but also investment firms and investment institutions numbering 400.

39 According to the University of Maryland's GTD, the most recent fatality due to terrorism in the Netherlands was the murder of the Dutch filmmaker Mr. Theo van Gogh in November 2004. In May 2002 Dutch politician Mr. Pim Fortuyn was murdered by a member of an environmental organization.

40 The National Coordinator for Counterterrorism distinguishes four threat levels: Minimal, Limited, Substantial, and Critical. According to the website this means that there are no new trends or phenomena that constitute a threat, activities by terrorist networks have been hindered, the Netherlands is seldom or never mentioned in statements issued by terrorist networks that pose a serious threat.

41 Nationaal Coördinator Terrorismebestrijding / National Coordinator for Counterterrorism.

42 Published on June 18, 2010 by the National Coordinator for Counterterrorism.

Assets financial sector	Q4 2009
	Million euro
Banks	2 649 890
Insurers	368 709
Pension funds	743 198
Investment companies	445 237
Other financial institutions	351 773

Banking

86. The banking sector is comprised of 103 banks, 58 of which are Dutch and banks that are part of a financial conglomerate. The remaining 45 are banks that have a foreign parent company (in or outside the EU) or are branches of EU banks or non-EU banks. The four largest banks (ABNAmro Bank, ING Bank, Rabobank, and SNSReaal) account for about 80 percent of the Dutch banking market. Up to October 2009, 28 money transaction offices (which included money transfer offices and bureaux de change) were registered with and supervised by DNB.

Insurance

87. In early 2010 the insurance sector was composed of a total of 312 insurers including 60 life insurers, 33 benefits-in-kind and funeral expenses insurers, and 213 nonlife insurers. Banking and insurance industries may be combined in a single financial institution, however the financial crisis has had an impact on this practice and ING, for example, is divesting its insurance business almost entirely. DNB supervises 62 life insurers.

88. Insurance companies in the Netherlands perform a number of functions. Insurance companies make substantial loans for which there is an extensive system of brokers. Insurance companies also grant morgages and purchase real estate.

Asset Management

89. The Netherlands has a large, well developed and managed asset management sector comprised of pension funds, investment funds including equity funds, bond funds, real estate funds, hedge funds and mixed funds. At the end of 2009 investment funds (excluding pension funds and insurers) had assets under management of EUR445 billion. The Netherlands has one of the world's most highly-developed pension fund industries with private assets under management among the highest in Western Europe. The value of pension funds' equity and debt portfolios stood at EUR649 billion at the end of 2009.

Financial activity	Type of financial institution that performs this activity	Supervisor
Acceptance of deposits and other repayable funds from the public	Credit institutions, financial institutions	DNB, AFM
Lending	Credit institutions, financial institutions	DNB, AFM
Financial leasing	Credit institutions, financial institutions	DNB, AFM
The transfer of money or value	Credit institutions, financial institutions	DNB, AFM
Issuing and managing means of payment (*e.g.*, credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).	Credit institutions, financial institutions	DNB, AFM
Financial guarantees and commitments.	Credit institutions, financial institutions	DNB, AFM
Trading in: (a) money market instruments (cheques, bills, CDs, derivatives etc.); (b) foreign exchange;	Credit institutions, financial institutions, investment firms.	DNB, AFM

Financial activity	Type of financial institution that performs this activity	Supervisor
(c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading.		
Participation in securities issues and the provision of financial services related to such issues.	Credit institutions, financial institutions, investment firms.	DNB, AFM
Individual and collective portfolio management.	Financial service providers, investment firms and investment institutions.	DNB, AFM
Safekeeping and administration of cash or liquid securities on behalf of other persons.	Investment firms, financial service providers.	DNB, AFM
Otherwise investing, administering or managing funds or money on behalf of other persons.	Investment firms, financial service providers.	DNB, AFM
Underwriting and placement of life insurance and other investment related insurance.	Insurance companies, pension funds	DNB, AFM
Money and currency changing.	Credit institutions, financial institutions, bureaux de change.	DNB, AFM

Financial corporations: balance sheet[1]						
Subjects		**Periods**	**Financial corporations**	**Institutional investors**	**Monetary financial institutions**	**Other non-monetary fin. institutions**
Assets	Total assets	2005	mln euro	1 108 522	1 746 703	469 822
		2006		1 208 227	1 911 905	547 212
		2007**		1 238 237	2 256 929	703 042
		2008*		1 121 503	2 190 269	680 090
© Statistics Netherlands, Den Haag/Heerlen April 19, 2010						

[1] Source: http://statline.cbs.nl

1.4 Overview of the DNFBP Sector

Casinos

90. Pursuant to the Games of Chance Act (*Wet op de kansspelen*), it is forbidden to compete for prizes or premiums if the winners are selected by any determination of chance on which the participants cannot exert an influence, unless a permit has been issued by the Minister of Justice according to the Games of Chance Act. At present, the Games of Chance Act does not provide for the granting of permits to organize games of chance via the internet, and therefore it is forbidden. The only organization licensed to run a casino under the Games of Chance Act is Holland Casino.

91. Holland Casino is under government control; the members of the Supervisory Board are appointed by the Minister of Finance. Net operating profit from Holland Casino fell in 2008 with 83.3 percent to EUR14.3 million (2007: 85.6 million). The total amount payable to the state in 2008 came up to EUR189.6 million (2007: 268.2 million).

Real estate agents

92. There are approximately 8 500 real estate agents in the Netherlands. Most of them are member of a professional organization. The three biggest professional organizations for real estate agents are the Dutch Association of Real Estate Brokers and Real Estate Experts (*Nederlandse Vereniging van Makelaars*, NVM, 4 200 members), Intermediary Association for Real Estate, (*Vereniging Bemiddeling Onroerend Goed*, VBO, 1 000 members) and National Association for Real Estate Agents (*Landelijke Makelaars Vereniging*, LMV, 500 members). Almost 70 percent of Dutch houses are sold by NVM members. NVM members had a total turn-over in 2008 of approximately EUR 972 million.

Dealers in precious metals and stones

93. In the Netherlands, every seller of goods acting in the course of a business or profession, insofar as payment for these goods is made in cash for an amount of EUR15 000 or more (regardless of whether the transaction takes place in one operation or in several related operations) falls under the scope of the WWFT. About 4 800 companies in the Netherlands are involved in the sale of precious stones, metals, jewelry, and jewels. Two of the professional organizations in this branch are the Federation for Gold and Silver (*Federatie Goud en Zilver)* and the Association for the Trade in Diamonds (*Vereniging voor de Diamanthandel).*

Notaries

94. Around 4 500 (junior) notaries are providing their services in the Netherlands. The Dutch law requires a notarial instrument for a number of agreements and legal transactions. The most important are conveying real property in the Netherlands, creating or cancelling mortgages, incorporating public or private limited liability companies or altering their articles of association, establishing foundations or associations (including cooperatives) or altering their constitution, drawing up, altering and executing wills, drawing up or altering marriage contracts (*i.e.* usually ante-nuptial settlements) and registered domestic partnership agreements, transferring registered shares, legalizing signatures and providing for gifts and donations in a notarial instrument. Civil-law notaries are by law members of the Royal Dutch Notarial Society.

Lawyers

95. There are approximately 16 000 lawyers in the Netherlands (3 800 offices). According to the Netherlands' Bar Association (*Orde van Advocaten*), about one third of this number provides, at least occasionally, services that fall within the scope of the WWFT, Lawyers are by law member of this Association.

Accountants

96. Approximately 12 000 public chartered accountants (*externe register accountants*, RA-accountants) are carrying out their activities in the Netherlands. Public chartered accountants are, by law, members of the NIVRA (*Koninklijk Nederlands Instituut van Registeraccountants*): a body governed by public law, appointed by the government. There are about 6 500 public chartered accountant-business administration consultants (*externe accountants-Administratieconsulenten, AA-accountants*) in the Netherlands. An AA-Accountant is an internationally-recognized accountant who is authorized to perform audits, comparable with the English Chartered or Certified Accountant. An AA-Accountant meets the European Directives for statutory audits and specializes in small and medium-sized enterprises. The profession of AA-Accountant and the use of the AA title are laid down and protected by law. This law guarantees the independence, expertise, and reliability of AA-Accountants. Public accountant-business administration consultants are, by law, members of the NOVAA: a body governed by public law,

appointed by the government. Certain tax advisors are privately organized (not by law). There are approximately 11 000 tax advisors in the Netherlands; 4 500 are members of the Dutch Association of Tax Advisors (*Nederlandse Orde van Belastingadviseurs*, NOB). Finally, there are about 10 000 other independent legal advisers and financial economic advisers performing activities in the Netherlands.

Trust and Company Service Providers

97. As per December 31, 2009, there are 167 licensed TCSPs. These TCSPs are supervised by DNB. The International Management Services Association (VIMS) and the Dutch Fiduciary Association (DFA) are the two professional organizations that are engaged in this type of business.

98. In 2006, the turnover realized by the TCSPs amounted to EUR247 million, coming from approximately 20 000 object companies and 16 000 clients.

1.5 Overview of commercial laws and mechanisms governing legal persons and arrangements

99. Book 2 of the Dutch Civil Code regulates the establishment, management, and dissolution of legal entities established under Dutch law. Pursuant to Article 3 of the Civil Code, legal entities in the Netherlands may take the form of an (1) association (2) cooperative (3) public limited company ("NV") (4) private limited company ("BV") or (5) foundation.

100. Legal entities in the Netherlands are set up by way of notarial deed. For BV's and NV's, a certificate of "no objection" issued by the Ministry of Justice has to be obtained as well. Legal entities set up under Dutch law are incorporated for an indefinite period of time.

101. All forms of legal entities are required to register with the Dutch Chamber of Commerce and to file annual tax returns with the Tax and Customs Administration. Foreign companies are registered with the Chamber of Commerce only if they have a branch or commercial undertaking in the Netherlands.

102. Dutch legal entities require at least one director, whereby both natural and legal, foreign and Dutch persons and residents may serve as company directors. The authorities stated that it would be very common for Dutch legal entities to have legal entity directors, including foreign legal entity directors. Company records have to be kept for at least seven years.

103. BVs may be set up by one or more natural or legal persons and are managed by one or more directors, which are elected by the shareholders. Any powers not conferred upon the directors remain vested in the general meeting of shareholders. BVs may issue only registered but no bearer shares. Any transfer of ownership of BV shares is subject to notarial authentication. Shares of a BV may not be offered for public trading or subscription.

104. NVs are subject to the same establishment requirements and closely follow the ownership and management structure of the BV. In contrast to BVs, however, NVs may issue both registered and bearer shares and the transfer of NV shares is not subject to any notarial oversight. Dutch NVs require a higher stock capital than BVs and its shares may be publicly traded.

105. Dutch Foundations just like BVs and NVs are set up by notarial deed and subsequent registration with the Chamber of Commerce. They have no members and may not issue any shares or possess any share capital. Foundations are incorporated to realize a certain stated objective. Any profits of the foundation's activities may only be used to accomplish its stated purpose and may not be distributed. Dutch foundations are usually set up for idealistic or social objectives but may also be used as asset (in particular share) holding entities or to carry out commercial activities. Foundations require at least one founder and one chairman.

106. An association under Dutch law is a partnership between two or more members to achieve a certain goal. Associations are allowed to make profits, however, these may be used only to further the common goal and profits may not be distributed. Only associations with full legal personality are set up by notarial deed and are required to register with the Chamber of Commerce. Associations with limited liability may but are not required to register.

107. Cooperatives are legal entities in which a number of persons combine their resources to facilitate their individual but similar interests. Cooperatives may be established by two or more members through a notarial deed and subsequent registration with the Chamber of Commerce. After incorporation, the number of members may be reduced to one. A Cooperative has no minimum capital requirement and may not issue any shares or certificates. Cooperatives may carry out any type of activity, including acting as holding company or finance company.

108. In addition to the above mentioned legal entities, European Companies (SE) and European Cooperative Societies may be established and registered in the Netherlands. Both are subject to the same registration requirements as BVs and NVs.

109. Statistics on legal persons are kept by the Central Bureau for statistics and the Chamber of Commerce. As of December 31, 2009, a total of about 1.1 million Dutch and 7 000 foreign and European companies were registered with the Chamber of Commerce. Representatives of the Chamber of Commerce stated that over the past years, the number of foundations incorporated increased significantly and explained that this may be due to the fact that foundations do not need a minimum capital, are easy to incorporate, and are not required to publish financial information.

Total Number of Companies Registered with the Chamber of Commerce as of December 31, 2009		
Number of legal persons		
Legal person	**Type**	**Number**
Private corporations		
	Private limited liability companies	763 766
	Public limited liability companies	3 642
	Foundations	181 936
	Associations	117 398
	Cooperative societies	5 277
	Mutual companies	426
	Associations of proprietors	115 000 (estimate)
Public corporations		1 000 (estimate)
Religious communities with corporate personality		unknown
Other entities registered		
	Foreign corporations	6 905
	European economic ventures	63
	Foreign corporation with main office in the Netherlands	45
	Branch of a corporation with main office abroad	7

110. Dutch NPOs may operate in the form of “foundation,” “association” (either formal or informal), NV, or BV. As outlined above, all foundations and formal associations are required to register with the Chamber of Commerce. Informal associations may but are not required to register. As of the end of 2009, 182 000 foundations and 125 425 associations with a “charitable purpose” were incorporated in the Netherlands.

Total Numbers of NPOs as of 2009.	
Foundations	182 000
Associations	125 425

Legal Arrangements:

111. Dutch law does not provide for the establishment of legal arrangements such as express trusts or *Treuhand*. However, trusts incorporated under the laws of another country may conduct business in the Netherlands and, if they operate an undertaking in the Netherlands, register with the Chamber of Commerce. At the time of the assessment mission it was not clear exactly how many foreign trusts were registered with the Chamber of Commerce. Anecdotal evidence suggests that the number of foreign trusts administered in the Netherlands is rather low. The Netherlands has signed and ratified The Hague Convention on Law Applicable to Trust and their Recognition on September 28, 1995.

1.6 Overview of strategy to prevent money laundering and terrorist financing

1.6.1 AML/CFT Strategies and Priorities

General

112. Tackling money laundering is of major importance in effectively combating a wide range of other serious crimes. It harms the integrity of financial and economic transactions and leads to a situation whereby (organized) crime becomes interlinked with the legal economy. Through concealing the criminal origin of proceeds from crimes, criminals can remain beyond the reach of investigating agencies. Moreover, the accumulated wealth provides criminals with the opportunity to obtain positions in bona fide enterprises.

113. The Netherlands runs a significant risk of terrorist attacks because it participates in military operations abroad, maintains close ties with the United States and has groups within its borders that are susceptible to radicalization. Central government has made counterterrorism in the Netherlands a priority. Large investments have been made to increase the capacity of the intelligence and security services and improve the exchange of information between them. The surveillance and protection system has been revamped and new legislation drafted to facilitate counterterrorism efforts and make it easier to prosecute perpetrators.

114. In all, the position of National Coordinator for Counterterrorism (*Nationaal Coördinator Terrorismebestrijding*, NCTb) was established to improve cooperation between agencies. More specifically, the NCTb is responsible for policy development, analysis of intelligence and other information and coordination of antiterrorist security measures.

Combating fraud

115. The main principle of combating fraud is prevention. Where prevention alone is not enough, this is followed by a differentiated approach: rapid and minor correction in the case of incidental fraud, and criminal enforcement in the case of systematic or methodical fraud. The level of fines is high, and the Tax and Customs Administration has the power to impose additional claims.

Reinforcing confiscation

116. The WvSr knows various bases for confiscation. The WvSr not only provides for a basis for the confiscation of objects, generally referred to as “ordinary confiscation” but also provides for “special

confiscation" proceedings. These proceedings may result in an obligation to pay a sum of money that represents illegally-obtained profits or advantages (confiscation order).

117. Confiscation is a general instruction of the Public Prosecution Service *(Aanwijzing ontneming*). This procedure urges all prosecutors to investigate and seize criminal proceeds in case of an intended required fine of at least EUR500 or criminal proceeds estimated at the moment of seizure to be EUR500.

Administrative approach

118. The authorities aim to reinforce the preventative and administrative approaches not only by fighting organized crime with traditional policing, but also with administrative measures under the leadership of *e.g.*, the local municipal authority.

119. Due to capacity constraints, it has been used almost exclusively in a few big municipalities, such as Amsterdam. The goal is to achieve a regional and national application of the administrative approach in order to prevent criminals from escaping simply by moving to a different municipality.

120. In order to solve this problem, 11 information and expertise centers (*Regionale Informatie en Expertise Centra*, RIEC's) are financed by the national government in the form of pilot programs.

121. The Public Administration (Probity Screening) Act (*Wet bevordering integriteitsbeoordelingen door het openbaar bestuur*, Wet BIBOB) is an effective tool for municipalities to obtain information to prevent the unintended facilitation of criminality by the local authority. The goal is a broader, clearer, and more selective use of the BIBOB Act.

Combating the financing of terrorism

122. Since the attacks in the United States on September 11, 2001 terrorism has been in the spotlight. They were followed by attacks on March 11, 2004 in Madrid and on July 7, 2005 in London. The Netherlands too experienced a terrorist attack when Dutch filmmaker and writer Theo van Gogh was murdered on November 2, 2004. In the Netherlands, the NCTb is responsible for ensuring cooperation between the national and international levels.

123. The combat of TF is organized centrally and locally. The central authorities responsible for terrorism in a broad sense, including TF, are the National Prosecution Service (*Landelijk Parket*, LP). Within the LP there are two specialized public prosecutors responsible for all terrorism cases investigated by the National Crime Squad (*Dienst Nationale Recherche*, (DNR)). These prosecutors link intelligence services and operational agencies. Within the DNR there is a specialized unit for investigations on terrorism.

124. Besides the LP, which focuses on combating (international) organized crime, there is also the National Public Prosecutor's Office for financial, economic, and environmental offenses (*Functioneel Parket*, FP) where the national public prosecutor on ML is stationed. This public prosecutor is directly linked to FIU-NL. Suspicious Transaction Reports (*Verdachte transacties*, STRs) concerning TF are therefore under supervision of the national public prosecutor on ML. The FIOD-ECD is the Specialized Investigation Division (*Bijzondere Opsporingsdienst*, BOD) linked to the FP. This means that every case on TF will be investigated by the FIOD-ECD. The DNR and the FIOD-ECD work closely together and, if necessary, the two agencies exchange personnel to efficiently use certain specialized knowledge. Besides the centralized organization of investigations concerning TF, every police region can initiate TF cases. If the case appears to be too complicated it can be transferred to the DNR.

125. The Counter Terrorism Infobox (CT-Infobox) is a new development in the fight against (the financing of) terrorism. It is a formalized partnership of the AIVD, the Immigration and Naturalization Service (IND), the National Police Services Agency (KLPD), the Military Intelligence and Security Service (MIVD), the Public Prosecution Service (OM), the FIOD-ECD and FIU-NL, with the AIVD as lead agency. Its objective is to combat terrorism by centrally compiling and comparing information. This concerns people and networks involved in some way with terrorism, particularly Islamist violence, and associated radicalization.

Tackling abuse and manipulation of real estate

126. On March 25, 2009, the National Steering Group for Combating Real Estate Fraud was established by the Decree establishing National Steering Group for Combating Real Estate Fraud. To carry out the action plan prepared by the National Steering Group, a Working Group for Combating Real Estate Fraud was established.

127. The Dutch government has identified the notary profession as a high-risk profession. Notaries are often involved in real estate transactions and are able to provide access to the international financial system and, knowingly or not, can also facilitate concealment of the true origin of funds. They may act as gatekeepers: their professional roles often involve them in a range of tasks that place them in an ideal position to detect signs of money laundering or terrorist financing.

128. Notaries are obligated to report unusual transactions to FIU-NL and to perform CDD. The Bureau of Financial Investigation (*Bureau Financieel Toezicht*, BFT) monitors the compliance of these obligations and has successfully implemented a policy that strongly involves the sector itself. The Royal Notarial Professional Organization (*Koninklijke Notariële Beroepsorganistie*, KNB) carries out its own investigations while requesting its members to provide a statement by which they declare in what way they have shaped their responsibilities. The authorities indicate that over the past five years there has been an increase have shown a steady increase in the number of reports by notaries.

Cooperation within the Financial Expertise Center (*Financieel Expertise Centrum*, FEC)

129. The FEC is a cooperative effort between various supervisory, investigative and enforcement agencies.[43] The FEC comprises all the organizations that carry out duties related to the financial sector: supervisory authorities; control, intelligence, and investigative institutions; and prosecution authorities.

130. For implementing its tasks as information platform, knowledge center and project bureau, the FEC is organized in an FEC Council and an FEC unit. The way the cooperation is designed is laid down in a covenant.

Supervision of legal persons (*Herziening Toezicht Rechtspersonen*, HTR)

131. A legal person is established in the Netherlands by a notarial deed. Before the notarial deed can be executed the founder of the legal person has to request a declaration of no objection. This declaration is provided by the Ministry of Justice (*Justis Office*). Criminal and financial records of company founders and the first managing and supervisory directors and their relatives are checked by the Department of Justice prior to granting the declaration of no objection.

132. On April 1, 2010 the penalty of company director disqualification was introduced in the Dutch Penal Code (*Wetboek van Strafrecht*, WvSr). The instruction of a civil company director's disqualification

43 See http://www.fec-partners.nl/

is in preparation. These penalties are meant for company directors that are guilty of mismanagement or are guilty of the abuse of legal persons for the purpose of money laundering, fraud or other criminal acts.

1.6.2 The institutional framework for combating money laundering and terrorist financing

133. Below is set out a brief description of the roles and responsibilities of the various governmental and non-governmental authorities and organizations.

1.6.2.1 Ministries

Ministry of Finance (*Ministerie van Financiën*)

134. The Ministry of Finance is responsible for financial supervision legislation and tax legislation. Within the Financial Markets Directorate, a specific Integrity Unit is responsible for AML/CFT policymaking, legislation (WWFT) and FATF-coordination.[44] AML/CFT policy is a joint responsibility with the Ministry of Justice.

Ministry of Justice (*Ministerie van Justitie*)

135. The Ministry of Justice is responsible for legislation in the following areas: i) civil law and procedure, ii) criminal law and procedure, iii) administrative law and procedure, and iv) constitutional law.[45] The Ministry liaises with other government departments and relevant parties when drafting legislation in these areas. Laws are drafted in consultation with the Dutch Upper and Lower Houses, after being reviewed by the Council of State. The Ministry also negotiates on numerous international regulations in the European Union and the United Nations. The national criminal investigation department is responsible for tackling serious and organized crime at the national level.

Ministry of the Interior and Kingdom Relations (*Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*)

136. At the central government level, the Minister of Interior and Kingdom Relations is responsible for overseeing the 25 regional police forces and is directly responsible for managing the National Police Services Agency (*Korps Landelijke Politiediensten*, KLPD).[46] Organizationally, FIU-NL is part of the KLPD. Within the KLPD, FIU-NL is positioned in the National Criminal Intelligence Department (IPOL).

Ministry of Foreign Affairs (*Ministerie van Buitenlandse Zaken*)[47]

137. The Sanctions Act 1977 gives the Minister of Foreign Affairs the power to create regulations to meet international obligations regarding international sanctions. On this basis a sanction regulation on terrorism was created by the Minister of Foreign Affairs in 2002.

National Coordinator for Counterterrorism (*Nationaal Coördinator Terrorismebestrijding*, NCTb)

138. The National Coordinator for Counterterrorism has been established to improve cooperation between all agencies in the Netherlands involved in combating terrorism.[48] The office of the NCTb and its staff fall under the responsibility of two ministers: the Minister of Justice (the lead minister for

44 See http://www.minfin.nl/english/Subjects/Financial_markets
45 See http://english.justitie.nl
46 See http://minbzk.nl/english
47 See http:///minbuza/nl/en
48 See http://english.nctb.nl/

counterterrorism) and the Minister of the Interior and Kingdom Relations. The NCTb is responsible for policy development, analysis of intelligence and other information and coordination of antiterrorism security measures.

1.6.2.2 Public Prosecution Service (Openbaar Ministerie, OM)

General

139. The Public Prosecution Service is one of the main parties involved in dealing with criminal cases.[49] It decides whether or not to prosecute, and how to deal with certain categories of crime without going to court. Within the Public Prosecution Service there are several specialized sections:

National Office of the Public Prosecution Service (*Landelijk Parket*, LP)

140. The Public Prosecution Service had a specialized section that deals with organized crime, called the *Landelijk Parket* (LP). The LP gives direction on criminal investigations of the National Crime Squad (*Dienst Nationale Recherche*, DNR).

National Public Prosecutor's Office for financial, economic and environmental offences (*Functioneel Parket*, FP*)*

141. The Public Prosecution Service has a specialized section that deals with crime concerning the environment, the economy and fraud called the *Functioneel Parket* (FP) This section of the prosecution service is active in those cases that are initiated by special investigative divisions. For financial crimes this entails that the FP is responsible for handling cases that are initiated by the FIOD-ECD.

Public Prosecution Service Proceeds of Crime Bureau (*Bureau Ontnemingswetgeving Openbaar Ministerie*, BOOM)

142. BOOM is the specialized confiscation agency of the Public Prosecution Service in the Netherlands. BOOM operates only in larger, more complex confiscation cases (exceeding one hundred thousand Euros). Other, "regular", confiscation in criminal cases is handled by the Public Prosecution Service. BOOM's task is to confiscate criminal gains. Confiscation can be initiated by prosecution authorities at the start of an investigation. Besides BOOM's primary mission of confiscation of criminal gains, it also cooperates with relevant partners such as: police (domestically as well as foreign police services) and other sections of the prosecution authority. Internationally, BOOM cooperates with EUROPOL, EUROJUST, and CARIN. Finally, BOOM has been given the status of "contact point" for foreign LEAs.

1.6.2.3 Operational agencies

Operational agencies with focus on AML/CFT

Financial Intelligence Unit-The Netherlands (*FIU-Nederland*, FIU-NL)

143. FIU-NL is the national center for receiving, requesting, analyzing, and disseminating disclosures of STRs and other relevant information concerning suspected ML or TF activities. Since 2006, the FIU-NL exists as a hybrid organization, partly administrative and partly law enforcement. In 2006, the Office for the Disclosure of Unusual Transactions (MOT) was transferred, together with the law enforcement unit specialized in AML cases (BLOM) in the Ministry of Interior. As a hybrid organization, FIU-NL comes

49 See http://www.om.nl/vast_menu_blok/english/

under the responsibility of Ministry of Justice and the Ministry of Finance (for policy) and of the Ministry of Interior (administration and management).

144. FIU-NL now has a staff of 56 individuals. They are divided into an administrative unit (the MOT), a law enforcement section (the BLOM), and a facilitation unit. FIU-NL acts as a buffer between the financial institutions/reporting entities and investigating authorities. It receives Unusual Transactions Reports (UTRs). The UTRs are analyzed/investigated and transformed into Suspicious Transaction Report (STRs). The head of FIU-NL is ultimately responsible for determining which UTRs should be transformed into STRs. The STRs are loaded (disseminated) into a special database (IVT), to which authorized law enforcement authorities have access to. FIU-NL is placed within the National Police Services Agency (KLPD). Its tasks are both in the field of AML and CFT.

Fiscal Intelligence and Investigation Service—Economic Investigation Service (*Fiscale Inlichtingen- en Opsporingsdienst—Economische Controledienst*, FIOD-ECD)

145. The FIOD-ECD is a subdivision of the Tax and Customs Administration. If the Tax and Customs Administration suspects fraud, the matter is referred to the FIOD-ECD. The FIOD-ECD then assesses whether fraud is indeed being committed. In consultation with the Public Prosecution Service it may decide to start a criminal investigation. In the case of fiscal fraud the public prosecutor may also opt for a penal settlement or an administrative settlement instead of going to court.

146. The FIOD-ECD also performs supervisory activities in the area of economic planning, financial integrity and movement of goods. This involves matters such as bankruptcy fraud, anti-laundering legislation and the Health Care Charges Act (*Wet tarieven gezondheidszorg*). In addition, the FIOD-ECD contributes to the fight against organized crime and terrorism by mapping out money flows of criminal and terrorist organizations.

National Police Services Agency (*Korps Landelijke Politiediensten*, KLPD)

147. The Netherlands has a single police organization divided into twenty-five regions and one National Police Services Agency (KLPD) with various supporting divisions. A regional police force is responsible for policing in a given area known as the police region.

National Crime Squad (*Dienst Nationale Recherche*, DNR):

148. The DNR, which is organizationally located within the KLPD, is responsible for the combating of (inter)national organized crime and serious crime. Investigation, the development of expertise and (inter)national information exchange is part of the National Crime Squad's work. All investigations that are carried out by the National Crime Squad are executed under authority of the national office of the public prosecutor.

National Criminal Intelligence Department (IPOL)

149. The National Criminal Intelligence Department (IPOL), which is organizationally located within the KLPD, receives, modifies and analyses information and shares this and makes this available to investigating police agencies. IPOL has a crucial strategic role in law enforcement and public order and safety.

Bureau of Financial Investigation (*Bureau Financieel Economische Recherche*, BFER)

150. Within the Police Region's criminal intelligence divisions there are financial investigation experts. There are also special divisions. Police regions may employ accountants and various kinds of

experts. The focus of BFER is on real estate, internal bank fraud, confiscation and facilitators. BFER is mainly composed of tactical investigators, next to experts like financial experts, accountants and lawyers.

Other relevant operational agencies

Netherlands Tax and Customs Administration (*Belastingdienst*)

151. The more than 30 000 staff members of the Dutch Tax and Customs Administration are responsible for a wide range of activities and are part of the Ministry of Finance. Part of their work includes fraud detection and the supervision of the import, export, and transit of goods.

General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst,* AIVD)

152. The AIVD safeguards the national security of the Netherlands by identifying threats, political developments and risks which are not immediately apparent. To this end, it conducts investigations both inside and outside the country. Where necessary, the AIVD shares information so that partners and other interested parties can take appropriate measures. The AIVD operates under the responsibility of the Ministry of the Interior and Kingdom Relations.[50]

Royal Netherlands Military Constabulary (*Koninklijke Marechaussee,* KMAR)

153. The KMAR falls under the Ministry of Defense, however, it performs most of its policing tasks under the responsibility of other ministries, principally Justice and the Interior. The Military Constabulary is divided into six districts in the Netherlands. It also operates abroad, protecting embassies and other buildings and accompanying Dutch service personnel on peace missions. The Military Constabulary is a police force operating in both military and civilian spheres. It serves as a police force for the Navy, Army, and Air Force. It also performs police and security tasks at Dutch airports, where it combats drug smuggling together with the fiscal investigation services. In addition, it is sometimes deployed to help civilian police forces maintain public order (for instance in riot squads) and to investigate offences. The Military Constabulary is responsible for guarding members of the Royal House and the Prime Minister's official residence. It also escorts armored transports for DNB.

Intelligence and Investigation Service of the Ministry of Social Affairs and Employment *(Sociale Inlichtingen- en Opsporingsdienst,* SIOD)

154. The SIOD was established in 2002 to uphold the rules and regulations of the Ministry of Social Affairs and Employment (SZW) through criminal investigations. The domain of the SIOD concerns in principle all legislation of the Ministry of Social Affairs and Employment. This mainly concerns subjects in the fields of employee insurance schemes, social assistance, (benefits and getting people back to work) and the labor market (employment of illegal aliens, temporary work agencies and labor market subsidies). However, other types of SZW-subjects such as labor conditions also fall under the remit of the SIOD.[51]

Intelligence and Tracking Service of the Inspectorate of the Ministry of Housing, Spatial Planning and the Environment (*Inlichtingen- en Opsporingsdienst van de Inspectie van het Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer,* VROM-IOD)

155. A special unit within VROM-Inspectorate, called *VROM-IOD*, deal with criminal investigation. Often it concerns organized crime in relation to international (financial) vehicles and trade. VROM-IOD

50 See http://www.aivd.nl/english/
51 See http://www.siod.nl/content/view/22/42/

investigation teams are formed by investigators and technicians supported by lawyers and accountants. Investigation teams are supervised by the public prosecutor, who is responsible for the investigation.

National Police Internal Investigation Department (*Rijksrecherche*)

156. In the context of repression of fraud and corruption affecting integrity of government or public administration, the *Rijksrecherche* serves as a separate criminal investigation service although it might cooperate with other criminal investigation services. Its focus is on the Dutch police, the national, regional and local governing bodies and the public administration. The *Rijksrecherche* can be deployed to investigate those cases where crimes committed by public officials seriously threaten integrity of government or public administration. It investigates such cases if they should not or could not be dealt with by regular police. *Rijksrecherche* has its own criminal intelligence service which can also act on anonymous reports.

***Justis* Office (*Justis*)**

157. *Justis* is a special service related to the ministry of Justice responsible for screening on integrity. Government, for example local governments, can request for background information on companies and persons before giving out permits or financial support. This task is based on the Public Administration (Probity Screening) Act (*Wet bevordering integriteitsbeoordelingen door het openbaar bestuur*, Wet BIBOB), mentioned above. *Justis* advices the requesting (local) government and they decide whether or not to follow the advice. *Justis* is also involved in the preventative supervision on companies. Establishers of companies in the Netherlands need a declaration of no objection (*Verklaring van geen bezwaar*, VVGB) from the Ministry of Justice. The VVGB is requested trough a notary by *Justis*. *Justis* screens the financial and criminal history and the intent of the company. On this base the requested VVGB will be issued or denied.

1.6.2.4 Supervisory authorities

Dutch Central Bank (*De Nederlandsche Bank*, DNB)

158. DNB is the central bank and the prudential and integrity supervisor for banks and other (financial) institutions in accordance with the Wft, WWFT, Wgt, Wtt, the Pension Act and the Sanctions Act.[52] DNB supervises compliance with AML/CFT legislation and regulation of a range of institutions: banks, life insurance companies, bureaux de change, payment institutions (*e.g.*, money transfer offices, creditcard companies), trust and company services providers and casinos.

The Netherlands Authority for the Financial Markets (*Autoriteit Financiële Markten*, AFM)

159. The AFM is responsible for supervising the operation of the financial markets. This means that AFM supervises the conduct of the entire financial market sector: savings, investment, insurance and loans.[53]

Bureau Financial Supervision (*Bureau Financieel Toezicht*, BFT)

160. The BFT is responsible for the supervision in connection with legislation on the prevention of ML and TF of lawyers, (junior) civil-law notaries, independent legal advisers, public chartered accountants, public accountant-business administration consultants, tax advisors and other independent

52 See http://www.dnb.nl/en/home/index.jsp
53 See http://www.afm.nl/en.aspx

finance economic advisers.[54] The BFT is also responsible for financial supervision of civil-law notaries and court bailiffs.

Netherlands Tax and Customs Administration, Holland-Midden, Unit MOT (*Belastingdienst Holland-Midden, Unit MOT*, BHM)

161. BHM is responsible for the supervision in connection with legislation on the prevention of money laundering and financing of terrorism regarding the sale (or the provision of intermediary services) of vehicles, ships, works of art, antiques, precious stones, precious metals, and jewelry. In addition, BHM is the authority responsible for the AML/CFT supervision regarding real estate brokers.

1.6.2.5 Cooperation between agencies

Financial Expertise Center (*Financieel Expertise Centrum*, FEC)

162. The FEC was established in 1998 to enhance the integrity of the financial sector. The Financial Markets Director of the Ministry of Finance and the Law Enforcement Director of the Ministry of Justice attend FEC Council meetings as observers.

National Steering Group for Combating Real Estate Fraud (*Regiegroep Aanpak Misbruik Vastgoed*)

163. On March 25, 2009 the National Steering Group for Combating Real Estate Fraud was established. This Steering Group is one of the measures from the government's strategy to pursue a coherent strategy to fundamentally tackle abuse of and manipulation with real estate (see *supra:* under subtitle "Tackling abuse and manipulation of real estate"). The Steering Group will be jointly chaired by the ministries of Justice and Finance. A Working Group for Combating Real Estate Fraud is established by the National Steering Group.

Committee on ML and TF (*Commissie Witwassen en Terrorismefinanciering*, BC MOT)

164. It was established when WMOT came into being. Under the WWFT, which entered into force on August 1, 2008, the committee is given a slightly modified mandate, which is more in line with its composition and its role in practice. The principal task of the new Committee will no longer be to monitor FIU-NL but to act as a discussion partner for the responsible Ministries as regards the functioning of the duty to disclose in practice and the determination of the indicators.

Task forces

165. In 2007, the Dutch government launched a new program of action to intensify the combat of (international) organized crime. Two main priorities in this program are 'human trafficking' and 'organized crime related to large scale cannabis cultivation.'

1.6.3 Approach concerning risk

1.6.3.1 National Threat Assessments

166. Every four years Dutch law enforcement agencies prepare a National Threat Assessment on serious and organized crime (*Nationaal Dreigingsbeeld zware en georganiseerde misdaad*) to identify and gauge the scale of the threats posed to the Netherlands by serious and organised crime, including money laundering.

54 See http://www.bureauft.nl/

167. The National Coordinator for Counterterrorism (*Nationaal Coördinator Terrorismebestrijding*, NCTb) prepares four times a year a Terrorist Threat Assessment (*Dreigingsbeeld Terrorisme Nederland*, DTN). This Assessment is a broad analysis of the threat posed by national and international terrorism, including terrorist financing, to the Netherlands and Dutch interests abroad. It is intended for use by senior civil servants, members of government and policymakers.

168. In 2009 the Ministry of Finance organised three workshops as a first step in conducting a national threat assessment on money laundering. Based on the output of these, the Financial Expertise Centre (*Financieel Expertise Centrum*, FEC) was tasked to work on a National Threat Assessment Money Laundering (National Threat Assessment (NTA) *Witwassen*).The FEC is a cooperative effort between various supervisory, investigative and enforcement agencies, working together on a policy as well as operational level. The FEC comprises all the organizations that carry out duties related to the financial sector: supervisory authorities; control, intelligence, and investigative agencies; and prosecution authorities. The national threat assessment is expected to be finalized in early 2011.

1.6.3.2 Implementing EU-legislation and the risk-based approach

169. The Act implementing the Third Money Laundering Directive (the WWFT) takes a "principle-based" approach. This means that the Act prescribes the result to be produced by the customer due diligence review, not the manner in which the review must be carried out.

170. By implementing the Third Money Laundering Directive in national legislation (WWFT), the risk-based approach was introduced. Institutions can tailor their CDD measures to the specificities of their organization as long as the outcome is as required by the WWFT. The approach means that institutions make their own assessment of the risks entailed by particular customers, transactions or products, and it also enables the institutions to bring the efforts and resources required for the customer due diligence in line with these risks. As a result, more attention can be devoted to monitoring accounts and transactions that represent an increased risk of money laundering or terrorist financing. With regard to customers, transactions or products that entail a lower risk less intensive monitoring will suffice.

1.6.3.3. Supervision

171. The supervisor can assess for each individual institution whether an institution has adequately identified the level of risk of customers, transactions and products and has developed adequate procedures and measures concerning customer due diligence to curtail these risks.

172. The supervisory authorities also apply a risk-based approach in the exercise of their supervisory function.

1.6.4 Progress since the last mutual evaluation or assessment

173. In September 2004, the IMF produced a Report on the Observance of Standards and Codes (ROSC). Recommendations were made. The authorities' view on the follow-up given to these recommendations is set out below.

a) Ensuring there is effective sharing of information by MOT (FIU) with supervisory authorities.

174. On a regular basis, supervisors and FIU-NL meet with each other to discuss issues regarding the reporting requirements.

b) Make confiscation of criminal proceeds for ML/TF mandatory.

175. A general instruction of the Public Prosecution Service (*Aanwijzing ontneming*) urges all prosecutors to investigate and seize criminal proceeds in case of an intended required fine of at least EUR500 or criminal proceeds estimated at the moment of seizure to amount to EUR500. However, confiscation measures under Dutch law remain in the discretion of the judge.

c) Address a requirement that there be renewal of identity documents if in the course of a business relationship doubts occur regarding the identity of a client.

176. Article 3 (3) (d) WWFT requires financial institutions to perform customer due diligence when they doubt the reliability of information obtained earlier from the customer. Additionally, Article 3 (2) (d) WWFT requires an institution to carry out, where possible, constant monitoring of the business relationship and the transactions conducted during the existence of the relationship.

d) Incorporate specific recordkeeping requirements for account relationship materials (post account opening) and transaction records as authorities adopt revisions to ISA/DUTA.

177. In the Netherlands it is mandatory to maintain all business records for at least 7 years. This general obligation is set out in Article 2:10 (3) of the BW and Article 52 of the General Tax Code (*Algemene wet inzake Rijksbelastingen*, AWR). With regard to the data that is provided to FIU-NL in the context of an unusual transaction report (Article 16 (2) WWFT), Article 34 WWFT requires that financial institutions retain this data in an accessible manner for five years following the moment when the report was filed. The data collected by financial institutions for CDD purposes, should be maintained in an accessible manner for five years (Article 33 (2) WWFT). In addition, the Wft requires that financial institutions store their CDD documentation for 5 years (Articles 14 (5) BPR Wft, Article 19 BPR Wft, Article 21 (5) BGFO Wft and Article 26 (4) BGFO Wft).

e) DNB should provide more specific guidance to licensees on measures that should be adopted to minimize the risk inherent in dealing with bearer shares.

178. The Netherlands has started a process in which bearer shares will be ultimately dematerialized. The first phase was mobilization and the second phase centralization; a central depository was set up for bearer securities. The third phase is the dematerialization phase, which will be completed by January 1, 2013. As of the time of the assessment mission, however, Dutch law still allowed for the issuance of new and the unregulated transfer of existing bearer shares.

179. The last few years, frequent use has already been made of the global note; this is a share issue with the decision of the shareholders meeting and closing figures for the issued share capital on one A4. The global note and the central share issue account at the depository institution Necigef (central securities depository) is conclusive. Banks are the first line of defense and they use the RIS List. The Dutch RIS List is the summary list of all the reports drawn up by the police with regard to stolen or missing bearer securities previously known as the “summary list of the investigation list issued by the police related to stolen or lost securities.” The objective of this RIS list is to administrate centrally the registration of stolen or lost physical bearer securities.

180. Figures published by DNB show that the number of banks with a deposit desk, which is needed to exchange physical certificates, has decreased drastically. The last large institutions that still use physical certificates will phase it out by January 1, 2013, as required by new legislation. This date runs in parallel with the closure of the transition phase in neighboring Belgium so that any shortcut, should it exist, will be made impossible.

f) Introduce an explicit requirement for internal procedures regarding ongoing training, and amend laws/regulations to create an internal audit function for any sector for which it is not explicit.

181. Articles 3:10, 3:17, 4:11 and 4:14 Wft require financial institutions to maintain internal procedures, policies and controls to mitigate integrity risks (including the risk of money laundering and terrorist financing). Further detailed requirements based on these Articles are compulsory under the BPR Wft and the BGFO Wft. Article 35 WWFT requires financial institutions to train their staff regarding these internal controls, procedures and policies. Regarding bureaux de change, the Wgt and the Wgt regulations on the conduct of business by and the Administrative organization apply.

g) Amend laws/regulations to require management level compliance officers.

182. Article 21 BPR Wft and Article 31c BGFO Wft require financial institutions to have an independent compliance function.

h) Expand scope of tipping off prohibition to cover those who come into contact with information regarding the reporting or consideration of a decision to report.

183. Financial institutions, their directors, officers and employees are prohibited by law to disclose ("tipping off") the fact that a UTR or related information is being reported or provided to FIU-NL, as stated in Article 23 (1) WWFT. Breach of this secrecy is an economic offense and will be punished according the WED.

i) Ensure in all sectors that institutions are required to maintain records of transactions considered for reporting but not reported and that these records are available for supervisory review.

184. See answer under Recommendation 4. Both Articles 33 (2) WWFT and Article 34 WWFT require that the data is kept in an accessible manner. According to Article 5:17 General Administrative law Act (*Algemene wet bestuursrecht*, Awb) supervisors have unrestricted access to all records maintained by entities under their supervision.

j) Extend integrity testing by supervisors in practice to a wider range of senior management outside of the Executive Board.

185. See next point.

k) Rectify the deficiency identified in the role played by the central organization of the cooperative bank in undertaking fit and proper examinations.

186. Articles 3:8 Wft, 3:9 Wft, 4:9 Wft, 4:10 Wft, 13 BPR Wft, 20 BGFO Wft and 25 BGFO Wft deal with the standards of hiring employees by financial institutions. DNB and AFM are responsible for this fit and proper testing. In this respect DNB and AFM gather information from the Public Prosecution Service, the Tax and Customs Administration, foreign (supervisory) authorities, professional organizations and their own databases. Also public sources are consulted like Graydon, the Chamber of commerce, LexisNexis and the Internet.

l) Within the two-year period referred to by FATF, amend relevant laws to require that accurate and meaningful originator information (name, address and account number) on fund transfers remains with the transfer throughout the payment chain.

187. The Netherlands is bound by "Regulation (EC) No. 1781/2006 of the European Parliament and of the Council of November 15, 2006 on information on the payer accompanying transfers," in force since January 1, 2007. This instrument is directly applicable in the Netherlands.

m) Impose an obligation, consistent with SR VII, on FSPs to give enhanced scrutiny to wire transfers that do not contain complete originator information and provide guidance that encourages compliance on an immediate basis.

188. This was covered by Articles 8, 9, and 10 of the EU Regulation.

n) The direction given to financial institutions in respect of their dealings with non-profit organizations should be expanded.

189. Guidance to financial institutions is given in a broader sense. See for example the Q & A's with respect to the WWFT.[55] Due to the risk-based approach, financial institutions have to perform their own risk assessment of the customer, transaction or product.

o) The working group on non-profits in the Netherlands should come up with reasonable measures to improve the transparency and monitoring of foundations and associations in general as well as with measures to improve the registration, regulation and monitoring of charities.

190. All non-profit organizations with legal personality, such as foundations and associations, have to register at the Chamber of Commerce. The BW entrusts the Public Prosecution Service with the supervision of foundations.

191. In 2008, the Tax and Customs Administration introduced a form of preventive fiscal supervision of charities. When an organization wants to make use of certain advantageous fiscal arrangements set up for charities and other non-profit organizations (jointly referred to as *Algemeen Nut Beogende Instellingen*, ANBIs) it has to request a judicial order from the Tax and Customs Administration. This order will only be provided if the ANBI meets a number of criteria, including a policy plan that sets out scheduled activities, ways of fundraising and planned expenditures. The ANBI is also obligated to provide a full overview of its financial administration, including all revenues on a yearly basis.

192. In addition to these legal measures, the CBF, which is a privately-run organization, provides a seal of approval to fundraising institutions which have issued a request on a voluntary basis. Supervision by the CBF is based mainly on annual reports and accounting declarations provided by the institutions themselves, along with investigations carried out by the CBF itself.

55 See http://www.dnb.nl/openboek/extern/id/en/all/41-197640.html and http://www.dnb.nl/openboek/extern/id/en/all/41-197640.html?xsl=/stylesheets/publication/OBfaqOverzicht.xsl

2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1 Criminalization of Money Laundering (R.1 & 2)

2.1.1 Description and Analysis

Legal Framework:

193. The Netherlands have criminalized ML through Articles 420 bis, 420 ter, and 420 quater *Wetboek van Strafrecht* (Penal Code). The provisions in their current form were first adopted in 2001. Prior to 2001, ML was investigated and prosecuted on the basis of the "receiving of stolen goods" (*Heling*) offense.

194. The statutory provisions as indicated above are further supported by a significant number of court decisions, including Supreme Court rulings, which provide guidance on how to interpret and correctly apply the ML provisions.

195. The Netherlands have ratified the Palermo Convention on May 26, 2004 and the Vienna Convention on September 9, 1993.

Criminalization of Money Laundering (c. 1.1—Physical and Material Elements of the Offense):

196. Articles 420 bis and 420 quater of the Penal Code criminalize (1) the concealing or disguising of the true nature, source, location, disposition or movement of an object, or of the person who has title to or possession of the object and (2) the acquisition, possession, transfer, conversion or use of an object if the offender either knows or may reasonably suspect that objects stem directly or indirectly from a criminal offense. In addition, Article 420 ter of the Penal Code sets out that the habitual commission of money laundering offenses under Articles 420 bis and 420 quater constitutes aggravating circumstances.

197. The ML offenses under Dutch law address all material elements of the offenses as defined in the Palermo and Vienna Conventions. The "conversion or transfer", the "concealment or disguise of the nature, source, location, disposition, movement or rights and ownership" and the "acquisition, possession and use" are all explicitly covered. Dutch law also does not require proof of a specific purpose in committing any of the above mentioned acts.

198. With respect to the offense of "possession," the Supreme Court in a judgment of October 2, 2007 (NJ 2008, 16) held that merely being in possession of money that has been obtained by the suspect through the commission of a predicate offense constitutes money laundering pursuant to Article 420 bis (2) of the Penal Code. In some countries, the principle of double jeopardy bars the authorities from prosecuting for both the predicate offense and the money laundering offense, in a scenario where the perpetrator engages merely in possession of his criminal proceeds. There is no such barrier in the Netherlands and in such scenarios the Dutch authorities can prosecute the same individual for both the predicate offense and for money laundering.

The Laundered Property (c. 1.2):

199. The ML offenses under Articles 420 bis and 420 quater both refer to "objects" that directly or indirectly stem from a criminal offense, whereby both provisions stipulate that the term would include "any good and property right." "Property right" is defined in Article 6 of Book 3 of the Civil Code to cover all "rights that are, either individual or as part of another right, transferable or provide the one who is eligible [to them] with material benefits or are received in exchange for supplied or promised material remuneration". The term "goods" is defined in Article 2 of Book 3 to extend to all "material objects susceptible for human control."

200. In discussions with the authorities, it was stated that the term "objects" would include everything of value, including but not limited to money, real estate and any other property. To support this view, the authorities provided a ruling of the Amsterdam Appeals Court (*Hof Amsterdam July 3, 2009, LJN: BJ1646, zaak Holleeder*), in which the court considered cash, bank accounts, apartment rights, real estate and company premises to constitute "objects that directly or indirectly stem from a criminal offense."

201. Based on the broad language of Articles 2 and 6 of Book 3 of the Civil Code and the cited case law, the assessors conclude that the Dutch ML provisions are applicable to assets of any kind, whether corporeal or incorporeal, moveable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets, and are thus in compliance with the FATF standard on this point.

Proving Property is the Proceeds of Crime (c. 1.2.1):

202. Articles 420 bis and Article 420 quater of the Penal Code do not require that a person be convicted of a predicate offense for the prosecution to establish the illicit origin of proceeds. The authorities confirmed that ML is an autonomous offense under Dutch law and may be prosecuted independently from the predicate offense.

203. This view has also been taken by the Supreme Court in a ruling of September 28, 2004 (*NJ 2007, 278*), where the court clarified that it is not necessary to prove that funds or property is proceeds of a specific criminal offense but that it would be sufficient to establish that objects "must have been derived from criminal activity."

204. In the specific case referenced above, the Supreme Court upheld the ML conviction based on the conclusion that "the existence and origin of the money were to remain concealed" and thus "the possibility that the money might have been obtained legally [is] so improbable that it [can be] assume[d] that the money was derived from a criminal activity."

205. In another ruling of September 27, 2005 (*NJ 2006, 473*), the court stated that "the circumstances of the actual case in question will have to convince the court that a transaction with the outward appearance of a money laundering construction [is in fact a transaction carried out for ML purposes]" whereby it is not necessary to "identify the precise offense from which the property originated" or to show that the entire funds or assets stem from a criminal activity. Funds or assets that only partially represent proceeds of crime and partially stem from licit sources are thus still considered proceeds of crime in their entirety.

206. In sum, Dutch law merely requires the prosecution to establish that objects are likely to be direct or indirect proceeds of crime, without the need to specify the predicate offense.

The Scope of the Predicate Offenses (c. 1.3):

207. Articles 420 bis and 420 quater of the Penal Code apply to proceeds from any criminal offense.

208. The Dutch Penal Code differentiates between "offenses" and "misdemeanours." "Offenses" are listed in Book II (Articles 92 to 420 quinquies) and "misdemeanours" are set out in Book III (Articles 424 to 476) of the Penal Code. As a general rule, the maximum available sanction for misdemeanours is imprisonment for up to six months whereas the maximum sanction available for offenses ranges between imprisonment for six months to imprisonment for life.

209. The table below establishes how each FATF designated category of predicate offenses is criminalized under Dutch law. All listed provisions constitute offenses as they are either set out in Book II of the Penal Code or in a separate statute but are punishable with imprisonment for six months or more.

Predicate Offense	**Dutch Criminal Provisions**
Participation in an organized criminal group and racketeering	Articles 140 Penal Code (WvSr)
Terrorism, including terrorism financing	Articles 46 (in combination with any terrorist offence), 92-96, 108 par 2, 114a-114b, 115 par 2, 117 par 2, 120a-120b, 121-122, 130a, 157 sub 3, 161quater sub 2, 164 par 2, 166 sub 3, 168 sub 2, 170 sub 3, 174 par 2, 176a-176b, 282c, 288a, 289a, -304a 304b, 415a-415b Penal Code; Articles 79, 80 par 2-3, Nuclear Energy Act; Article 33b Act on the Use of Explosives for Civilian Purposes ; Article 6 par 4, Economic Offences Act ; Article 55 par 5, Act on Weapons and Ammunition .
Trafficking in human beings and migrant smuggling	Articles 197a and 273F Penal Code
Sexual exploitation, including sexual exploitation of children	Article 273f Penal Code
Illicit trafficking in narcotic drugs and psychotropic substances	Articles 2-3, 10-13 Act on Illegal Substances
Illicit arms trafficking	Articles 14(1) and 55 Firearms, Ammunition and Offensive Weapons Act
Illicit trafficking in stolen and other goods	Articles 416, 417 and 417 bis Penal Code
Corruption and bribery	Articles 177-178a, and 362-364a Penal Code
Fraud	Articles 225, 326, and 323a Penal Code
Counterfeiting Currency	Articles 208-214 Penal Code
Counterfeiting and piracy of products	Article 337 Penal Code
Environmental crime	Article 1a Economic Offences Act
Murder, grievous bodily injury	Articles 287-291 and, 302-303 Penal Code
Kidnapping, illegal restraining and hostage-taking	Articles 278-282c Penal Code
Robbery or theft	Articles 310-312, 317-318 Penal Code
Smuggling	Articles 10:1-10:4 General Customs Act
Extortion	Articles 317 and 326-326a Penal Code
Forgery	Articles 216-234 Penal Code
Piracy	Articles 381-385a Penal Code
Insider trading and market manipulation	Articles 5:53-5:58 Financial Supervision Act and Article 1 Economic Offences Act

210. Tax offenses under Articles 68, 69, and 72 of the General Law Concerning National Taxes, including tax evasion, are punishable in the Netherlands with a maximum sentence of imprisonment for four to six years and thus constitute predicate offenses for ML. This was also confirmed by the Supreme Court in a ruling of October 7, 2008 (*NJ 2009, 92*).

Threshold Approach for Predicate Offenses (c. 1.4):

211. The Netherlands follows a threshold approach in defining predicate offenses for ML. Articles 420 bis and 420 quater of the Penal Code are applicable to objects that were obtained through the commission of "a criminal offense" but not to objects that stem from misdemeanours. As indicated above, the maximum sentence for "offenses" ranges between imprisonment for six months to imprisonment for life. "The maximum imprisonment sanction available for misdemeanours generally does not exceed six months."

212. Dutch law is thus in compliance with the FATF standard on this point.

Extraterritorially Committed Predicate Offenses (c. 1.5):

213. Articles 420 bis and 420 quater of the Penal Code do not expressly refer to predicate offenses committed abroad. However, the authorities stated that the reference to "objects that directly or indirectly stem from an offense" would be interpreted to also include objects that have been obtained through criminal conduct committed outside of the Netherlands. This view was also confirmed by the Supreme Court in a ruling of December 1, 1998 (*NJ 1999, 470*), where the court held that the Dutch ML provisions are, at a minimum, applicable to predicate offenses that have been committed abroad if the relevant conduct has been criminalized both under Dutch law and the law of the country in which it took place.

214. Dutch law is thus in compliance with the FATF standard on this point.

Laundering One's Own Illicit Funds (c. 1.6):

215. The language of the Dutch ML provisions seem to include both cases in which a person launders the proceeds of his/her own criminal conduct and cases in which a person launders the proceeds of another person's criminal conduct. This interpretation was confirmed by the Supreme Court in a judgment of October 2, 2007 (*NJ 2008, 16*), where the court confirmed the lower court's decision to convict the appellant for laundering the proceeds of his own criminal conduct.

Ancillary Offenses (c. 1.7):

216. Ancillary offenses are set out in the general provisions of the Penal Code and are applicable to all specific offenses set out in Book II of the Penal Code, including the ML provisions. Article 45 of the Penal Code criminalizes the attempt to commit a criminal offense and provides that the offender may be sanctioned with the maximum penalty available for the attempted offense reduced by one third, or with a term of imprisonment for up to twenty years in cases where the attempted offense is punishable with life imprisonment.

217. Articles 47 and 48 of the Penal Code further criminalize the procuring, assisting, solicitation or aiding and abetting of an offense and stipulate that such conduct may be subject to the same sanction as the main offense.

218. Article 140 Penal Code stipulates that it is a criminal offense for any person to participate in an organization whose aim it is to commit a crime and sanctions such conduct with imprisonment of up to six years or a fine of up to EUR76 000. The term "organization" has been interpreted by the courts to mean "a structured and lasting form of collaboration between two or more persons that is directed at the commission of an offense." A person could thus be held criminally liable for "association to commit" a ML offense under Article 140 of the Penal Code.

219. The outlined provisions set out appropriate ancillary offenses to ML, including attempt, aiding and abetting, facilitating and counseling the commission thereof. In addition, association to commit ML can be prosecuted as "participation in a criminal organization."

Additional Element—If an act overseas which does not constitute an offense overseas, but would be a predicate offense if occurred domestically, lead to an offense of ML (c. 1.8):

220. As indicated under criterion 1.5 above, Articles 420 bis and 420 quater of the Penal Code do not expressly refer to predicate offenses committed abroad. However, the authorities stated that the reference to "any offense" would be interpreted to include conduct within and outside the Netherlands. In line with this argument, the Supreme Court in a ruling of December 1, 1998 (*NJ 1999, 470*) suggested that for the ML provisions to apply it would "probably not be necessary" to establish that conduct committed abroad was criminalized under the law of the foreign jurisdiction so long as the conduct is an offense under Dutch law. However, as under Dutch law it is not necessary to establish exactly which predicate offense has been committed or where a predicate offense has taken place for the ML provisions to apply, the court has not yet had an opportunity to issue a binding ruling on this matter.

Liability of Natural Persons (c. 2.1):

221. As outlined above, Articles 420 bis and 420 quater of the Penal Code require that the perpetrator either knew or may have reasonably suspected (which effectively applies an objective "could have known" test) that objects are the proceeds of crime. Dutch law is thus not only in line but goes beyond the Vienna and Palermo Conventions on this point.

The Mental Element of the ML Offense (c. 2.2):

222. Dutch law does not provide for a statutory provision that would regulate the inference of the mental element from objective factual circumstances. However, with respect to Article 420 bis of the Penal Code, the Supreme Court has confirmed application of this principle in a number of cases *(Hoge Raad September 27, 2005, NJ 2006, 473; Hoge Raad September 28, 2004, NJ 2007, 278).* In particular, the Supreme Court held that the intentional elements of the act of ML (the procuring, concealing, transferring…) can be deduced from the conduct itself and that the criminal origin and knowledge thereof by the main perpetrator can be deduced from the factual circumstances of the case.

Liability of Legal Persons (c. 2.3):

223. Articles 420 bis and 420 quater of the Penal Code apply to "any person" who commits an act of ML. While the provisions do not specify how the term "person" is to be interpreted, Article 51 of the Penal Code establishes that any criminal offense under Dutch law may be committed by a natural or legal person.

224. Legal persons may thus be subject to criminal liability for ML and be sanctioned with penalties and non-punitive orders as appropriate. In cases where a ML offense is committed by a legal person, a fine of up to EUR760 000 may be applied based on Article 23 (7) Penal Code. In addition, a confiscation order may be issued.

225. The authorities stated that while in the past, a number of legal entities have been held criminally liable under Article 420 bis, no bank or other FI has ever been convicted for ML.

Liability of Legal Persons should not preclude possible parallel criminal, civil or administrative proceedings (c. 2.4):

226. Article 51 of the Dutch Penal Code expressly stipulates that holding a legal person criminally liable for a criminal offense does not preclude the possibility of parallel criminal proceedings against the persons who ordered the commission of or controlled the prohibited act.

227. In addition, the authorities stated that it would be possible to initiate criminal proceedings against a legal person concurrently with civil or administrative proceedings. In practice, however, the criminal proceedings would be carried out first and civil and administrative proceedings would be proceeded with only at a later stage.

Sanctions for ML (c. 2.5):

228. Intentional ML pursuant to Article 420 bis is sanctioned with imprisonment for a term of up to four years and/or a fine of up to EUR76 000. If the prosecution is based upon the failure to reasonably suspect that property is the proceeds of crime, Article 420 quater provides for imprisonment for a term of up to one year and/or a fine of up to EUR76 000.

229. Article 420 quater of the Penal Code further stipulates that anybody who commits ML habitually is liable to imprisonment for a term of up to six years or a fine of up to EUR76 000. In addition, for each ML case, a confiscation order or special confiscation order as outlined under Recommendation 3 below may be issued.

230. The general provisions of the Penal Code allow for prison sentences and fines to be accumulated in cases involving a number of isolated criminal offenses, whereby accumulation of prison sentences is limited to $1^{1/3}$ of the highest maximum sanction applicable to any of the offenses involved.

231. In addition to criminal sanctions and to avoid prosecution of a specific case, for conduct liable to a maximum sentence of not more than six years of imprisonment, the public prosecutor's office has the power under Article 74 of the Penal Code to offer payment of a certain amount of money, surrender of property that is liable to confiscation, the payment of the estimated value of these objects and/or the payment of compensation for damages caused by the offense. As indicated in the tables with the total number of prosecutions for ML or ML and another offense below, persons have made use of this possibility in a number of cases, whereby it is unclear what measures or amounts were involved in each case.

232. The sanctions in place for ML seem to be in line with the sanctions applicable to other serious criminal offenses under Dutch law. For example, illicit trafficking in stolen and other goods, basic corruption and basic fraud offenses are sanctioned with imprisonment of up to four years and a fine of up to EUR76 000. Forgery is punishable with imprisonment of up to six years and a fine of up to EUR76 000.

233. The sanctions for basic ML offenses are low when compared to some FATF countries (*i.e.* Argentina=2–10 years imprisonment, Brazil=3–10 years imprisonment, Mexico=5–15 years imprisonment, Italy=4–12 years imprisonment, United States=fine and/or imprisonment up to 20 years or both, United Kingdom=fine, imprisonment up to 14 years or both) but are in line with the sanctions applicable in other FATF countries (*i.e.* Finland=fine or imprisonment up to 2 years, Japan=fine and/or imprisonment up to 5 years).

234. In terms of actual application of the statutory sanctions, between 2004 and 2009 sanctions were imposed in 525 pure ML cases, whereby about 259 or 46 percent of these cases led to a prison sentence. Of these 259 cases, only about 60 or 11 percent resulted in a prison sentence for more than one year. The

authorities indicated that this was due to the fact that some of them were smaller cases involving cash couriers. Of the 525 convictions, six related to legal as opposed to natural persons, whereby the fine imposed in each case was in excess of EUR5 000.

235. Due to privacy reasons, the statistics provided by the authorities do not indicate the exact duration of prison sentences imposed. Also, it is not clear whether any sanctions have been imposed for habitual ML and the extent of those sanctions, if any. Fines were imposed in about 60 cases but the statistics provided by the authorities do not state the exact amounts. The authorities indicated that due to privacy reasons, statistics on sanctions cannot be quantified in greater detail if the number of cases is less than ten.

Sentences for pure ML Offenses					
YEAR	**TOTAL**	**FINE**	**COMMUNITY SERVICE**	**IMPRISONMENT UP TO 1 YEAR**	**IMPRISONMENT MORE THAN 1 YEAR**
2004	20	Less than 10	10	Less than 10	Less than 10
2005	26	Less than 10	13	10	Less than 10
2006	62	Less than 10	29	19	Less than 10
2007	112	Less than 10	50	49	Less than 10
2008	162	14	82	56	Less than 10
2009	164 natural persons and 6 legal persons	15	70	52	13

236. A slightly different trend can be observed in cases where a conviction was obtained for both ML and another offense. While the total percentage of cases that led to a prison sentence seems to be the same as for pure ML cases (about 70 percent), the sentences imposed seem to be slightly more severe. Between 2004 and 2009, 1 757 cases for ML combined with another offense resulted in the application of sanctions. About 1 234 or 70 percent of these cases resulted in a prison sentence. Of the 1 234 cases, 917 or 52 percent led to imprisonment of up to two years and 317 or 18 percent to imprisonment for more than two years. The statistics provided by the authorities do however not indicate the exact duration of the sentences and whether sanctions for habitual ML have ever been imposed. Additionally, fines were imposed in about 102 cases but the exact amounts were not provided due to the already mentioned privacy rules.

Sentences for ML combined with other Offenses						
YEAR	**TOTAL**	**FINE**	**COMMUNITY SERVICE**	**IMPRISONMENT UP TO 1 YEAR**	**IMPRISONMENT 1 TO 2 YEARS**	**IMPRISONMENT MORE THAN 2 YEARS**
2004	108	13	26	22	19	33
2005	156 natural persons and 2 legal persons	16	46	49	23	37
2006	237 natural persons and 3 legal persons	12	58	106	35	38
2007	371 natural persons and 1 legal person	22	95	147	61	77
2008	483	26	150	183	61	82
2009	520 natural persons and 3 legal persons	27	144	210	75	76

237. In the period 2004 to 2009, the majority of convictions for pure or mixed ML have resulted in a prison sentence, whereby it appears that a good number of them resulted in imprisonment for a year or more. In the absence of more detailed information regarding the length of the prison sentences and the amounts of fines imposed, the assessors are not able to determine in full the degree of the effective application of the statutory sanctions regime. Equally, in the absence of information on the types and number of sanctions applied to legal persons, the effective application of the ML provisions to legal persons cannot be fully evaluated.

238. In sum, while a conclusion that the statutory sanctions are fully effective is not possible without more specific information, it is clear that the sanctions regime has been effective to a certain degree in that it has resulted in significant number of prison sentences.

Statistics (R.32):

239. The authorities indicated that the most relevant predicate offenses for money laundering are illicit trafficking of humans, weapons and drugs offenses. General crime statistics that would allow the assessors to draw a conclusion regarding the scale of these offenses or other significant types of proceeds generating predicate offenses committed in the Netherlands were not available. Furthermore, the authorities stated that available information on the predicate offenses involved in ML cases would be limited due to the fact that Dutch law does not require identification of a specific predicate offense for the ML provisions to apply.

240. Furthermore, complete and accurate statistics on the number of criminal investigations carried out for ML were not made available to the assessors. Dutch law requires that all cases investigated be presented to the public prosecutor. It thus seems that the table with the Number of Criminal Investigations in the Netherlands for pure or mixed ML investigations brought to the Public Prosecutor and the table with the Total Number of Cases for ML or ML and another offense brought to the Public Prosecutor by initiating law enforcement authority 2006–2009 below would to some extent be reflective of the number of investigations carried out. However, criminal investigations that were terminated at an early stage and preliminary investigations would not be covered by these tables. In addition, it remains unclear how ML investigations in the Netherlands are triggered, in particular how many of them have been initiated by STRs, and how many investigations were terminated and based on what grounds. It also could not be established in relation to which underlying criminal conduct ML investigations were carried out. While assessors acknowledge that it may be difficult for the Dutch authorities to maintain statistics on the underlying predicate offenses given that the prosecution is not required to establish exactly which offense that generated the property that is laundered, the assessors still consider it important that the authorities collect comprehensive statistics on the general crime categories involved in ML cases.

241. Statistics on the number of prosecutions for ML are maintained by the Ministry of Justice and suggest that a significant number of prosecutions have been obtained for ML since 2004.

242. The table below regarding the Excerpts Crime and Criminal Justice Statistics in the European Union, Crimes recorded by the Dutch Police represents an excerpt from the European Crime and Criminal Justice Statistics. The numbers only pertain to certain types of crimes and do not give a full picture of the types and trends of predicate offenses committed in the Netherlands. The statistics are also slightly outdated as they only cover the years 2004–2006. Statistics were not available for the years 2007-2010 or for any other crimes than those listed in the table below.

Excerpts Crime and Criminal Justice Statistics in the European Union, Crimes recorded by the Dutch Police			
CRIME	**2004**	**2005**	**2006**
Total Crimes	1 319 482	1 255 079	1 218 447
Robbery	17 683	15 463	13 716

Excerpts Crime and Criminal Justice Statistics in the European Union, Crimes recorded by the Dutch Police			
Burglary	95 952	92 890	91 235
Drug Trafficking	15 662	15 305	16 361

243. The table below with the Number of Criminal Investigations in the Netherlands for pure or mixed ML investigations brought to the Public Prosecutor and the one further below with the Total Number of Cases for ML or ML and another offense brought to the Public Prosecutor by initiating law enforcement authority 2006–2009 indicate the total number of ML cases (including cases in which both ML and the predicate offense were investigated) brought to the public prosecutor by year and initiating law enforcement authority. As indicated above, the numbers are indicative of but do not comprehensively set out the total number of investigations conducted for ML.

244. The table with the Total Number of Cases for ML or ML and another offense brought to the Public Prosecutor by initiating law enforcement authority 2006–2009 indicates that more than 70 percent of all ML cases brought forward to the public prosecutor stemmed from criminal investigations conducted by the regional police. The FIOD-ECD is also handling a large number of ML-investigations. This table does however not indicate how many cases brought to the public prosecutor were initiated based upon information provided by the FIU. The authorities stated that this information was difficult to obtain as the police would have direct access to the STR database and it is thus not clear how many prosecutions were triggered by STRs rather than other information obtained by law enforcement authorities.

Number of Criminal Investigations in the Netherlands for pure or mixed ML investigations brought to the Public Prosecutor (provided by the Ministry of Justice)	
Year	
2004	332
2005	365
2006	861
2007	1 174
2008	1 170
2009 (1/1-30/6)	770
Total	**4 672**

Total Number of Cases for ML or ML and another offense brought to the Public Prosecutor by initiating law enforcement authority 2006–2009 (provided by the Ministry of Justice)	
Law enforcement authority	**Number of cases**
Regional Police	3 279
FIOD-ECD	586
KMAR	356
KLPD	287
Interregional fraud team	126
Other	38
TOTAL	**4 672**

245. The table with the Total number of prosecutions for ML or ML and another offense and the one with ML prosecutions combined with certain other offenses **(**see both below**)** show the total number of prosecutions initiated for ML (including cases in which the ML and underlying predicate offense were jointly prosecuted) broken down by year. The table with the Total number of prosecutions for ML or ML and another offense indicates that the number of prosecutions almost doubled in the year 2006 and again

increased by 30 percent in 2007 mainly due to a Supreme Court ruling issued in 2005, which clarified that it is not necessary to prove the underlying criminal offense when prosecuting ML. Furthermore, it was stated that awareness by law enforcement authorities of the relevancy and usefulness of the ML provisions has increased significantly over the last years and has resulted in an increase of cases. In particular, a general instruction issued by the public prosecutor's office, which requires the initiation of an ML investigation whenever a crime generated proceeds of EUR500 or more, may have contributed to this trend.

246. The table with the ML prosecutions combined with certain other offenses provides statistics on the number of cases in which both ML and drug trafficking, human trafficking or criminal organization were prosecuted. The authorities indicated that these three predicate offenses can be considered the most significant proceeds generating crimes committed in the Netherlands.

Total number of prosecutions for ML or ML and another offense (provided by the Ministry of Justice)				
Year	**Prosecution for ML**	**Prosecution was initiated for another offense than ML**	**Fines or other measures applied under Article 74 Penal Code**	**Investigation Terminated**
2004	182	27	6	27
2005	217	27	15	64
2006	397	35	30	76
2007	860	53	102	136
2008	893	49	56	168
2009 (1/1-30/6)	484	27	32	137

ML prosecutions combined with certain other offenses (provided by the Ministry of Justice)			
year	**ML & human trafficking**	**ML & drug related offense**	**ML & criminal organisation**
2004	6	111	62
2005	1	107	71
2006	3	254	189
2007	16	356	223
2008	29	325	152
2009 (1/1-30/6)	13	150	77

247. The table with the results from prosecutions for pure and mixed ML prosecutions sets out the number of convictions and acquittals obtained for pure ML offenses and for ML in connection with a predicate offense. The references to "merge" relate to cases where one court proceeding was later merged with another court proceeding against the same person. The reference to "other" means any other decision than a conviction, merger, or acquittal, such as for example, invalidity of the subpoena, incompetency of the court, stay of prosecution, etc. The numbers in the table suggest that in the first half of 2009, more than three quarters of the prosecutions for ML or/and another offense ended up in a conviction for ML. Only 14 percent of the suspects were acquitted.

Results from prosecutions for pure and mixed ML prosecutions (provided by the Ministry of Justice)				
year	**Conviction**	**Merge**	**Acquittal**	**Other**
2004	128	7	17	
2005	184	7	23	1

Results from prosecutions for pure and mixed ML prosecutions (provided by the Ministry of Justice)				
2006	302	5	36	8
2007	487	26	54	6
2008	647	25	81	8
2009 (1/1-30/6)	348	7	57	3

Analysis of effectiveness

248. The authorities demonstrated a high level of knowledge of the various aspects of the Dutch ML provisions and the application of the provisions is further facilitated by a strong and mature institutional framework and a significant number of court decisions.

249. In comparison to other countries based on GDP and the number of citizens, the Netherlands have conducted a significant number of prosecutions and obtained a good number of convictions either for standalone ML or ML in connection with a predicate offense. These numbers reflect the fact that the Netherlands has a quite liberal approach to applying the money laundering offence, *e.g.* by not requiring the prosecution to establish exactly where and which predicate offense is involved in a specific case. As outlined above, however, in the absence of complete statistics on the number of investigations for ML it is impossible to put the number of ML prosecutions and convictions in a domestic context.

250. While the overall number of prosecutions and convictions for ML is impressive, given the lack of more specific information on types of predicate offense and the nature of ML cases in which convictions were obtained, it is difficult for the assessors to determine how the ML provisions are being used by the authorities, *e.g.*, whether they are mainly used in the context of basic offenses such as theft or whether they are also utilized as a tool to combat serious, organized and transnational crime. Based on the sanctions imposed between 2004 and 2009 and the statistics provided in the table with the ML prosecutions combined with certain other offenses; however, it seems that the ML offenses are applied in both types of situation.

2.1.2 Recommendations and Comments

- The authorities should review all information available with respect to the fines and prison sentence imposed in ML cases to determine whether the sanctions regime is applied effectively, including in relation to legal persons.

- To determine whether the ML provisions are applied effectively in the Netherlands, accurate and complete statistics should be maintained on (1) the number and types of predicate offenses committed in the Netherlands (2) the number of investigations conducted for ML, including information on how these cases where initiated and the types of crime these cases relate to, the number of investigations terminated and the reasons for the termination, and the number of cases pending and (3) the types of predicate offenses involved in ML prosecutions and convictions.

2.1.3 Compliance with Recommendations 1 & 2

	Rating	Summary of factors underlying rating
R.1	**LC**	• Although it is clear that a significant number of investigations, prosecutions and convictions have been obtained, incomplete statistics in some important areas and the lack of information on the types of predicate offenses to which the ML provisions are being applied make it impossible to determine that the ML provisions are applied in a fully effective manner.

R.2	**LC**	• Due to the assessors' lack of access to statistics on the exact amount of fines and the duration of prison sentences imposed in ML cases, it is not possible to establish that the sanctions regime is fully effective. • Although it is clear that a significant number of investigations, prosecutions, and convictions have been obtained, incomplete statistics in some important areas and the lack of information on the types of predicate offenses to which the ML provisions are being applied make it impossible to determine that the ML provisions are applied in a fully effective manner.

2.2 Criminalization of Terrorist Financing (SR.II)

2.2.1 Description and Analysis

Legal Framework:

251. The Netherlands do not have a separate statutory offense of "terrorism financing". The authorities stated that terrorism financing activities would be prosecuted either as "preparation of an offense" under Article 46 of the Penal Code or, where the financing relates to a terrorist organization, as "participation in a terrorist organization" under Article 140a of the Penal Code. Furthermore, criminal liability for terrorist financing may be incurred under the provisions of the Sanctions Act. It is worth noting at the outset that in practice, neither Article 46 nor Article 140a of the Penal Code has ever been used to prosecute or convict a person for terrorism financing activities

252. The Netherlands have ratified the International Convention for the Suppression of the Financing of Terrorism ("FT Convention") on February 7, 2002 and have ratified all nine Conventions and Protocols listed in the Annex to the TF Convention.

Criminalization of Financing of Terrorism (c. II.1):

253. Article 46 of the Penal Code criminalizes the intentional acquisition, manufacturing, import, conveyance in transit, export or possession of any objects, substances, information carriers, premises or vehicle to be used in the commission of a criminal offence that is sanctionable with imprisonment for a term of eight years or more. Conduct pursuant to Article 46 of the Penal Code may be sanctioned with half the maximum penalty available for the underlying offense or, where the underlying offense is punishable with life imprisonment, with imprisonment of a term not exceeding fifteen years.

254. In extensive discussion with the authorities, it was explained that terrorism financing activities could be prosecuted under Article 46 even if no overt act has yet been undertaken to carry out or attempt the financed activity. The reference to "to be used" supports the authorities' view that for Article 46 to apply, it is not required that objects have actually been used for the commission or attempted commission of a criminal offense and that the mere acquisition or possession of objects with the intention that they are to be used to commit a specific underlying offense is sufficient to trigger criminal responsibility for the preparation offense. This interpretation was also confirmed in discussions with representatives of the judiciary. Furthermore, the Supreme Court in a ruling of February 20, 2007 (*Hoge Raad LJN: AZ0213*) clarified that "preparation" is "an incomplete form of a criminal offense" whereby the "punishable preparation is further away from the completed criminal offense than the attempt […] but involves acts in which the perpetrator […] intentionally fabricate[s] or ha[s] at his disposal means that are […] intended for the commission of the criminal offense he has in mind." In another ruling of September 17, 2007, the Amsterdam Court of Appeal held that "contrary to the principle of the 'punishable attempt', no first act towards the commission of the offense on which the intention of the offender is focused applies as yet during preparatory acts. Whereas the attempt always—by the first act in the commission—has a direct link with this 'basic offence', the preparatory act should rather be considered as an independent basic offense,

which is generally characterized by the fact that the preparations for said offense are at such an early stage that a first act in the commission of the offense does not yet apply. This early stage is therefore characteristic for the preparation doctrine."

255. While Article 46 can be applied even if the underlying offense is still far removed, the fact remains that Article 46 is set out in the general parts of the Penal Code and that the sanctions that apply to the preparation offense are calculated based on the statutory sanction available for the prepared offense. As indicated in Dutch parliamentary documents, the offense of preparation is thus an offense "of which the reach and meaning are entirely accessory with respect to the actual interdiction of the autonomous offense."[56] The Supreme Court in a ruling of September 17, 2002 (*Hoge Raad NJ 2002, 626*) further stated that a charge under Article 46 must make it sufficiently clear what the prepared criminal offence was. In the context of terrorism financing this means that Article 46 can only be used to prosecute the financing of specific terrorist acts but generally not the financing of individual terrorists or terrorist organizations.

256. Article 140a of the Penal Code provides that it is a criminal offense to participate in an organization whose aim it is to commit terrorist offenses, whereby paragraph 4 stipulates that the lending of monetary or other material support as well as the raising of funds or recruiting of persons for the benefit of such an organization would qualify as "participation."

257. The sanctions applicable to Article 140a are imprisonment for a term not exceeding fifteen years or a fine of up to EUR76 000 or both. Stricter sanctions may be applied for leaders, founders and directors of such organizations.

258. In addition to Articles 46 and 140a of the Penal Code, the provision of funds, financial assets or economic resources to or for the benefit of the individuals, entities, or organizations designated under UNSCR 1267, 1373, the EC Regulation or Sanctions Regulations may be punished based on the Sanctions Act. The collection of funds for the purpose of financing a designated person or entity would be criminalized only in relation to persons conducting such activity as part of professional financial services but not in relation to private persons collecting such funds. In addition, the above-cited Sanctions Regulations do not extend to situations where funds are merely intended to be but have not yet been provided to a designated individual or entity.

259. Special Recommendation II of the FATF standard requires that the terrorist financing offense extend to any person who provides or collects funds by any means, directly or indirectly, with the intention that they be used (1) for terrorist acts as defined in the TF Convention, (2) by a terrorist organization or (3) by an individual terrorist.

260. The authorities stated that under Dutch law, the material element of "collecting funds" is covered under Article 46 of the Penal Code through the notions of "intentional acquisition" and "possession of" objects. The assessors agree that these references cover the collection of funds in many but not in all instances as funds do not necessarily have to be in possession of or be acquired by the person who is collecting them.

261. In particular, the provision would not apply in situations where funds are not physically acquired or in actual possession of the financer. In response to this concern, the authorities provided a Supreme Court case (*Hoge Raad 12 September 1978, NJ 1979, 84)* in which the term "possession" had been interpreted to cover any situations in which a person has certain objects "at his disposal." However, the term "collecting" as commonly used not only entails disposition authority over things but also covers situations in which a person merely locates or organizes funds. For example, sophisticated terrorism cells

56 Kamerstukken II 1990-1991, 22 268, nr. 3, p. 3.

may employ a person exclusively for the purpose of developing fund raising strategies and organizing fund raising events. Such a person would typically not have any control powers over the funds raised and thus could not be held liable for terrorism financing pursuant to Article 46. The assessors acknowledge that in certain cases such a person could be held criminally liable under Article 140a of the Penal Code for "raising funds" for the benefit of a terrorist organization. However, the fact remains that the "collection" of funds with the intention to support a specific terrorist act is not criminalized under Dutch law and in particular Article 46 of the Penal Code in all cases.[57]

262. The "provision of funds" is not expressly referenced in Article 46 but the authorities explained that the provision of funds would necessarily require the financer to "acquire" or "possess" the funds first. The notions of "acquisition" and "possession," interpreted by the Supreme Court to mean "having disposal over" such funds thus also warrant criminal liability for "the provision" of funds to support terrorist acts.

263. Article 140a of the Penal Code covers both "collection and provision" through the references to "lending monetary and other material support" and "raising funds."

264. Under Special Recommendation II, the terrorist financing provisions shall apply to assets of every kind, whether tangible or intangible, moveable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to or interest in such assets, including but not limited to bank credits, travelers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit, whether from a legitimate or illegitimate source.

265. Article 46 of the Penal Code stipulates that the term "object" shall include any good or property right. A detailed discussion of the scope of this is provided under criterion 1.2 above. The term is used in criminal as well as civil law and includes both legitimate and illicit funds.

266. Until 2007, the language of Article 46 of the Penal Code required that objects must be "manifestly intended" to commit the prepared crime. Following a legislative amendment in 2007, the language of the provision was changed to merely require that objects are "to be used" in the commission of the prepared offense. In a ruling of November 18, 2003 (*Hoge Raad LJN: AJ0535*), which interpreted the meaning of "manifestly intended" as used under the previous version of Article 46, the Supreme Court held that the provision would apply also to legitimate property, such as for example a car, if the property was "clearly intended to be used for a criminal purpose." In a ruling of February 20, 2007 (*Hoge Raad; LJN AZ0213*), the court considered this requirement to be met "if the items, separately or jointly, according to their outward appearance, could be instrumental to the criminal purpose that the Defendant had in mind with the use of these items" and further that "the suspect's intent can give normal objects the status of preparatory objects." The court thus applied a subjective test to determine whether objects were to be used for the commission of the prepared act.

267. The provisions may thus also be applied in relation to legitimate funds that are or intended to be used for terrorism financing.

268. In comparison, the reference in Article 140a to "monetary and other material support" suggests that the term is to be interpreted rather broadly and that the provision can thus be applied to all types of assets as required under the FATF standard, including legitimate funds. This view was also confirmed in the explanatory memorandum that was discussed at parliament before adoption of Article 140a.

57 A clear ministerial commitment to pursue the criminalization of terrorist financing (TF) in line with FATF Special Recommendation II (SR II) has been communicated by the Dutch authorities.

Financing of Terrorist Acts as defined in the TF Convention:

269. Pursuant to Article 2 TF Convention, countries are required to criminalize the financing of "terrorist acts," whereby the term includes (1) conduct covered by the offenses set forth in the nine Conventions and Protocols listed in the Annex to the TF Convention and (2) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

270. As discussed above, Article 46 could be used to prosecute the financing of specific terrorist acts, including in situations where the act that was financed or intended to be financed has not yet been attempted. A number of offenses set out in the nine Conventions and Protocols listed in the Annex to the TF Convention are sanctioned under Dutch law with imprisonment of eight years or more and these provisions thus fall within the scope of Article 46.

271. In some cases, however, the statutory sanctions available are less than eight years. As a result, the financing of such acts cannot be prosecuted under Article 46. Examples of such offenses are "threat to commit a violent attack upon the person or liberty or property of an internationally protected person" (required under the Diplomatic Agents Convention), and "passing on information which is known to be incorrect and may jeopardizes the safety of an aircraft in flight" (required under the Civil Aviation Convention).

272. In other cases, the statutory sanctions available for the basic offense are less than eight years but can be increased to eight years or more if the offense was committed with a "terrorist intent." Accordingly, Article 46 of the Penal Code would apply in such cases. The term "terrorist intent" is defined in Article 83a of the Penal Code as "the objective to cause serious fear in (part) of the population in a country and/or to unlawfully force a government or international organisation to do something, not to do something, or to tolerate certain actions and/or to seriously disrupt or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation". Article 2 of the TF Convention, however, requires countries to criminalize the financing of offenses defined in the Conventions and Protocols listed in the Annex to the TF Convention regardless of whether or not they were committed with a terrorist intent. The additional intent requirement under Dutch law thus goes beyond the TF Convention and is not in compliance with the FATF standard.

273. Offenses within the scope of the generic conduct of "carrying out any act intended to cause death or serious bodily injury to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act" are covered under Dutch law by way of reference to existing criminal offenses carried out with a terroristic intent as indicated above. In particular, intentionally destroying or damaging public property or facilities, including infrastructure, depriving another of his liberty or committing manslaughter with terrorist intent are punishable with more than four years and thus the financing of such acts would fall within Article 46 of the Penal Code.

274. In sum, under Dutch law, a person may be held criminally liable for the financing of many but not all "terrorist acts" as defined under the FATF standard.[55]

Financing of Individual Terrorists pursuant to Special Recommendation II:

275. As indicated above, Article 46 of the Penal Code is limited in scope to situations where "objects, substances, information carriers, premises or vehicles [are] to be used in the commission of [a terrorism] offense." The "making available" of funds, other assets or economic resources to persons, entities and organizations designated under UNSCR 1267, 1373, EC Regulations 881/2002, 2580/2001 or under Sanctions Regulation issued by the Dutch authorities is criminalized under the Sanctions Act, including in situations where the financer has no intention to support a specific terrorist act. However, the Sanctions Act would only cover the "provisions" but not in all cases the "collection" of funds for such persons, entities and organizations. Furthermore, the Regulations do not criminalize the financing of terrorists other than those designated under the Regulations listed above or apply in situations where the funds are merely indented to be but have not yet been provided to a designated individual.

276. As discussed above, Article 46 applies only in relation to a specific underlying offense and thus criminalizes the financing of individual terrorists only if funds are provided with the intention to support a specific terrorist act. In the absence of such intent, the general provision of support to an individual terrorist for example in form of shelter, food or education does not fall within the scope of Article 46. This interpretation was also confirmed by representatives of the judiciary with whom the assessors met.

277. While representatives of the public prosecutor's office argued that the financing of individual terrorist could be covered under Article 46 even in cases where funds are not provided to support a specific terrorist act, the assessors do not see how this interpretation could possibly be applied in practice. For example, if person A provides support to person B, who has committed a terrorist attack in the past but has no intention to do so in the future, A could not be prosecuted for a preparation offense as the terrorist act has been committed before A provided any material support. Furthermore, the sanctions applicable to the "preparatory" offense are based on the sanctions applicable to the underlying criminal offense. In the absence of a determination as to which offense a preparatory act relates to, it is unclear which sanctions would be available for the financing activity.

278. In sum, Article 46 and the provisions of the EC and Sanctions Regulations are not sufficient to criminalize in all cases the provision and collection of funds with the intention that they are to be used by an individual terrorist. Dutch law thus falls short of the requirements of the FATF standard on this point.[55]

Financing of Terrorist Organizations pursuant to Special Recommendation II:

279. Article 140a of the Penal Code as outlined above covers the material elements of "collection and provision" of material support and funds for the benefit of an organization whose aim it is to commit terrorist offenses.

280. As indicated above, Article 140a applies to situations where a person finances an organization whose aim it is to commit a terrorist offense. The provision does not require that the funds are provided or collected with the intention to finance a specific terrorist act, or that the funds have actually been used in the commission of such an offense. Rather, Article 140a applies in all cases where funds are collected or provided for the benefit of a terrorist organization.

281. The term "terrorist offense" as defined in Article 83a of the Penal Code does not cover all acts that are within the definition of "terrorist act" for purposes of Special Recommendation II. The financing of organizations aimed at carrying out a criminal act not covered by Article 140a are nevertheless criminalized under Dutch law based on Article 140 of the Penal Code, which criminalizes the financing of an organization aimed at the commission of any criminal offense.

282. As discussed above, the "provision" of funds to terrorist organizations designated under UNSCR 1267, 1373, EC Regulations 881/2002 and 2580/2001 or under Sanctions Regulation issued by the Dutch authorities is criminalized even if the support is not provided in relation to a specific terrorist act. However, the Regulations do not cover the "collection" of funds for such organizations and are not applicable in relation to terrorist organizations other than those designated under the Regulations listed above. Furthermore, the cited Regulations do not cover situations in which funds are merely intended to be but have not yet been provided to a designated organization or entity.

283. In sum, Articles 140a, 140, and the provisions of the EC and Sanctions Regulations are sufficient to criminalize the provision and collection of funds with the intention that they are to be used by a terrorist organization in line with the FATF standard.

Attempt and ancillary offenses pursuant to Article 2(5) TF Convention:

284. "Terrorism financing" is not set out as a separate criminal offense under Dutch law. As outlined above, in certain cases terrorism financing activities could be prosecuted under the offenses of "preparation of an offense" or "participation in a terrorist organization" under Articles 46 and 140a of the Penal Code.

285. In relation to terrorism financing activities pursuant to Articles 140a, a wide range of ancillary offenses apply as discussed under Recommendation 1 above. In particular, attempt to commit, aiding and abetting, facilitating and counseling the commission of an act pursuant to Article 140a is all criminalized.

286. With respect to terrorism financing activities prosecuted as "preparation" offense, the ancillary offenses set out under Articles 47 and 48 of the Penal Code (procuring, assisting, solicitation or aiding and abetting of an offense) are applicable. This was also confirmed in a ruling by the Court of Appeal of October 9, 2006 (LJN: AZ0908). However, the offense of "attempt" is not applicable in relation to Article 46 as the former carries a stricter sentence than the latter and, should the case arise, the attempt to finance terrorism would thus be prosecuted as an attempt to commit the terrorist act.[55]

Predicate Offense for Money Laundering (c. II.2):

287. "Terrorism financing" is not a separate statutory offense under Dutch law and does therefore not *per se* qualify as predicate offense for ML. However, as indicated in the discussions under Recommendations 1 and 2 above, any offense under Dutch law may constitute predicate offenses for ML. Terrorism financing activities that fall within the scope of Articles 46 or 140a of the Penal Code are thus predicate offenses for ML.

Jurisdiction for Terrorist Financing Offense (c. II.3):

288. Articles 46 and 140a of the Penal Code do not address extraterritorial jurisdiction. However, the authorities stated that both Articles 46 and 140a could be applied regardless of whether the financed act or organization is located in the Netherlands or abroad. The authorities' claim was supported by a number of rulings by the Supreme Court (*Hoge Raad NJ 2008, 559, Hoge Raad NJ 2003, 315; Hoge Raad NJ 2009, 346*) in which the court held that Article 46 also applies to the preparation of acts that are to be committed abroad and that Article 140 also applies to the participation in criminal organizations located outside the Netherlands. To the extent that Dutch law criminalized FT, the relevant legal provisions thus also apply in situations where merely the financing activity is carried out in the Netherlands but the financed act/individual/organization is located abroad.

289. In addition, Articles 4 and 5 in combination with Article 78 of the Penal Code provide for extraterritorial jurisdiction in relation to the preparation of a list of offenses if these offenses are to be carried out with a terrorist intent.

The Mental Element of the TF Offense (applying c. 2.2 in R.2):

290. "Terrorism financing" is not a separate statutory offense under Dutch law. As discussed in detail above, in many instances, terrorist financing activities could however be prosecuted as "preparation of a serious offense" or "participation in a terrorist organization" under Articles 46 and 140a of the Penal Code.

291. Article 46 Penal Code requires that the perpetrator acts intentionally in carrying out the preparatory act (*e.g.*, the acquiring, possessing, etc.).

292. In addition, Article 46 applies only in respect to objects that are "to be used" in the commission of the prepared offense. As indicated above, this requirement is established based on the perpetrator's subjective intent. The Supreme Court in a ruling of July 7, 2009 (*LJN: BH9025*) held that the subjective intent requirement under Article 46 of the Penal Code is one of a "conditional intent" and thus that the mens rea requirement is met if the prosecution can establish that the defendant in carrying out his/her action deliberately accepted the change that the underlying crime is completed" ("*dolus eventualis*").

293. Article 46 of the Penal Code does, however, not apply in situations where funds or other property are collected for or provided to an individual terrorist or a terrorist organization for purposes other than to commit a specific terrorist act.

294. Article 140a is wider in scope than Article 46 in that it merely requires that the financier provides support or raises funds for the benefit of a terrorist organization. The provision thus also applies in the absence of intent or knowledge of a specific terrorist act.

295. Dutch law does not provide for a statutory provision that would regulate the inference of the mental element from objective factual circumstances. However, the Supreme Court has confirmed application of this principle in a number of criminal cases (*Hoge Raad September 27, 2005, NJ 2006, 473; Hoge Raad September 28, 2004, NJ 2007, 278*) and the authorities confirmed that if the case was to arise, the principle would also apply to terrorism financing conduct prosecuted under Articles 46 or 140a of the Penal Code.

Liability of Legal Persons (applying c. 2.3 & c. 2.4 in R.2):

296. Article 140a of the Penal Code applies to "any person" who carries out an act that constitutes participation in a terrorist organization. Article 46 applies to any perpetrator without differentiating between natural and legal persons.

297. Article 51 of the Penal Code establishes that any criminal offense under Dutch law may be committed by natural and legal persons. The provision thus also applies to the offenses under Articles 46 and 140a. Legal persons may be subject to criminal proceedings and be sanctioned with the penalties and non-punitive orders as and where appropriate.

298. Article 51 of the Dutch Penal Code expressly stipulates that holding legal persons criminally liable does not preclude the possibility of parallel criminal proceedings against the persons who ordered the commission of or controlled the prohibited act. The authorities clarified that it would in theory be possible to initiate criminal proceedings against a legal person and at the same time to conduct civil or administrative proceedings. As a general rule, however, criminal proceedings would be carried out first and civil and administrative proceedings would be initiated only later. In certain cases, administrative permits may be revoked concurrently with the filing of criminal charges.

299. Legal persons designated pursuant to UNSCR 1267 or 1373 are automatically prohibited under Dutch law. In all other cases, a legal ban can be solicited by way of civil proceedings and based on Article 220(1) of the Penal Code.

Sanctions for TF (applying c. 2.5 in R.2):

300. Criminal conduct under Article 46 Penal Code is sanctioned with half the maximum penalty for the prepared criminal offense itself or imprisonment of a term not exceeding fifteen years if the main offense is punishable with life imprisonment. Given that only offenses punishable with imprisonment for eight years or more fall within the scope of Article 46, the minimum sanction applicable to conduct prosecuted under this provision would be four years.

301. The sanctions for offenses within the scope of Article 46 range from imprisonment for up to eight years to imprisonment of up to thirty years. The financing of such offenses could thus be punished under Article 46 with imprisonment for four years to fifteen years and a fine, depending on the severity of the underlying offense.

302. This is slightly stricter than the sanctions available for terrorism financing offenses in other FATF countries (Germany-six months to ten years; Norway—up to ten years; and Finland—four months to eight years) but in line with the sanctions available for other serious offenses under Dutch law, such as for example counterfeiting of currency or extortion (imprisonment of up to nine years and a fine of up to EUR76 000) and trafficking in human beings or illicit arms trafficking (imprisonment of up to eight years and a fine of up to EUR76 000).

303. Article 140a of the Penal Code sets out sanctions of imprisonment for a term not exceeding fifteen years or a fine of up to EUR76 000. Stricter sanctions may be applied for leaders, founders and directors of such terrorist organizations. The sanctions applicable to Article 140a seem to be stricter than the sanctions applicable to other serious crimes under Dutch law. For example, participation in an organized criminal group is punishable with imprisonment of up to six years and a fine of up to EUR76 000.

304. In the absence of any convictions for FT, it could not be determined that the amount and types of sanctions applied in practice are effective and dissuasive.

Statistics (R.32):

305. It is not clear how many investigations for TF have been conducted in the Netherlands but from discussions with the authorities, it seems that only two cases have so far been investigated. There have not been any prosecutions or convictions for FT.

Analysis of effectiveness

306. FT has not been established as a separate statutory offense under Dutch law. Nevertheless, the existing criminal provisions as outlined above allow the authorities to prosecute terrorism financing activities in certain situations envisaged by the international standard.

307. In the absence of reliable and accurate statistics on the number of investigations carried out in relation to terrorism financing activities and given the lack of any prosecutions and convictions for such activities, however, it is difficult to assess whether the authorities effectively apply the offenses of “preparation of a serious offense” or “participation in a terrorist organization” in relation to terrorism financing conduct. From discussions with the authorities it seems that there have been increased efforts by law enforcement authorities, including the FIU, to detect cases of TF and to investigate money flows in the

context of terrorist investigations. However, those efforts have not yet resulted in any actual case. In discussions with law enforcement authorities, it was stated that this may be due to the fact that TF is not criminalized as a separate offense and thus is not treated as an autonomous offense by law enforcement and prosecutorial authorities.[55]

308. Subsequent to the onsite visit, the assessors received a letter by the Board of Procurators General, in which it was stated that "the Public Prosecution Service does not experience any obstructions in current criminal provisions to the investigation and prosecution of the financing of terrorism." While the assessors appreciate the clarification received by the Board of Procurators General, given the consistent message received in discussions with different law enforcement authorities, concerns remain that the lack of a specific FT offense may have a negative impact on the effective investigation and prosecution of terrorism financing activities in the Netherlands.

2.2.2 Recommendations and Comments

- Criminalize terrorism financing fully in line with the FATF standard as per Ministerial Commitment.
- Amend the law to expressly criminalize in all circumstances the "collection" of funds to commit a terrorist act, including in cases where the financer is neither in possession of nor has acquired the collected funds.
- Amend the Penal Code to ensure that the financing of all "terrorist acts" as defined under the FATF standard is criminalized.
- Criminalize the financing of individual terrorist including in cases where funds are provided for purposes other than to support the commission of a specific terrorist act or where the financing relates to terrorists other than those designated through the UN, EC and Ministerial Sanctions Regulations.
- Criminalize the attempt to finance a specific terrorist act.
- Put in place mechanisms to ensure that FT activities are investigated and prosecuted effectively in the Netherlands, for example by providing for TF as a separate criminal offense in line with the UN Convention for the Suppression of the Financing of Terrorism.

2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	**PC**	• The "collection" of funds to commit a terrorist act is only criminalized if the perpetrator has acquired or actually possessed the funds. • Article 46 of the Penal Code does not sufficiently criminalize the financing of conduct covered by the offenses set forth in the nine Conventions and Protocols listed in the Annex to the TF Convention. • The criminalization of financing of an individual terrorist is only limited to the case in which the financed person has been designated under the UN, EC, or Dutch Sanctions Regulations. • Attempt to finance a specific terrorist act is not criminalized. • The absence of an autonomous TF offense has a negative impact on the effective investigation and prosecution of terrorism financing activities.

2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)

2.3.1 Description and Analysis

Legal Framework:

309. Articles 33a and 36e of the Penal Code allow for the confiscation of proceeds of and instrumentalities used or intended to be used in the commission of criminal offenses. Provisional measures are set out in Articles 94 and 94a of the Criminal Procedure Code.

310. Confiscation measures pursuant to Article 33a and 36e are both conviction based. While confiscation under Article 33a must take place in relation to specific types of property or assets, which may also include instrumentalities, confiscation measures under Article 36e are value based and can only be applied to proceeds but not instrumentalities of crime.

311. However, the scope of Article 36e goes beyond that of Article 33a as the latter only covers proceeds or instrumentalities of the crime for which the criminal conviction was obtained. In comparison, Article 36e provides for confiscation not only of proceeds obtained from the offense for which the conviction was obtained but also of offenses that are likely to have been committed in the course of the sanctioned act.

312. Both confiscation measures under Articles 33a and 36e are discretionary and can be and in practice have been applied both in parallel and in series. While confiscation under Article 33a is possible only as part of the conviction for the underlying criminal conduct, an application for a confiscation under Article 36e may be submitted by the public prosecutor up to two years after a conviction for a criminal offense has been issued by the court of first instance.

313. A general instruction by the Public Prosecution Service urges all prosecutors to initiate confiscation proceedings under Article 36e whenever criminal proceeds are estimated to amount to a value of EUR500 or more.

Confiscation of Property related to ML, TF, or other predicate offenses including property of corresponding value (c. 3.1):

314. Article 33a of the Dutch Penal Code allows for the court to order the confiscation of property and instrumentalities used or intended for use in the commission of crime as part of a conviction for any offense. Article 33a clarifies the types of property and assets that may be subject to confiscation under Article 33a, namely:

- Objects that are owned or possessed or can be used by the convicted person and that have been fully or largely obtained through the criminal offense for which the conviction was obtained.
- Objects in relation to which the offense has been committed (the objects of the crime).
- Objects which have been or were intended to aid or were manufactured for the commission of the offense or were used to obstruct the criminal investigation.

315. The term “objects” includes any items and property rights. “Property right” is defined in Article 6 of Book 3 of the Civil Code to cover all “rights that are, either individual or as part of another right, transferable or provide the one who is eligible [to it] with material benefits or are received in exchange for supplied or promised material remuneration.” The term “goods” is defined in Article 2 of Book 3 to extend to all “material objects susceptible for human control.”

316. In discussions with the authorities it was stated that the term "objects" would include everything of value, including but not limited to money, real estate and property. To support this view, the authorities provided a ruling by the Amsterdam Appeals Court (*Hof Amsterdam 3 July 2009, LJN: BJ1646, zaak Holleeder*) in which the court considered cash, bank accounts, apartment rights, real estate and company premises to constitute "objects" that directly or indirectly stem from a criminal offense.

317. Based on the broad language of Articles 2 and 6 of Book 3 of the Civil Code and the cited case law, the assessors conclude that the term "objects" includes assets of any kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets, and that Dutch law is thus in compliance with the FATF standard on this point.

318. Article 36e of the Dutch Penal Code sets out an additional and rather broad confiscation provision. Pursuant to the provision, the court, upon request by the Public Prosecutor's Office and based on a criminal conviction for any criminal offense, may order the convicted person to pay "a sum of money […] in confiscation of illegally obtained profits and advantages [obtained] by means of or from the commission of the criminal offense." In addition, Article 36e also allows for confiscation of the following:

- Profits and advantages gained from "similar offenses" as the one for which the conviction was obtained or from "any offense which is punishable with EUR76 000" based on "sufficient evidence" that the convict has committed that offense.

- Only in cases where the conviction was obtained for an offense punishable with up to EUR76 000 profits and advantages that based on the results of a financial investigation are "likely" to have been obtained through the commission of any other criminal offense.

319. The notion "similar offense" is not defined in the law but the authorities explained that the term would extend to any offenses that fall within the same category as the offense for which the conviction was obtained. For example, if person A is convicted for drug trafficking and it can be shown based on "sufficient evidence" that he also committed other drug offenses such as for example cultivation, Article 36e may be used to also confiscate the proceeds or benefits of the cultivation offense even though no conviction has been obtained for this act. Asked how the "sufficient evidence" standard was applied in practice, the authorities stated that the threshold could be met by showing, for example, that the person has been indicted for the "similar offense."

320. With respect to the second case, namely where the conviction was obtained for an offense punishable with up to EUR76 000, the prosecutor on the basis of the findings of a financial investigation may establish that the defendant is "likely" to also have obtained profits and advantages through the commission of other criminal offenses. Upon establishing this assumption, the defendant has an opportunity to show that the funds in question have in fact been obtained through licit means. Otherwise the funds may be confiscated based on Article 36e.

321. With respect to equivalent value of proceeds of crime, confiscation orders under Article 36e are issued on the estimated benefit and it therefore does not matter whether the order is satisfied through the payment of illicit or legitimate funds or assets. While Article 33a does not allow for equivalent value confiscation, Article 36e can be applied in parallel to Article 33a as indicated above.

322. It is up to the court to determine the amount of the profits or advantages. Article 36e (4) provides that in calculating the amount to be confiscated, costs saved are to be treated as part of the profit and legal claims are to be subtracted. The value of property and property rights are to be estimated according to their market value at the time of the court order. The court has discretion to set the confiscation order at less

than the estimated profit or advantage and also makes frequent use of this discretionary power in practice. The authorities stated that in the case where a confiscation order is not fully satisfied during the execution stage, the order would be adjusted to reflect the actual outstanding amount.

323. In sum, Article 33a allows for the confiscation of laundered property as well as of proceeds from, instrumentalities used and instrumentalities intended to be used in the commission of any criminal offense. In addition, Article 36e provides for the confiscation of property laundered and proceeds from any criminal offense, including their equivalent value.

324. As indicated in Recommendation 1 above, all FATF designated categories of predicate offenses are criminalized under Dutch law and thus Articles 33a and 36e apply to all such offenses. However, the shortcomings identified with respect to the existing provisions of "preparation of a serious offense" and "participation in a terrorist organization" only allow for a limited application of Articles 33a and 36e in relation to terrorist financing offenses.

Confiscation of Property Derived from Proceeds of Crime (c. 3.1.1 applying c. 3.1):

325. Article 36e (2) expressly refers to profits or advantages that have been obtained "by means of or from proceeds of the criminal offense" and the authorities confirmed that this language is to be interpreted to also cover indirect proceeds. While the general confiscation provision under Article 33a does not cover indirect proceeds, Article 36e can be applied in parallel to Article 33a as indicated above.

326. Under Article 33a, property held by third parties may be confiscated if the prosecution can establish that the defendant is the actual owner of the property or that the third party owning the property is aware or should have suspected that the property was obtained through or was used in connection with or in the commission of the criminal offense, or that it could not be determined by whom the property in the possession of a third party is owned.

327. While value-based confiscation orders under Article 36e are only applicable against property held or owned by the defendant but not versus third parties, Article 33a meets the requirements of the FATF standard on this point.

Provisional Measures to Prevent Dealing in Property subject to Confiscation (c. 3.2):

328. Article 94 and 94a of the Criminal Procedure Code set out seizing measures with respect to property laundered, proceeds of and instrumentalities used or intended for use in the commission of any criminal offense.

329. Under Article 94, any object which "may serve to uncover the truth or to demonstrate illegally obtained gains pursuant to Article 36e of the Criminal Code" can be seized. In addition, Article 94a allows for the seizing of objects in the course of an investigation for a crime that is punishable with a fine of up to EUR76 000 and to safeguard the right of recourse with respect to "a fine to be imposed" or "the obligation to pay a sum of money to the state for the confiscation of illegally obtained benefits." While Article 94 thus allows for seizure of both instrumentalities and proceeds, the application of Article 94a is limited in scope to proceeds of crime.

330. Seizing measures under Article 94 may be carried out based on prosecutorial consent. In comparison, seizing measures under Article 94a require a judicial order or, in cases where a criminal financial investigation is carried out based on approval by an examining magistrate, a decision by the public prosecutor. Seizing orders are not subject to any time limitations. The authorities explained that the reference to confiscation under Article 36e in both Article 94 and 94a allows for proceeds of crime to be initially seized under Article 94 and subsequent to the obtaining of judicial order to be converted into a

seizing measure pursuant to Article 94a. In urgent cases, law enforcement authorities are thus in a position to seize proceeds of crime even in the absence of a court order.

331. Legitimate assets equivalent in value to proceeds of crime or property laundered may be seized pursuant to Article 94a. Under Article 94a property held by a third party may be seized if it can be established that the property is owned by the defendant. In all other cases, property owned by third parties may be seized only if it can be shown that the property constitutes proceeds of crime and may be confiscated under Article 33a or 36e of the Penal Code that the objects are owned by the third party to impede the sale thereof and that the third party knew or should have suspected that the objects were proceeds of crime. Instrumentalities held by third parties are also subject to seizure under Article 94 as the provision applies with respect to any evidence, regardless of where it is located.

332. In summary, Dutch law allows for the seizing of all objects that are or may become subject to confiscation under Articles 33a and 36e.

Ex Parte Application for Provisional Measures (c. 3.3):

333. The authorities indicated that seizing measures under both Article 94 and 94a of the Penal Procedure Code could and have in the past been issued ex-parte and without prior notice. Notification to the person by whom property is owned or held is, however, provided after the seizure has been applied.

Identification and Tracing of Property subject to Confiscation (c. 3.4):

334. For a detailed discussion of law enforcement authority's tracing and identification powers, including the powers to access confidential information, see the discussion of Recommendation 28 of this report. In summary, law enforcement authorities have a wide range of mechanisms available to identify and trace assets that are or may become subject to confiscation. Information and documents held by FIs and DNFBPs may be accessed based on a prosecutorial decision. Information and documents held by lawyers and other legal professionals may however only be accessed in very limited circumstances, such as for example if the lawyer or legal professional himself is a suspect in a criminal investigation. Further information on this point is provided under Recommendations 28 below.

Protection of Bona Fide Third Parties (c. 3.5):

335. Bona fide third parties are protected under Dutch law through Articles 33a (2) and (3) of the Criminal Procedure Code, which allows for the confiscation of assets owned by a third party only if it can be established that the third party had actual knowledge or should have known that property represented proceeds or instrumentalities of crime.

336. Any affected person may challenge seizing measures at the district court level. From there, recourse to the Court of Appeal is possible. Bona fide third parties may also participate in a criminal trial as a victim of the crime.

Power to Void Actions (c. 3.6):

337. Article 3:40 of the BW stipulates that any acts in breach of public order are null and void. Contracts that were entered into in order to prejudice the recovery of confiscated property would thus not be valid under Dutch law. In addition, under Article 94d (2) of the Criminal Procedure Code the public prosecutor may declare null and void any fraudulent conveyances, including legal acts, which an accused or convicted person has entered into or carried out within one year prior to the commencement of a criminal investigation of that person.

Additional Elements (Rec 3)—Provision for a) Confiscation of assets from organizations principally criminal in nature; b) Civil forfeiture; and, c) Confiscation of Property which Reverses Burden of Proof (c. 3.7):

338. Assets from organizations principally criminal in nature may be confiscated under Article 36e of the Criminal Procedure Code, as the provision allows for confiscation of assets not only in relation to the crime for which the conviction was obtained but also in relation to assets obtained from similar crimes. In cases where the conviction was obtained for a crime punishable with up to EUR76 000, assets of a criminal organization may also be confiscated after it has been determined based on a financial investigation that such assets are "likely" to have been obtained through the commission of any other criminal offense.

339. Confiscation without a prior criminal conviction is generally not possible in the Netherlands. As noted in the analysis section above, in certain cases proceeds can however be confiscated even if they do not result from the offence for which the conviction was obtained.

340. At the time of the assessment, Dutch law did not yet provide for a reversed burden of proof in confiscation proceedings. However, the authorities advised that a new draft law which would introduce such a reversed burden had been submitted to and was being discussed by parliament.

Statistics (R.32):

341. Statistics provided by the authorities as indicated in the table "Amounts confiscated in criminal cases between 2006 and 2009" and "Types and Amounts of assets seized in criminal cases 2008 and in 2009" (see both tables below) show that between 2006 and 2009, the Dutch authorities have confiscated a total of EUR104 million (EUR93 on the basis of Article 36e and EUR11 on the basis of Article 33a) and seized EUR618 million in criminal cases.

Amounts confiscated in criminal cases between 2006 and 2009				
	2006	**2007**	**2008**	**2009**
Special Confiscation (Article 36e)	EUR 17 million	EUR 23.5 million	EUR 23.5 million	EUR 39 million
Confiscation (Article 33a)	unknown	unknown	unknown	EUR 11 million
Currently seized , pending treatment before the court	unknown	unknown	EUR 552 million	EUR 618.6 million

Types and Amounts of assets seized in criminal cases 2008 and in 2009		
	2008	**2009**
Bank account	EUR 113.5 million	EUR 111 million
Claims/Bank guarantees	EUR 141 million	EUR 196 million
Registered property	EUR 268 million	EUR 284 million
Other property	EUR 23.5 million	EUR 21 million
International	EUR 6 million	EUR 6 million
Total amount	**EUR 552 million**	**EUR 618 million**

342. The table below provides statistics on the number of Article 33a confiscation orders issues in relation to pure or mixed money laundering offenses and the relevant legal basis for the preceding seizure.

Judicial decision confiscation 33/33a Penal Code		**Year of judicial decision**						
	Legal basis for seizure	2005	2006	2007	2008	2009	2010	
	Art 94 PC	13	47	72	86	112	101	
	Art 94a PC		1		2	3	1	
	Both	9	15	22	29	38	24	
	Not registered	1		2	2	5	3	
	Total	23	63	96	119	158	129	588

343. The table below shows statistics on the number of Article 36e confiscation orders issued in relation to pure or mixed money laundering offenses and the number of cases in which a confiscation order was supported by a seizing measure either under Article 94 or 94a. According to these statistics, the Netherlands between 2005 and 2010 have confiscated approximately EUR93 million based on Article 36e in ML cases. The authorities indicated that the orders are not yet final and may be subject to appeal.

Judicial decision special confiscation 36e Penal Code Year of judicial decision							
		2005		2006		2007	
Type of seizure	Decision	Number	Amount	Number	Amount	Number	Amount
Art 94 PC	rejected	9	0	1	0	5	0
	Partially sustained	1	1 500.00	6	385 377.68	12	55 688.85
	sustained	18	1 005 128.82	19	4 626 685.60	29	303 217.10
Total		28	1 006 628.82	26	5 012 063.28	46	358 905.95
Art 94a PC	rejected	2	0	6	0	3	0
	Partially sustained	2	1 410 825.23	4	352 283.28	7	12 393 470.15
	sustained	16	4 558 489.61	8	1 432 796.78	16	4 789 889.45
Total		20	5 969 314.84	18	1 785 080.06	26	17 183 359.60
Total		48	6 975 943.66	44	6 797 143.34	72	17 542 265.55
Total (without differentation art. 94/94a)							
	rejected	11	0	7	0	8	0
	Partially sustained	3	1 412 325.23	10	737 660.96	19	12 449 159.00
	sustained	34	5 563 618.43	27	6 059 482.38	45	5 093 106.55
Total		48	6 975 943.66	44	6 797 143.34	72	17 542 265.55
		2008		2009		2010	
Type of seizure	Decision	Number	Amount	Number	Amount	Number	Amount
Art 94 PC	rejected	12	0	21	0	23	0
	Partially sustained	5	46 614.57	6	90 735.77	12	213 925.47
	sustained	43	5 013 515.76	47	2 459 331.12	47	1 613 306.78
Total		60	5 060 130.33	74	2 550 066.89	82	1 827 232.25
Art 94a PC	rejected	12	0	11	0	7	0
	Partially sustained	5	809 665.47	9	4 469 460.62	6	347 662.46
	sustained	52	20 723 849.27	50	9 206 395.37	52	17 270 426.12
Total		69	21 533 514.74	70	13 675 855.99	65	17 618 088.58
Total		129	26 593 645.07	144	16 225 922.88	147	19 445 320.83
Total (without differentiation art. 94/94a)							
	rejected	24	0	32	0	30	0
	Partially sustained	10	856 280.04	15	4 560 196.39	18	561 587.93
	sustained	95	25 737 365.03	97	11 665 726.49	99	18 883 732.90
Total		129	26 593 645.07	144	16 225 922.88	147	19 445 320.83

344. The authorities do not maintain accurate statistics on the total number of ML cases in which seizing measures were applied, or the amounts seized in each case. In addition, the statistics provided under Recommendation 1 do not indicate how many investigations for ML were conducted in the Netherlands. In the absence of more comprehensive statistics assessors are not in a position to come to a final conclusion of whether the seizing powers are applied effectively in ML cases.

345. With respect to confiscation, it seems that between 2005 and 2010, confiscation orders either based on Article 33a or Article 36e have been issued in about 1 172 pure or mixed ML cases, which equals about 60 percent of all cases in which a conviction was obtained. This seems to be in line with the number of confiscations in the context of other offenses.

346. Between 2006 and 2009 seizing measures were applied in approximately 3 000 cases and confiscation measures in approximately 5 000 cases related to drug offenses. Relying on the data provided under Recommendation 1 for the years 2004–2006 and assuming that the number of drug related investigations has not gone down significantly, it can be estimated that in about 50 percent of all drug related cases confiscation measures were applied.

347. The total amount of assets confiscated is EUR104 million. The amounts actually realized between 2006 and 2009 are unclear.

Analysis of effectiveness

348. In the absence of better statistics on the number of ML and TF investigations conducted in the Netherlands and the number of cases in which assets were seized and the amounts seized in each case; and the amounts eventually realized in each case, it is not possible for the assessors to come to a final conclusion as to whether the seizing and confiscation measures are effectively applied with respect to ML, TF and predicate offenses.

349. A preliminary analysis by IMF staff of freezing, seizing, and confiscation data in 15 countries assessed under the FATF 2004 Methodology for which data are available suggests that the Netherlands is slightly less effective at obtaining orders to get assets confiscated than other countries (EUR104 or $139 million in the Netherlands vs. $177 million comparative groups average).

Comparative Information for Assets frozen, restrained, seized, forfeited or confiscated taken from 15 Mutual Evaluation or Detailed Assessment Reports for countries evaluated as LC or higher under the FATF 2004 Methodology		
Indicator	**Comparative Group Average[1]**	**Netherlands (2005-2010)**
Assets frozen, restrained or seized		
Total latest 4 years	$246 million	Not Available
Annual value	$104 million	Not Available
Annual value per million of population	$1.46	Not Available
Annual value as % of GDP	0.0060%	Not Available
Assets ordered forfeited (or confiscated)		
Total	$177 million	$139 million
Annual Value	$70 million	$27.8 million
Annual value per million of population	$1.11	$1.68
Annual value as % of GDP	0.0044%	0.0048%
Annual value compared to annual value assets frozen, restrained or seized	67%	Not Available
Assets forfeited or confiscated		

Comparative Information for Assets frozen, restrained, seized, forfeited or confiscated taken from 15 Mutual Evaluation or Detailed Assessment Reports for countries evaluated as LC or higher under the FATF 2004 Methodology		
Total	$2 902 million	Not Available
Annual Value	$733 million	Not Available
Annual value per million of population	$2.94	Not Available
Annual value as % of GDP	0.0270%	Not Available
Annual value compared to annual value assets frozen, restrained or seized	702%	Not Available
Annual value compared to annual value assets ordered forfeited or confiscated	1 045%	Not Available

[1] The countries are: Australia, Canada, Denmark, Ireland, Italy, Japan, Mexico, Norway, Portugal, Russia, Singapore, Spain, Sweden, Thailand, U.K., and U.S.A.

350. With respect to confiscation, anecdotal evidence suggests that there remains a disconnect between the amount of assets requested by the prosecution to be confiscated, the amount of assets confiscated by the courts and the amount of assets eventually recovered through execution of the confiscation orders. In the absence of any comprehensive and accurate statistics on this point, however, it is not possible for the assessors to verify this information.

351. Efforts are currently underway to further increase law enforcement authorities' ability and skills to apply the seizing and confiscation provisions and to further recognize their usefulness in fighting ML, by, for example, putting in place training and outreach programs. One law enforcement authority also established a pilot program in some regions of the Netherlands (outside the main metropolitan areas as Amsterdam, Rotterdam, and The Hague), which resulted in a significant increase in the amount of assets and funds seized and eventually confiscated.

352. Overall, the assessors are of the view that the Netherlands have a strong and comprehensive legal confiscation framework in place. The application of the framework seems to be effective to a certain degree but could be further improved.

2.3.2 Recommendations and Comments

- Ensure that access to appropriate information and documents held by lawyers and other legal professionals is available in all cases.

- To determine whether the confiscation framework is applied effectively better statistics on (1) the number of ML and TF investigations conducted in the Netherlands and the number of cases in which assets were seized and the amounts seized in each case; (2) the total number of assets confiscated in ML and TF cases, including on the basis of Article 33a; and (3) the amounts requested to be seized and eventually realized in each case should be maintained.

2.3.3 Compliance with Recommendation 3

	Rating	Summary of factors underlying rating
R.3	**LC**	• The scope of legal privilege hinders appropriate access to information and documents held by lawyers and other legal professionals. • While the application of the confiscation framework seems to yield some results, in the absence of more comprehensive statistics the assessors are not in a position to conclude that the provisions are applied in a fully effective manner.

2.4 Freezing of funds used for terrorist financing (SR.III)

2.4.1 Description and Analysis

Legal Framework:

353. The Netherlands freeze funds and assets used to finance terrorism on the basis of EC-regulations and complementary domestic legislation. UN Security Council Resolution 1267 (1999), 1390 (2002) and 1455 (2003) are implemented by EC Regulation No. 881/2002 of May 27, 2001 and most parts of UN Security Council Resolution 1373 is implemented by EC Regulation No. 2580/2001 of December 27, 2001. Whereas the EC Regulation applies to any terrorist individuals or organizations, the latter applies only to such individuals and organizations that are linked or related to non-EU countries.

354. Both EC Regulations are directly applicable in the Netherlands and funds and assets may thus be frozen directly and immediately based on the Regulations' provisions. However, infringements of the relevant provisions need to be penalized via national Dutch legislation.

355. The Sanctions Act 1977 serves as a legal basis for the penalization of infringements of the EC Regulations and for the Dutch authorities to freeze funds and assets of terrorist and terrorist organizations under UNSCR 1373. Article 2 of the Sanctions Act empowers the Minister of Foreign Affairs in concurrence with the Minister of Finance and the Minister of Justice to issue "orders and regulations to comply with international resolutions related to the fight of terrorism" (referred to in this report as "Sanctions Regulations"). Any person or entity located in the Netherlands could thus be subject to Sanctions Regulations and the freezing obligation stipulated therein could be applied to any assets and property within the scope of the two Security Council Regulations. The authorities provided the assessors with a translated copy of a number of Sanctions Regulations, which confirmed that Sanctions Regulations issued by the Ministry of Foreign Affairs are in fact applicable to all persons and entities located in the Netherlands and freeze both funds and other property held or controlled by designated terrorists or terrorist organizations.

356. As indicated above, persons, groups and entities based or residents within the European Union, including the Netherlands (referred to herein as EU-residents) do not fall within the scope of Council Regulation 2580/2001. Such persons are, however, covered under EU Council Common Positions No. 2001/931/CFSP and the Netherlands have implemented this Common Position through Sanctions Regulation Terrorism 2002–II. A cross reference to the Common Position ensures that any changes to the list of entities and persons attached to it are automatically integrated into Dutch law.

357. In addition, the Sanctions Act can be utilized to freeze the assets and funds of persons and entities that have not yet been designated by the EC but which the Dutch authorities consider to fall within the scope of UN Security Council Resolution 1373. The authorities stated that the funds and assets of twenty-one individuals and legal entities have so far been frozen based on the Sanctions Act, eleven of which have only been listed on the national list. Sanctions Regulations were issued with respect to six organizations of which five are legal entities and their assets were frozen on the basis of such Regulations. One of these cases was triggered by a request of a foreign jurisdiction to freeze assets pursuant to UN Security Council Resolution 1373. All other cases were initiated by the Dutch authorities based on sufficient indications. It was further stated that in the majority of these cases, the Dutch authorities later successfully requested the designation of those individuals and entities under EC Regulation 2580/2001.

Freezing Assets under S/Res/1267 (c. III.1):

358. The Netherlands implements the financing of terrorism aspects of UNSCR 1267 and subsequent resolutions through EC Regulation 881/2002, which is directly applicable in the Netherlands and thus does

not require any implementing domestic legislation. However, infringements of the relevant provisions need to be penalized via national legislation; in particular Sanction Regulations on Osama bin Laden, Al-Qaida, and the Taliban 2002. Under the Regulation, all funds and economic resources belonging to or owned or held by a natural or legal person, group or entity designated by the EU Sanctions Committee and listed in the annex to the regulation are automatically frozen. The list under EC Regulation 881/2002 contains both EU-externals and EU-internals. Funds are frozen directly and immediately upon entry into force of the amendments to the Council Regulation.

359. The freezing mechanism under EC Regulation 881/2002 applies to a broad notion of financial assets and economic resources, however acquired, that belong to or are owned, controlled or held by designated persons or entities. The definition also covers funds derived from property owned or controlled by designated person such as interest, dividends or other income on or value accruing from or generated by such assets.

360. EC Regulation 881/2002 does not expressly cover financial assets and economic resources that are jointly owned or held property but only applies to funds and economic resources belonging to, or owned or held by, a designated person. However, EC Regulation 1286/2009, which amended EC Regulation 881/2002, later expanded the scope of the freezing measures to any "funds and economic resources belonging to, owned, held or controlled by a natural or legal person, entity, body or group that is listed in Annex 1 to the Regulation", thus allowing for a broad and unrestrictive application of the freezing measures also to funds and economic assets owned or controlled jointly by a designated and a non-designated person, entity or organization.

361. However, EC Regulation 881/2002 does not expressly cover "indirect" ownership or control over funds or economic assets and such reference is also not provided for in EC Regulation 1286/2009 or the EU Best Practices.

362. Situations in which a person is acting on behalf of or based on instructions from a designated person, entity or organization and thus allows the latter to indirectly control funds or economic resources would thus not be covered by the Regulation. This falls short of the international standard, which specifically requires the freezing measures under UNSCR 1267 to apply to "funds or other assets owned or controlled directly or indirectly" by a designated person, entity or organization.

363. Due to procedural and translation requirements, the European Commission takes a certain amount of time to update Regulation 881/2002 after the UN Security Council Committee lists a person, entity or organization. In previous years, this delay has ranged from ten days to two months. To ensure that freezing measures under UNSCR 1267 are nevertheless applied without delay in the Netherlands, the Dutch authorities through Sanctions Regulations may also apply temporary freezing measures with respect to funds and assets of individuals and entities that have already been designated under UNSCR 1267 but not yet been added on the list under EC Regulation 881/2002.

364. While the assessors acknowledge that the Dutch legal framework allows for the possibility to freeze without delay and thus to circumnavigate the time delay on European level, it is questionable how effectively the authorities have made use of this possibility in the past as it was indicated that in only one case Sanctions Regulations were issued to overcome the indicated time delay.

Freezing Assets under S/Res/1373 (c. III.2):

365. The Netherlands implement the financing of terrorism aspects of UNSCR 1373 through EC Regulation 2580/2001 with respect to individuals and entities linked to non-EU Member States (referred to

herein as non-EU residents) and various Sanctions Regulations issued based on Section 2 of the Sanctions Act with respect to EU residents.

366. Under the EC Regulation, all funds, financial assets and economic resources, however acquired, belonging to, directly or indirectly owned, controlled or held by a natural or legal person designated by the EU Sanctions Committee and listed in the annex to the Regulation are automatically frozen. The measure also applies to funds, financial assets and economic resources owned or held jointly by a listed person or entity and a non-designated one. Funds are frozen directly and immediately upon entry into force of the amendments to the Council Regulation. Infringements of the relevant provisions are penalized via national legislation, in particular, the Sanctions Regulation on Terrorism 2002.

367. With respect to EU residents, including Dutch residents, the Netherlands can apply freezing measures through Sanctions Regulations based on Article 2 of the Sanctions Act as outlined above. Article 2 of the Sanctions Act allows for such Regulations to implement international resolutions for fighting terrorism and thus is applicable to the same types of funds and assets as UN Security Council 1373. As indicated above, Sanctions Regulations issued by the Ministry of Foreign Affairs are applicable to both funds and other property held or controlled by designated terrorists or terrorist organizations.

368. To implement the provisions of the Sanctions Act, the Ministry of Foreign Affairs, the Ministry of Finance, the Ministry of Justice (the National Coordinator of Counter Terrorism), the Intelligence Service and the Public Prosecutor meet at least twice a year to discuss the status of existing freezing mechanisms and to review the appropriateness of possible new measures under the Sanctions Act, whereby evidence will be reviewed and advise be formulated for the Minister of Foreign Affairs whether a new freezing measure should be applied. Meetings can also be called on an ad hoc basis if needed. In 2009, four meetings were held.

369. A decision as to whether or not a freezing measure should be applied will be taken by the Minister of Foreign Affairs on the basis of “sufficient indications” of terrorism or terrorism financing activities for a court to uphold the decision in case of a challenge. The authorities indicated that “sufficient indications” would thus be more than mere suspicion. One important weighing factor in this regard is the impact of such measures on possible criminal investigations or prosecutions.

370. Once the decision to apply a new measure has been made, the agencies forming part of the above mentioned protocol informs the financial institutions of the freezing obligation. After that, the designation decision is published in the Dutch official journal and thus enters into force. The authorities stated that it would take about two weeks from the time a proposal for a decision is discussed between the agencies until publication of a decision by the Ministry of Foreign Affairs in the official journal. The designated individual or entity will only be informed of the measure after publication in the Official Journal. No prior notice is given.

371. Once a freezing measure based on the Sanctions Act has been taken, all financial institutions are instructed by the explanatory memorandum to the Regulation on Supervision Pursuant to the Sanctions Act to “ensure a timely check of its records” to prevent a dissipation of the financial assets prior to the freeze, whereby the institution may itself decide what exactly continues timely action given the services and products it offers. Representatives of the DNB further stated that in the past it had taken financial institutions about 2 business days from the day of publication of a Sanction Regulation to report any freezing measures taken on the basis thereof.

372. For persons and entities other than FIs and TCSPs, for example real estate agents and lawyers, there is no express obligation to check client databases for any matches with the Sanctions Regulations and no guidance has been issued with respect to the timeframe within which assets and funds must be frozen.

However, Article 4 of Regulation 2580/2001 requires bodies and persons other than banks and financial institutions to provide immediately any information which would facilitate compliance with the Regulation (such as accounts and amounts frozen in accordance with Article 2 and transactions executed pursuant to Articles 5 and 6) to the competent authorities of the Member States listed in the Annex and to cooperate with the competent authorities listed in the Annex in verifying this information.

Freezing Actions Taken by Other Countries (c. III.3):

373. For persons and entities designated through the EU regulations, the freezing mechanisms set out in the EU Regulations as explained above apply in the Netherlands. The authorities stated that EU Member States would generally opt to propose a specific person or entity for EU wide designation through the EU regulations rather than to request a freeze based on a Sanction Regulation.

374. However, where a foreign freezing measure relates to EU residents and therefore does not fall within the scope of EC Regulation 2580/2001, or where a request relates to a non-EU resident that has not yet been integrated in the lists under the EC Regulations, the Netherlands may apply freezing measures through Sanctions Regulations issued on the basis of the Sanctions Act. The process outlined above is used to examine a foreign request and, where appropriate, give effect to it by freezing any funds or assets located in the Netherlands. The authorities stated that in one instance, a Sanctions Regulation has been issued based on a foreign request.

Extension of c. III.1-III.3 to funds or assets controlled by designated persons (c. III.4):

375. As indicated above, the freezing mechanisms under the EU Regulations apply to a broad notion of financial assets and economic resources, however acquired, that belong to or are directly owned, controlled or held by designated persons or entities. The definition also covers funds derived from property owned or controlled by a designated person such as interest, dividends or other income on or value accruing from or generated by assets. This understanding is also confirmed by the EU Best Practices Paper relating to Restrictive Measures, which provides that “the freeze covers all funds and economic resources belonging to or owned by designated persons and entities, and also those held or controlled” by such persons (paragraph 28 EU Best Practices Paper).

376. While EC Regulations 1276/2001 expressly applies to all funds, financial assets and economic resources, however acquired, belonging to, directly or indirectly owned, controlled or held by a natural or legal person designated by the EU Sanctions Committee, EC Regulation 881/2001 does not expressly cover “indirect” ownership or control over funds or economic assets and such reference is also not provided for in EC Regulation 1286/2009 or the EU Best Practices. Situations in which a person is acting on behalf of or based on instructions from a designated person, entity or organization and thus allows the latter to indirectly control funds or economic resources would thus not be covered by the Regulation.

377. With respect to EU residents, Sanctions Regulations may be issued to implement international resolutions related to the furthering of the international rule of law, or to the fighting of terrorism, and could thus also be applied to the same type of funds and assets as UNSCR 1267 and 1373. Past freezing measures were issued with respect to both funds and other property held or controlled by designated terrorists or terrorist organizations.

378. The authorities stated that so far freezing measures resulted in the freezing of funds and also of insurance, pension claims, and real estate.

Communication to the Financial Sector (c. III.5):

379. Any Dutch person, whether natural or legal, including financial institutions and DNFBPs are required to comply directly with EC Regulations 881/2002 and 2580/2001, both of which are published in the Official Journal of the European Union. Infringements of the EC Regulations are penalized based on the Sanctions Act 1977. The authorities further stated that financial institutions would operate sophisticated IT systems which automatically update the relevant lists of designated entities and persons under the EC Regulations.

380. Moreover, as a service to financial institutions and others applying sanctions, the European Commission after amending the Annex to the relevant the EU Regulation enters the details of those listed in an electronic consolidated list of persons and entities subject to financial sanctions. The consolidated list includes all individuals, groups and entities subject to asset freezing in accordance with legislation based on the EC Treaty, so its contents goes beyond the lists made pursuant to Council Regulations (EC) No 2580/2001 and 881/2002, covering also persons and entities subject to other targeted sanctions decided on in the framework of the EU Council Common Positions. (It does not include the targets of asset freezing decided by an EU Member State.) The electronic consolidated list can be downloaded from the Commission website.

381. Sanctions Regulations based on the Sanctions Act are issued in the Dutch official journal. In addition, the Dutch Central Bank and the Authority for Financial Markets send circulars to all supervised financial institutions, TCSPs, and casinos to inform them of newly imposed freezing measures under the Sanctions Act. This circular is sent out once the decision to apply a new measure has been made and before the designation decision has been published in the Dutch official journal.

382. Pursuant to Section 10 of the Sanctions Act, financial institutions and TCSPs are supervised by the DNB and AFM for compliance with both the EC Regulations and the Sanctions Regulations. For such institutions and businesses, the Regulation on Supervision Pursuant to the Sanctions Act sets out a direct legal requirement to check any client, beneficiary of a transaction product, ultimate beneficiary of financial assets, correspondent banks, and any other party to a financial product or transaction against the lists under the EC and Sanctions Regulations. Section 3 of the Regulation further requires financial institutions to report any hits with any of these lists and furnish any relevant data in relation to the case to the AFM or the DNB, as the case may be.

383. Advocates are obliged on the basis of Article 7 of the By-Law on the Administration and Financial Integrity to satisfy the identity of the client and to check that there are no reasonable grounds to believe that the assignment may serve the preparation or support of or cover for illicit activities. Similar obligations exist for notaries based on the By-Law on Professional and Ethical Rules, which obliges notaries to verify the legal status of goods subject to compulsory registration. As part of this obligation, advocates and notaries have to check the names of customers against the lists set out under the EC Regulations and the Sanctions Regulations. Casinos fall under the Sanctions Act and the Regulation on Supervision Pursuant to the Sanctions Act through their money exchange permit and are supervised for this purpose by the DNB.

384. For real estate agents, there is no express obligation to check client databases for any matches with the Sanctions Regulations.

385. Overall, FIs the assessors met with were well aware of their obligations under both the EC and Sanctions Regulations and had received circulars with listed entities from the DNB. In practice, many institutions utilize external service providers to ensure that the client database is regularly checked against

the lists under the EC Regulations. It is unclear whether such service providers also integrate Dutch Sanctions Regulations into their databases.

Guidance to Financial Institutions (c. III.6):

386. The Dutch Central Bank provides general guidance on its homepage for persons who hold funds or economic resources that are subject to an asset freeze (http://www.dnb.nl/openboek/extern/id/en/all/41-161263.html). The guidance sets out the obligations under the various legal instruments as outlined above and advises financial institutions and TCSPs on how to report a 'hit' to the Dutch Central Bank. The guidance also makes clear that queries concerning asset freezing and questions about the identity of designated persons and entities can be addressed to the Central Bank. The authorities stated that questions directed to DNB would generally relate to the procedures applicable to identify possible terrorists, *i.e.* how to verify that the person in their client files is the same as the person on one of the lists.

387. In addition, the EU has issued a Best Practices Paper for the effective implementation of restrictive measures, which is available through the DNB homepage.

388. The explanatory memorandum to the Regulation on Supervision Pursuant to the Sanctions Act also sets out in great detail the requirements by financial institutions and TCSPs under the EC Regulations and the Sanctions Regulations. Furthermore the Ministry of Finance and DNB participate frequently in the sanctions working group of the bankers association, which meets about twice a year. To address any practical challenges in the implementation of freezing measures, the Ministry of Finance works closely together with the financial supervisors, the intelligence service and the bankers association on the basis of the Interagency Protocol outlined above. Both the Ministry of Finance and the DNB have designated points of contact for the private sector.

389. Based on meetings with private sector participants, however, the assessors gained the impression that there is still a certain level of uncertainty by persons or entities other than FIs or TCSPs as to what the obligations under the Regulations entail. In particular, no guidance specifically relevant to lawyers, accountants and notaries has been issued.

De-Listing Requests and Unfreezing Funds of De-Listed Persons (c. III.7):

390. The EC Regulations do not grant national governments autonomy in deciding to de-list persons or entities or to unfreeze funds and assets as a whole. As such, any freezing (whether pursuant to EC Regulation 881/2002 or 2580/2001) remains in effect until otherwise decided by the EU. Common Position 2001/931/CFSP of the European Union implements S/RES 1373(2001) and provides for a regular (at least bi-annual) review of the sanctions list which it has established. Moreover, listed individuals and entities are informed about the listing, its reasons and legal consequences. They are granted due process rights, including the possibility to present material which they consider sufficient for a delisting. If the EU maintains the person or entity on its list, the latter can lodge an appeal before the General Court of Justice of the EU in order to contest the listing decision. Requests by the Dutch Government for de-listing have to be directed through the Ministry of Foreign Affairs and its representative in the relevant UN or EU body to the UN Sanctions Committee or the European Commission, as the case may be.

391. Delisting from the EC Regulations may only be pursued before the EU courts. In the case of refusal of a request of delisting, the applicant can decide to have the matter presented to the European Court of First Instance and in second instance to the European Court of Justice. If the challenge is to the legality of a designation under the EC Regulations, the European Court of Justice of the EU can hear the complaint if made within two months after the designation.

392. Designations pursuant to the Sanctions Act can be challenged under the General Administrative Law Act (Awb). After a decision to designate has been issued in the Dutch Official Journal, the person affected by the decision is being notified of the freezing measures and is provided with information on how to initiate a de-listing request.

393. As a first step, the designated person can file an objection to the Minister of Foreign Affairs' decision to freeze funds and assets. In a hearing the person then has the possibility to explain his/her objection. The Minister of Foreign Affairs decides on the objection within six weeks or within twelve weeks in some circumstances. If no decision has been made within this timeframe or the decision was to deny the objection, the designated persons can contest the decision (or the absence thereof) before an administrative court in a hearing before one to three judges. The administrative court will decide on the appeal within four or in some circumstances within 12 weeks. Based on the administrative court decision, the designated person has the possibility to lodge an appeal with the Administrative Jurisdiction Division of the Council of State (*Afdeling bestuursrechtspraak Raad van State*). If at any step of this process the Minister's decision is lifted, the frozen funds or other assets will immediately be unfrozen. The Minister of Foreign Affairs will immediately thereafter inform the de-listed person or entity as well as the DNB or AFM of the court's decision to lift the freezing measure. The DNB or AFM will in turn inform the financial institutions and TCSPs. The authorities stated that so far, freezing measures under the Sanctions Regulations have been lifted with regard to nine individuals, seven of which were on an EU list.

Unfreezing Procedures of Funds of Persons Inadvertently Affected by Freezing Mechanism (c. III.8):

394. Due to the legal framework of freezing funds and assets through directly applicable EC Council Regulations, in a legal sense funds of persons that are not designated but bear, *e.g.*, a name identical to, very similar to or just resembling the name of a designated person, are not frozen in the Netherlands.

395. However, financial institutions may have blocked funds of such a person up until its identity is verified. In those cases, the person concerned as well as the financial institution may address the Ministry of Finance with a request to review the case. In cases where a reported freezing action is determined by the Ministry of Finance to not be an 'exact hit', the DNB or AFM will immediately communicate this finding to the relevant financial institution, which in turn will immediately 'unfreeze' the funds/assets.

396. Individuals and entities inadvertently affected by a freezing mechanism under the Sanctions Act may file an objection as previously described under III.7.

Access to frozen funds for expenses and other purposes (c. III.9):

397. UNSCR 1267, as amended by UNSCR 1452, is implemented in the EU through a new Article 2a in EC Regulation 881/2002, which is directly applicable in the Netherlands. This provision authorizes access to funds that are frozen for basic expenses, certain fees, or for extraordinary expenses. The Ministry of Finance is the designated competent authority to receive requests from affected persons for exemptions under the Regulations. Any request received is also notified to the Al-Qaida or Taliban Sanctions Committee which, within, 48 hours may object to the exemption. The competent authority must also promptly notify the person that made the request, and any other person, body or entity known to be directly concerned, in writing, whether the request has been granted or not. Before a request may be granted, the competent authority has to inform other Member States as well.

398. A procedure is also envisioned in Articles 5 and 6 of EC Regulation 2580/2001 which relates to designations emanating from UNSCR 1373. Under Article 5 the competent authority may grant a specific authorization to unfreeze funds for essential human needs under such conditions as it deems appropriate. Article 6 establishes a broader power for competent authorities of EU Member States to grant specific

authorizations, to protect the interests of the community and the interest of its citizens and residents and after consultations with the other Member States, the Council and the Commission of the EU.

399. Funds frozen under the Sanctions Act may be accessed based on an exemption granted through a unilateral decision of the Minister of Finance based on Article 9 of the Sanctions Act. The Ministry can use its competence both upon request of an interested party (the designated person or entity, but also third parties with a directly related interest) and by virtue of its own office. These procedures are in accordance with S/RES/1452(2002). The authorities explained that a petition for exemption would be submitted to the Ministry of Finance, explaining why the exemption is requested and providing proof of the actual existence of the relevant claims or expenses. The authorities stated that about 20–30 exemptions have been granted in the past, whereby with respect to each freezing measure multiple exemptions may be granted.

400. Decisions by the Minister of Finance with respect to exemptions are subject to legal review by the administrative courts as outlined under criterion 7 above.

Review of Freezing Decisions (c. III.10):

401. As mentioned above, the freezing mechanisms in the relevant EC Regulations can be challenged at the European Court of Justice by any natural or legal person that is directly and individually affected under the general principle established by Article 230 of the Treaty on the functioning of the EU.

402. A number of appeals against freezing orders based on Council Regulations (EC) No. 2580/2001 and 881/2002 are pending in the European Court of Justice. The appeals focus on claims that the human rights of the designated individuals, groups, and entities were not respected. As regards Council Regulation (EC) No. 2580/2001, the Court of First Instance held in three judgments in 2006 and 2007 (T-228/02, People's Mujahedin of Iran (OMPI), T-47/03, Sison, T-327/03, Stichting Al Aqsa) that the Council had to provide a statement of reasons to the designated individuals, groups and entities concerned, so as to allow them to make their views known on it and to allow the court to conduct a review. These judgments are final. The Court of First Instance upheld this line of argument on April 3, 2008 in the cases T-229/02 and T-253/04, Kurdistan Workers' Party (PKK) and Kongra-Gel, which concern Council decisions made in 2002 and 2004.

403. On September 3, 2008, the European Court of Justice issued a judgment in the Kadi and Al Barakaat International Foundation cases (C-402/05 P and C-415/05 P) that annulled the 2002 EU Council regulation that implements UNSCR 1267 and successor resolutions insofar as the regulation concerned the appellants. However, the Court, in essence, left the EU regulation in place for up to three months to permit the European Commission to remedy the violations found by the Court. The Court found violations of fundamental human rights, specifically, the right of defense and the right to an effective legal remedy. In December 2009, the EU issued EC Council Regulation 1286/2009 amending Regulation 881/2001 to ensure compliance with the judgment of the European Court of Justice.

404. For freezing mechanisms under the Sanctions Act, the review procedures as outlined under criterion III.7 are available. The authorities stated that so far, freezing measures under the Sanctions Regulations have been lifted in one case.

Freezing, Seizing, and Confiscation in Other Circumstances (applying c. 3.1-3.4 and 3.6 in R.3, c. III.11)

405. In the context of domestic criminal investigations, seizing measures pursuant to Article 94 and 94a can be used to restrain instrumentalities and proceeds of TF and terrorism offenses. For further detail on this issue see the analysis section under Recommendation 3 above.

Protection of Rights of Third Parties (c. III.12):

406. The rights of bona fide third parties affected by a freezing measure under the EC Regulations, the Sanctions Regulations, or a seizure otherwise ordered in the Dutch system are protected by the relevant EC Regulation as well as by the general principles of Dutch law.

407. In relation to freezing measures imposed through Regulation 881/2002 or 2580/2001, bona fide third parties may institute proceedings before the European Court of Justice. EC Regulation 881/2002 through Article 6 also protects natural or legal persons that freeze assets or funds in good faith. The provision does, however, not protect negligence.

408. If the freeze has been undertaken pursuant to a Sanction Regulation under the Sanctions Act or a bona fide third party is adversely affected by the EC Regulations, a challenge based on the Dutch administrative law as outlined under criterion 7 above can also be brought.

Enforcing the Obligations under SR III (c. III.13):

409. Both Article 10 of the Council Regulation (EC) No. 881/2002 and Article 12 of the Council Regulation (EC) No. 2580/2001 oblige Member States to lay down rules on sanctions applicable to infringements of the provisions of the respective Council Regulation and ensure that they are implemented. Those sanctions must be effective, proportionate and dissuasive. The penalty for violation, circumvention, or attempted violation or circumvention, of Council Regulations 2580/2001 and 881/2002 is a term of imprisonment of up to five years (see Section 34(4) of the FTPA). Negligent violations are sanctioned with imprisonment of up to three years or fines (see Section 34(7) of that Act). The Council Regulations also establish certain communication and notification requirements to the competent authorities of the Member States, concerning information that can guarantee compliance as far as frozen accounts and amounts are concerned. Failure to comply with the reporting obligations is an administrative offense.

410. Article 10 of Sanctions Act and the Regulation on Supervision pursuant to the Sanctions Act designate the DNB and AFM as the relevant authorities to ensure compliance by FIs and TCSPs with the obligations under the Sanctions Act, any Sanction Regulations issued on the basis thereof and with the requirements under the EC Regulations. Pursuant to the Regulation on Supervision pursuant to the Sanctions Act, financial institutions and TCSPs are required to have internal administrative and control systems in place to enable the institution to comply with all requirements deriving from the above mentioned laws and regulations for example by screening all customer relations for a match with the lists under the EC Regulations, informing the DNB or AFM of any hits and keeping records of any such notification and underlying data for a period of five years after the designation. The DNB and AFM also have the power, based on the Sanctions Act 1977, to impose administrative fines and to issue “cease and desist” orders for failure to comply with such the Sanctions Act, Sanctions Regulations issued on the basis thereof or the obligations under the EC Regulations.

411. Furthermore, the Dutch Customs Authority has the power to control the import, transit and export of the goods, including money and related goods that are subject to any sanction measures.

412. Pursuant to Section 13 of the Sanctions Act, Dutch nationals who commit an act under the Sanctions Act may be held criminally liable. Although criminal sanctions have not been applied under the Sanctions Act in relation to violations with obligations to freeze the funds of designated individuals or entities, the Public Prosecutor has recently indicted several individuals for violation of the Sanctions Act in relation to a listed entity.

413. Representatives of the DNB stated that onsite inspections exercises would in all cases involve an examination of the various procedures in place to ensure compliance with the Sanctions and EC

Regulations, a verification that senior management is aware of the latest lists of entities and persons and a sample testing to see whether certain names on the list should have resulted in a report to the supervisor. The DNB stated that, following audits held in the first quarter of 2010, in two cases FIs have been considered not to be in compliance with the EC Regulations and the Sanctions Regulations because the FIs did not check their client database against these lists on a regular basis. In both cases, sanctions are being considered.

414. The extent to which supervisory activities carried out by the AFM include monitoring for compliance with the EC Regulations and the Sanctions Regulations is less clear. In fact, the assessors could not establish that onsite monitoring exercises address these Regulations at all and which mechanisms are used by the AFM to evaluate FI compliance with the Regulations. The AFM has never detected or applied sanctions for non-compliance of supervised entities with the Sanctions Regulations.

415. The authorities confirmed that DNFBPs other than TCSPs are not subject to monitoring by specific supervisory body under the Sanctions Act. The FIOD-ECD as a general supervisory body and investigation service in the area of financial integrity could in theory carry our supervision in relation to DNFBPs to ensure compliance with the EC and Sanctions Regulations. Furthermore, the lawyer's association could use its disciplinary sanctioning powers in relation to lawyers and notaries that fail to comply with the provisions of the EC or Sanctions Regulations. From meetings with the private sector it does not seem that in practice the FIOD-ECD and lawyers association have made use of their power in this area. Casinos are subject to the monitoring mechanisms under the Sanctions Act through their money exchange permit.

416. Violations of the Sanctions Regulations or the EC Regulations may be sanctioned as economic offenses based on Articles 1 and 6 of the Economic Offenses Act. The statutory sanctions available include a prison sentence, community service or a fine. In addition, for TCSPs and casinos administrative sanctions may be imposed by the DNB or AFM.

Additional Element (SR III)—Implementation of Measures in Best Practices Paper for SR III (c. III.14):

417. The authorities indicated that they have implemented the best practice paper for SR.III by way of the EU and domestic legislation described earlier in this section and that they fully cooperate with foreign jurisdictions.

Additional Element (SR III)—Implementation of Procedures to Access Frozen Funds (c. III.15):

418. See discussion under criteria 9.

Statistics (R.32):

419. The DNB maintains statistics on the reported freezing actions by financial institutions and gives an overview of the number of reports in its Annual Report. Since 2002, freezing measures were applied with respect to funds and other economic assets with respect to twenty-one subjects, whereby five of those subjects were legal persons. In most cases the freeze related to bank accounts. Some cases also involved pension rights and health insurance claims. One case involved real estate. Other property of designated individuals or entities has so far not been identified in the Netherlands.

420. In total, EUR339 382 are frozen in the Netherlands pursuant to the obligations under UNSCR 1267 and 1373. The majority of funds were frozen based on a domestic Sanctions Regulation, whereby in a significant number of cases the relevant person or entity was later added to the list of

designated persons under EC Regulation 2580/2001. In three cases were freezing measures applied pursuant to EC Regulation 881/2002.

Total of Reports received by DNB pursuant to the EC and Sanctions Regulations	
2004	40 reports
2005	14 reports
2006	6 reports
2007	18 reports
2008	30 reports
2009	21 reports
2010 (till July)	17 reports

Analysis of effectiveness

421. The Netherlands have a strong and comprehensive framework in place to implement its obligations under UN Security Council Resolutions 1267 and 1373 and in a number of cases have effectively applied this framework to freeze the funds and assets of designated terrorists and terrorist organizations. The most important financial sectors are effectively supervised for compliance with their obligations under the EC and Sanctions Regulations and the procedures in place ensure that freezing measures are effectively communicated to the private sector. Merely some technical deficiencies have been identified as outlined in the analysis section above. Some concerns remain as to whether funds and assets are frozen without delay in all cases.

2.4.2 Recommendations and Comments

- Provide more guidance to the private sector, especially the non banking financial industry and DNFBPs, on the freezing obligations stemming from the international standard, including the obligation to check client files and databases against those lists.
- Ensure that all FIs, not only banks, are effectively monitored for compliance with the EC and Sanctions Regulations.
- Extend the freezing obligations under UNSCR 1267 to funds and other assets owned or controlled "indirectly" by a designated individual, entity, or organization.
- Ensure that funds and assets are frozen without delay in all cases.

2.4.3 Compliance with Special Recommendation III

	Rating	Summary of factors underlying rating
SR.III	**LC**	• There is insufficient guidance for persons and entities other than FIs that may be holding targeted funds or assets regarding the freezing obligations stemming from the international standard, including the obligation to check client files and databases against those lists. • FIs other than banks are not always sufficiently supervised for compliance with the EC and Sanctions Regulations. • The freezing obligations under EC Regulation 881/2001 do not expressly extend to funds and assets that are owned or controlled "indirectly" by a designated individual, entity, or organization. • Concerns remain as to whether funds and assets are frozen without delay in all instances.

Authorities

2.5 The Financial Intelligence Unit and its Functions (R.26)

2.5.1. Description and Analysis

***Legal Framework*:**

Foreword

422. The Dutch Financial Intelligence Unit was first established in 1994 as a "Disclosures Office" (*Meldpunt ongebruikelijke transacties* -MOT), pursuant to Article 2 of the Disclosure of Unusual Transaction Act (Act of 16 December 1993), an administrative-type FIU under the Ministry of Justice (MoJ). According to the 1993 law, the MoJ was responsible for the overall management organization and administration of the MOT.

423. With a view to enhance the use of financial information "at the heart" of the law enforcement community, the Netherlands decided in 2005 to place the MOT in the Netherlands Police Agency (hereinafter KLPD) under the Ministry of Interior (MoI) and with the goal to create a new structure, the FIU-Netherlands (hereinafter: FIU-NL), consisting of the MOT and of the Office for Police Support of the national officer of Justice (BLOM, a law enforcement unit established under the National Public Prosecutor, "for cases involving suspicious transactions", specialized in the investigation of ML cases and also relocated within the KLPD, prior to MOT's relocation).[58]

424. The new structure was established as an "umbrella organization" in the KLPD pursuant to an order of the MoJ of December 13, 2006 ("establishment decision"). The Minister of Justice maintained the legal responsibility for the overall management, organization and administration of the MOT, but delegated it to the Minister of Interior ("delegation decision" of October 13, 2006). The new structure was meant to operate in a "test phase" and in a "project form", at the end of which (July 2008) a decision on the final merger between MOT and BLOM and on a definitive transfer of responsibility for the management of the MOT from the MoJ to the MoI should have been taken, based also on the results of an "evaluation study", commissioned by the MoJ and conducted by an independent firm between May and September 2008 (the major findings of the study are discussed under criterion 26.6 and in the effectiveness section). In July 2008, when the agreement expired, the authorities agreed informally to extend the duration of the expired agreement until a new one was in place. A new delegation of authority concerning the MOT was adopted, following which appropriate changes in the legal framework should have followed to finalize the merger between the MOT and BLOM and the transfer of responsibilities.

425. The new AML/CFT law (WWFT, which entered into force on August 1, 2008 and replaced the 1994 AML law) confirmed the responsibility of the MoJ for "overall management, organization and administration of the FIU" (Article 13).

426. A new management agreement between the MoJ and the MoI was drafted in January 2009 (with a view to replacing the 2006 one, which expired on July 1, 2008 and addressing the main findings and recommendations of the evaluation study) and a new governance model for the FIU-NL designed. The authorities planned to finalize the merger between MOT and BLOM into the FIU-NL by the fall of 2009,

58 The decision was a follow up to the Dutch government's policy plan adopted in response to the 2004 Research and Documentation Centre (WODC) report "From an unsuspicious source–Evaluation of the chain of unusual money transactions."

as indicated in the MoJ Letter to the Head of the FIU-NL[59], containing the policy objectives for the year 2010. The Parliament was informed about the relevant ministries' intention not to undo the project organization, as well of the intention to place definitively the MOT into the KLPD.

427. However, at the time of the onsite visit, the finalization of the merger between MOT and BLOM had not yet taken place and the NL-FIU was still operating in a "project form". Nor had the January 2009 draft management agreement been signed, although it had been drafted for more than one year, because of disagreements between the MoJ and the MoI, including over the responsibility of the management of the UTR database and the level of security of the UTR database (the issue will be discussed more in detail later).

428. After the onsite visit, on September 8, 2010, the Minister of Justice issued a decree to amend the two 2006 establishment and delegation decisions with a reference to the WWFT's "*Meldpunt ongebruikelijke transacties"* (MOT) in the articles of these decisions that refer to the "FIU-Netherlands". The Decree entered into force on September 22, 2010. The Explanatory Notes of the Decree note the decision to merge MOT and BLOM definitively and state that these amendments anticipate a legislative proposal to change the law "which would anchor the positioning of FIU-Netherlands in the law".

429. Another development that occurred after the onsite visit, on September 10, is that a new Management Agreement for the FIU-Netherlands was signed by the MoJ and the MoI. The Management Agreement foresees that the management of the FIU-Nederland "will" be handed over to the Minister of the Interior and Kingdom Relations and that thereby the general management, the organization and the management of the *Meldpunt ongebruikelijke transacties* MOT "will be" mandated from the Minister of Justice to the Minister for the Interior and Kingdom Relations. The mandate provided "will" then be delegated to the manager of the KLPD. The management agreement also states that "That the Minister of Justice, in consultation with the Minister of Finance, will put forward a proposal to amend the WWFT with the purpose of changing the legal framework to the new situation, whereby the *Meldpunt ongebruikelijke transacties*-MOT and the BLOM are definitively merged to form FIU-Nederland and that the FIU-Nederland is housed with the KLPD, with due regard for national and international legislation, including the FATF (Financial Action Task Force) Recommendations."

430. To date, the changes to the law referred to in the Minister of Justice Decree of September 8 and the Management Agreement as well as the final transfer of responsibilities for the FIU-Netherlands from the MoJ to the MoI[60] have not yet taken place.

Establishment of FIU as National Center (c. 26.1):

431. Article 12 of the WWFT establishes that a Reporting Point for Unusual Transaction (*Meldpunt ongebruikelijke transacties*-MOT) "shall be in place." Article 13 of the WWFT establishes the functions of tasks of the FIU "with the view to the prevention and detection of money laundering and terrorist financing". These tasks include the core functions of the FIU envisaged by Recommendation 26 and, specifically:

59 "It is expected that in the autumn the Ministers of Justice and of Finance, in consultation with the Minister of interior, will decide to merge the MOT and the BLOM. The new agency will be known as FIU-Netherlands and, for administrative purposes, will fall under the Dutch Police Services Agency's International Police Intelligence Department (KLPD/IPOL)".

60 The authorities informed the mission that, as result of the new government in place since October 2010, the Ministry of Justice (renamed Ministry of Security and Justice) has the overall responsibility (including the managerial one) for the Police (and that includes the KLPD and the FIU). This change will likely affect the new management agreement which was signed on September 10, 2010, at a time in which the MoI had responsibility over the Police and the FIU.

- "To gather, register, edit and analyze the data that it obtains, in order to determine whether this data may be relevant to the prevention and detention of crimes" and "investigate developments in the area of money laundering and terrorist financing and the improvement of the methods to prevent and detect money laundering and terrorist financing" ("**receiving**" and "**analysis**", Article 13 (a)).

- "To pass on personal data and other information in accordance with this Act (the WWFT) and the provisions laid down in or pursuant to the Police Data Act" ("**dissemination of STR and other relevant information regarding potential money laundering or terrorist financing**" function, Article 13 (b)).

432. In addition to the FIU's core functions envisaged by Recommendation 26, the FIU is also responsible to provide feedback to the institutions that made a disclosure of an unusual transaction (for the discussion of unusual transaction reporting-UTR, see analysis under R.13); to issue recommendations to the business sectors on the introduction of appropriate procedures for internal control and communication of other measures to be taken to prevent ML and FT, including the provision of information for prevention/detection purposes to business sectors and professional groups, the supervisors and the general public; and to provide information on the "disclosure behavior" of the reporting entities to the competent supervisory authorities.

433. The FIU is the national centre for the performance of the above mentioned tasks, in the case of money laundering and terrorist financing, as clearly stated by Article 13.

434. With regard to the FIU's "receiving" task, this, as explained under the analysis of R.13, concerns "unusual transaction reports" received from the institutions subject to the WWFT, on the basis of "objective" and "subjective" indicators. For the purpose of the assessment of R13, only the UTRs filed under the "subjective indicators" are considered as amounting to "suspicious transaction reports". Throughout the analysis of R.26, reference will be made to "UTR"s to indicate suspicious transaction reports in the sense of R.13 (i.e. the subjective indicators) and "other information regarding potential money laundering or terrorist financing"—*i.e.* "objective indicators and the other reports that the FIU receives from other public bodies. With regard to the latter, the FIU receives data from the Customs on the cross-border transportation of cash (by virtue of the EC Regulation 1889/2005 and a 2007 agreement with the Customs); from the Tax authorities (upon authority and on a voluntarily basis); from the Supervisory authorities (pursuant to Article 25 of the WWFT) and by "Government administration" (upon authority and on a voluntarily basis).

435. It has also to be noted that, with regard to the institutions' obligation to report UTRs, the Explanatory Memorandum to Article 16 WWFT (UTR-obligation) explains that when there is a "strong suspicion" of ML and TF it is possible to report such "urgent" disclosures also to the Police "at the same time." The FIU confirmed that it receives copies of these reports, which are classified under a special code and analyzed as in the case of the other information received pursuant to the WWFT. The authorities and the financial institutions met by the assessors explained that these cases of "strong suspicions" amount to a situation closer to "awareness of a crime being committed", and indicated that in these circumstances general principles of Dutch law require that the Police should be notified.

436. Please refer to the section on effectiveness for a more detailed explanation and analysis of the characteristics of the receiving and analysis process of the UTRs and the dissemination to law enforcement. It suffices to say here that the UTRs, as a result of the analysis, may be classified by the FIU as Suspicious Transaction Reports-STRs and loaded into a database, the access to which, unlike the UTR database, is granted to law enforcement agencies.

Guidelines to Financial Institutions on Reporting STR (c. 26.2):

437. Article 18 of the WWFT empowers the FIU to "determine the manner in which a disclosure must be made", including with regard to requests of additional information. Article 14 (2) of the WWFT states that "rules shall be laid down by order in council about the categories of persons whose data is processed by the FIU's, the provision of data, the retention and destruction of data and the protocol requirement." The Minister of Justice, in consultation with the MoF would be the responsible authority to issue this order, but, to date this power has not been exercised.

438. The FIU provides guidance on the manner of reporting and on the procedures to be followed when reporting, and has issued a reporting regulation that also includes the specification of a reporting form. The FIU' website contains a section on "reporting", which specifies who is subject to reporting, including registration to the website and download of a software (MOT-explorer) that allows reporting online to the FIU. MOT-Explorer also contains a manual that explains, inter alia, reporting procedures. Codes are provided to the reporting institutions for the classification of the transactions based on the subjective/objective indicators.

Access to Information on Timely Basis by FIU (c. 26.3):

439. The FIU has access to financial, administrative and law enforcement information, although there is no specific power laid down in the WWFT or in any other regulation for the FIU to request such information (except to reporting institutions). There are rules, laid down in the Police Act, that allows the provision of Police-related data to certain institutions/officials for the performance of the tasks attributed to these institutions/officials: this is the case of the MoJ "for the performance of the tasks of the Office for the Disclosures of Unusual transaction (*i.e.* the MOT) and to "the persons employed by the Office for the Disclosures of Unusual transaction for the task of this office as referred to in Article 13 of the WWFT (which sets out the FIU's responsibilities)," pursuant to Articles 4.3.1.a., and 4.6.c, respectively, of the Police Data Act.

440. In addition to information maintained in various Police database (the VROS, which contains arrests, criminal records, and criminal intelligence files and the "Blueview" that allows consultation of enforcement updates and investigation information) the FIU-NL has access to a wide range of information, both from "closed" sources—fiscal information, income, assets, turnover of companies, imported/exported goods, through the 4 liaison officers of FIOD operating within the FIU–and from publicly accessible database (such as the Commercial Register, the Cadastre and the Public Service for Road). The FIU has also signed several agreements with public bodies for the exchange of information (with the Tax and Customs administration, with FIOD-ECD, the real Estate Information Centre, the FINEC program and BOOM). The following table illustrates in detail the additional information the FIU has access to, broken down per type of information that can be accessed directly" or upon request.

441. Access to information is timely (as most information is directly accessible and available through the consultation of the above mentioned databases) and enables the FIU to properly undertake its tasks, except when the request of information needed by the FIU leads to a disclosure of UTR-related personal data, which is classified as "secret". I f the FIU needs information (*e.g.* on a certain individual/company) which cannot be obtained otherwise (*e.g.* through access to a database), and the request of such information would lead to the disclosure of UTR-related information (*e.g.*: the name of the person involved in a UTR), the information cannot be requested/obtained. As discussed with the FIU, this is the case for convictions (as the VROS does not contain such information) and for the information on the Commercial Register that is not available on line (such as in the case of the companies' shareholders, which is only in the situations in which a single shareholder holds 100 percent of the shares; although in this situation the FIU stated that,

with some safeguards, the information could be obtained, albeit that would require an onsite visit at the Commercial Register).

Systems and sources FIU-Netherlands
Direct accessible
* Motion: Consulting unusual transactions
* Winston: Consulting suspicious transactions, national public prosecutor requests, other requests and FIU investigations
* HKS: Consulting antecedents
* RDW: Consulting vehicle registration holders, driver's licences and vehicles
* OPS: Consulting national alerts and unpaid fines
* NSIS: Consulting international alerts
* GBA: Consulting municipal personal records database
* KVK: Consulting Chamber of Commerce
* Kadaster: Consulting property and owners
* Lexis Nexis: Consulting international companies and newspapers/magazines
* Blueview: Consulting enforcement updates and investigation information
* BVO: Consulting serious-crime information and (current) investigations
* Internet: Consulting all relevant information
* IPS/Mars: Consulting requests for legal assistance, Interpol messages and serious-crime information
* VDS: Consulting incidents involving weapons
* VIP: Consulting sentences of individuals
* FCM: Consulting photographs of subjects
* BVR: Consulting first taking up residence in the Netherlands
Indirect accessible
* CJIB: Consulting penalties and fines by individual and by registration number
* GRIP: Consulting information about prisoners (*e.g.* visitors' lists)
* BDD : Consulting detention history
* Buro Documenten van IND: Consulting aliens documents
* FIOD: Consulting tax information
* Luris: Consulting international legal aid
* DIC: Consulting Customs files (import/export etc.)
* KMAR: Consulting authenticity of documents
Table 1. Indirect accessible (upon request of the National Public Prosecutor)
***** Compass: Consulting convictions
* KVK: Consulting Chamber of Commerce

442. Access to Customs information related to the cross-border transportation of cash is not entirely adequate. The FIU only receives the data from the declarations (which is not always accurate, as the information is loaded manually by Customs into their database from the hand-written declarations, so errors are frequent).

Additional Information from Reporting Parties (c. 26.4):

443. The WWFT clearly establishes the power of the FIU-Netherlands to request additional information from reporting entities (Article 17 (1)). This power is not only limited to the reporting institution that has made the disclosure of an UTR, but clearly extended to any institution "involved in a transaction about which the FIU gathered data" in order to assess whether the data gathered should be disseminated to LEAs. Article 17 (2) provides for the obligation of the requested institution to provide such data, within the deadline established by the FIU, in writing or verbally in urgent cases. Noncompliance to such obligation is subject to a fine, pursuant to Article 27 WWFT. The FIU-Netherlands explained that it has encountered no difficulties in obtaining such additional data, including from professions that are subject to privilege (except that this power was not tested but in one case concerning a lawyer). Despite the straightforward language of the law the representatives from the Bar association and some private lawyers with whom the mission met held a different opinion, and considered that the FIU-Netherlands has no power to obtain additional information held by a lawyer. However, the representatives of the Chamber of notaries met by the mission—notaries have same legal privilege as lawyers—confirmed that legal privilege would not impede the FIU to request additional information pursuant to the WWFT and needed for the analysis of an UTR. For a more detailed discussion on the provision of information covered by legal privilege please refer to R.13.

Dissemination of Information (c. 26.5):

444. The legal basis for the FIU to disseminate information is laid down by Article 13 b) and f) (3), described above. For a detailed description of the analysis of UTRs see the implementation/effectiveness section. The analysis of UTRs consists mainly of matching the UTR information with other information the FIU has access to. In this case the UTR is classified as an STR and loaded into the STR database, which can be accessed by Law Enforcement authorities for criminal investigations concerning any crime, not only ML/FT. The authorities explained that the rationale of the process for the substantiation of an UTR into an STR is to determine whether the transaction-related information is "relevant" for law enforcement authorities and to establish a link between the transaction and criminal activities, hence the loading of the information into a database that can be accessed by law enforcement authorities. This task represents the most common way in which in practice the FIU is disseminating the information. In addition to this modality, there are also other ways, in which the information is pro-actively disseminated to law enforcement agencies. Six officials in the BLOM unit (so called "account managers") are responsible for Police at regional level, to whom they provide specific STR-related information of suspects operating in a certain area; 4 liaison officers of the FIOD operate within the BLOM; when STRs are linked to organized crime the National Crime Squad is informed by the account managers assigned to follow cases that follow within the responsibility of the National Crime Squad. STR-related information and cases are also discussed in the context of the financial expertise centre and the Supervisory authorities meeting (on a quarterly basis). Team leaders, who, across MOT/BLOM follow more complex cases are also involved in the dissemination of information to law enforcement authorities. Cases related to TF are also disseminated to the National Crime Squad, with copy to the National Security Service.

445. The FIU explained that law enforcement authorities do not provide information as to whether queries to the STR database result or not in the opening of a criminal investigation. The FIU can determine, however, when STR-related information is used for an "official report": a law enforcement user can request individuals or transaction-related information and draw up an official report (OR). Such an 'official report' (*proces verbaal*) is used in criminal court proceedings and is regarded as legal evidence. An 'official report' can trigger a new criminal investigation (*start process verbaal*) but can also be part of evidence in an ongoing investigation. Hence a distinction cannot be made between 'official reports' that have triggered new criminal investigations and 'official reports' that are part of an ongoing investigation.

Also, these queries that generate an "official report" can be done in the context of an investigation of crimes other than ML or FT.

446. The table below shows the STR database searches per investigation service.

Use of STR database by law enforcement (IVT)												
Year	2009				2008				2007			
Investigation Service	*Detail*	*OR*	*R*	*Total*	*Detail*	*OR*	*R*	*Total*	*Detail*	*OR*	*R*	*Total*
KENNEMERLAND	*11.872*	*100*	*184*	*12.156*	*3.443*	*37*	*229*	*3.709*	*2.726*	*106*	*203*	*3.035*
FLEVOLAND	*2.042*	*25*	*159*	*2.226*	*3.132*	*16*	*205*	*3.353*	*3.108*	*13*	*261*	*3.382*
GELDERLAND-MIDDEN	*717*	*40*	*255*	*1.012*	*1.857*	*37*	*943*	*2.837*	*1.054*	*35*	*389*	*1.478*
HOLLANDS MIDDEN	*1.181*	*66*	*85*	*1.332*	*1.316*	*42*	*319*	*1.677*	*1.592*	*110*	*304*	*2.006*
IJSSELLAND	*1.038*	*105*	*158*	*1.301*	*1.115*	*38*	*344*	*1.497*	*924*	*30*	*180*	*1.134*
ROTTERDAM-RIJNMOND	*18.879*	*551*	*344*	*19.774*	*13.901*	*556*	*380*	*14.837*	*23.511*	*422*	*320*	*24.253*
KLPD	*15.407*	*259*	*661*	*16.327*	*15.281*	*255*	*882*	*16.418*	*10.540*	*195*	*420*	*11.155*
KMAR	*8.258*	*188*	*304*	*8.750*	*3.957*	*51*	*406*	*4.414*	*1.665*	*40*	*179*	*1.884*
UTRECHT	*3.991*	*70*	*214*	*4.275*	*5.898*	*18*	*542*	*6.458*	*3.281*	*87*	*192*	*3.560*
MIDDEN- EN WEST-BRABANT	*3.266*	*10*	*113*	*3.389*	*6.762*	*41*	*129*	*6.932*	*4.505*	*37*	*102*	*4.644*
AMSTERDAM-AMSTELLAND	*4.902*	*116*	*126*	*5.144*	*3.215*	*68*	*51*	*3.334*	*1.389*	*11*	*33*	*1.433*
BOOM	*3.581*	*8*	*68*	*3.657*	*4.765*	*2*	*5*	*4.772*	*0*	*0*	*0*	*0*
HAAGLANDEN	*3.265*	*134*	*157*	*3.556*	*2.566*	*64*	*116*	*2.746*	*5.326*	*226*	*202*	*5.754*
BRABANT-NOORD	*2.847*	*18*	*112*	*2.977*	*1.687*	*14*	*239*	*1.940*	*1.456*	*4*	*259*	*1.719*
NOORD-HOLLAND-NOORD	*1.258*	*73*	*49*	*1.380*	*3.131*	*114*	*85*	*3.330*	*1.558*	*112*	*69*	*1.739*
FIOD	*1.634*	*0*	*0*	*1.634*	*2.564*	*0*	*0*	*2.564*	*1.513*	*0*	*0*	*1.513*
ZUID-HOLLAND-ZUID	*947*	*19*	*51*	*1.017*	*3.004*	*78*	*69*	*3.151*	*2.287*	*7*	*194*	*2.488*
GRONINGEN	*857*	*13*	*49*	*919*	*2.922*	*86*	*88*	*3.096*	*1.721*	*22*	*26*	*1.769*
ZEELAND	*803*	*5*	*210*	*1.018*	*1.569*	*12*	*855*	*2.436*	*628*	*9*	*253*	*890*
NOORD- EN OOST-GELDERLAND	*1.014*	*32*	*183*	*1.229*	*1.295*	*11*	*623*	*1.929*	*838*	*58*	*251*	*1.147*
TWENTE	*910*	*13*	*244*	*1.167*	*1.266*	*60*	*321*	*1.647*	*767*	*36*	*191*	*994*
BRABANT-ZUID-OOST	*765*	*8*	*81*	*854*	*805*	*38*	*34*	*877*	*761*	*13*	*95*	*869*
ZAANSTREEK-WATERLAND	*416*	*21*	*27*	*464*	*958*	*121*	*81*	*1.160*	*1.220*	*43*	*136*	*1.399*
LIMBURG-NOORD	*676*	*10*	*78*	*764*	*831*	*3*	*25*	*859*	*420*	*10*	*92*	*522*
LIMBURG-ZUID	*730*	*41*	*22*	*793*	*658*	*22*	*108*	*788*	*1.397*	*42*	*46*	*1.485*
SIOD	*830*	*16*	*322*	*1.168*	*265*	*3*	*120*	*388*	*402*	*140*	*22*	*564*
GELDERLAND-ZUID	*782*	*8*	*324*	*1.114*	*321*	*4*	*99*	*424*	*137*	*18*	*32*	*187*
FRIESLAND	*300*	*5*	*150*	*455*	*635*	*3*	*401*	*1.039*	*866*	*7*	*247*	*1.120*
DRENTHE	*527*	*8*	*57*	*592*	*740*	*44*	*32*	*816*	*671*	*15*	*14*	*700*
GOOI EN VECHTSTREEK	*182*	*4*	*95*	*281*	*161*	*1*	*103*	*265*	*166*	*0*	*93*	*259*
NR-MIDDEN NEDERLAND	*0*	*0*	*0*	*0*	*368*	*7*	*10*	*385*	*233*	*4*	*14*	*251*
TOTAL	93.877	6.848	4.882	100.725	90.388	9.690	7.844	100.078	76.662	6.671	4.819	83.333
explanation:												
DETAIL: query on subject or transaction information, result watched 'on screen', total number												
OR: query on subject or transaction information, result transformed into an 'official report' (see text), total number												
R: query on subject or transaction information, result transformed into a report, total number												

447. The FIU could not indicate the number of new criminal investigations that were triggered by the UTRs that are "transformed" in STRs and loaded in the STR database, including for those that are loaded

in the STR database separate investigation module. Hence, it is not possible to establish the ratio of ML/FT related new criminal investigations vis-à-vis the number of UTRs that are transformed into STRs.

448. The tables below indicate the number of cases which were "disseminated" by the six account managers and the "ongoing investigations". The authorities explained that in the STR database there is a separate investigations module. This module registers all cases on related suspicious transactions that have been provided to law enforcement by the operational account managers of the Dutch FIU. A case file contains transaction-related information, and it is not a criminal case.

Year	No. Cases-files disseminated by account managers
2007	5 470
2008	8 151
2009	3 342
2010	1 894

Year	No. Cases-files disseminated by account managers Ongoing Investigations
2007	761
2008	667
2009	598
2010	396

449. The authorities also explained that the figures in the second table do not differentiate between ML/FT cases or investigations of other criminal offences. They only show instances in which the information in the STR database investigation module was used in the context of (any) criminal investigations, which could be for crimes other than ML/FT. Hence, it is not possible to determine, from the cases in which this information is used in the context of a criminal investigation, how many of such criminal investigations concern ML/FT.

Operational Independence (c. 26.6):

450. The FIU governance model is quite complex, and—in accordance to a Dutch tradition of public governance which values the sharing of responsibilities among public agencies/government as a way to enhance coordination among parties who may have a common interest in a certain area—sees the involvement of several institutions/officials, at policy and management level. This model became more complex when the FIU was placed in the MoI, as more "actors" where involved in the process.

451. It has to be clarified at the outset that, despite the complexity of the model, the responsibility to decide whether an UTR should be classified as an STR and "disseminated" to law enforcement (one of the fundamental standards to assess whether the FIU enjoys a desirable level of operational independence, which is particularly relevant when the FIU is placed within another government agency or ministry) is clearly and solely of the head of the FIU-NL, without any interference from other "actors" involved in the FIU governance model. This is stated in the Agreement of October 13, 2006 between the Ministers of Justice and of Interior. In addition to this, the WWFT sets an important safeguard for the independence of the head of the FIU-NL, providing that the head of the FIU is appointed, suspended and discharged by Royal Decree, on the recommendation of the Minister of Justice, in agreement with the Minister of Finance.

452. There are, however, some elements that could—and in the case of the FIU-NL are—affecting the operational independence of the FIU, especially considering that, in the case of the Dutch FIU, a significant change has occurred since the FIU was created (the placement of the FIU from the MoJ to the

MoI) and that, despite the "test phase" has been concluded in 2008, the FIU-NL still operated as a "project organization" at the time of the onsite visit

453. There are several actors that come in to play in the FIU's governance model: the MoJ and the MoF (the latter in the area of the budget) have policy-management responsibility, whereas the MoI has organization/administration responsibility (this is delegated by the MoJ, which has the legal responsibility "for the overall management, organization and administration of the MOT, according to Article 12 of the WWFT). The policy management of the MoJ consists in setting out policy objectives for the FIU to achieve during each calendar year. The MoJ, in agreement with the MoF, is also responsible for determining (and approving) the budget of the FIU Article 12 (3) WWFT.

454. According to the new management agreement the FIU prepares an annual plan with the policy objectives, which is to be approved by the MOJ. The approval process involves several players: the Public Prosecution Service, the MoF and the MoI. It appears that under the governance model existing at the time in which the FIU-MOT was operating under the MoJ, the MOT played a greater role in the setting of the objectives, whereas in the existing model the FIU has become part of a broader process that involves also other actors. The policy objectives-setting is integrated in the budget plan, which the MoJ "determines" in agreement with the MoF (Article 12 (5) if the WWFT. This governance model, which, as noted later, is also characterized by a series of delegation of authorities from the MoJ to the MoI with regard to the MOT, is far too complex.

455. The situation with regard to the placement of the FIU in the MoI-KLPD is more complex. As explained earlier, although the WWFT law (and the Disclosure of Unusual Transaction Act) establishes that the overall management, administration and organization of the MOT are the MoJ's responsibility, these responsibilities have been delegated to the MoI. The first point that should be noted is that the delegations were not revised to take into account the new tasks assigned to the FIU by the WWFT, some of which are broader than those envisaged by the Disclosure of Unusual Transactions Act, under which the existing delegations were granted, nor were they revised after the new management agreement was signed on September 10, 2010. This has created uncertainties with regard to the clear determination of tasks, responsibilities and reporting line, which remain today and which have had and still have an impact on the operational independence of the FIU.

456. As also mentioned earlier on, an evaluation study was conducted between May-September 2008 by an independent firm to assess the FIU-NL project organization. The study pointed out that MOT staff was concerned about the independent position of the FIU-NL within the KLPD and about attempts from KLPD to have access to the UTR database, and determined that the management of the KLPD had some adverse effect on the independence and autonomy of the FIU-NL. This included recruiting, appointment, ranking, transfer and promotion of FIU staff as well as making expenditure, which, under the sub-delegation requires the consent of the head of the KLPD. More in general, the report noted that the powers of the head of the FIU-NL, although broader and greater with regard to other head of units of the KLPD, are yet different than the ones assigned to the head of MOT, in that the exercise of these powers, despite the sub-delegation, requires the consent of the head of the KLPD. Concerns were expressed also with regard to the Police job-matrix, which may not be well suited for the FIU-NL (especially for the analysts). The study concluded, inter alia, that the added value of the placing of the FIU-MOT in the KLPD and its merger with BLOM into the FIU-NL project organization has not yet proved fully "in part due the uncertainties with regard to the implementation of the policy-related and managerial tasks and responsibilities of the owners (the MoJ and MoF) and managers (the MoI and the head of the KLPD)". The study also concluded that the FIU would perform better in a more stable environment and recommended to clarify managerial responsibilities and reporting lines and to decide as soon as possible on the "final organization form and placement of the FIU-NL".

457. While some of the conclusions of these study (for example those regarding the concerns of staff over the operational independence) may no longer be actual (during the meetings with the FIU, a good level of satisfaction was manifested for the integration of the FIU-NL into the KLPD), concerns remain on those conclusions that are based on legal/structural aspects of the governance model. While a new governance model has been drafted already more than a year ago, the model has only been approved after the onsite mission. This situation has created uncertainties about the governance model of the FIU (enhanced also by the conflict between the MoI and the MoJ with regard to the administration of the UTR database, discussed later on). These uncertainties are a major factor that affects the operational independence of the FIU[61].

458. The new management agreement emphasizes more the operational independence of the FIU-Netherlands, but it was only signed after the onsite visit and it still relies on a system of delegations/sub-delegations of authority. A section of the agreement is dedicated to "Independence" and states, inter alia, that the FIU-Netherlands is a separate, independent and recognizable entity that can carry out its tasks within the KLPD/IPOL service on the basis of "no undue influence or interference"; sets out supplementary powers for the head of the FIU; clarifies that the staff assigned to the FIU will work exclusively for it; and prescribes that access to the UTR database is only permitted to the authorized staff of the FIU Netherlands.

459. In conclusion, the very convoluted system of delegations and sub delegations of authority and the overall complexity of the system, with the involvement of three Ministries (MOJ, MoI and MoF) and the Public Prosecution Service for the approval of the annual plan FIU, erode the operational independence of the FIU. The stalemate that the FIU had to face because of the disagreements between these ministries for more than two years since the completion of the project phase has also undermined the independence of the FIU.

Protection of Information Held by FIU (c. 26.7):

460. The WWFT prohibits in broad terms "a party that performs or used to perform any duty for the purpose of the application of this Act or of decisions taken pursuant to this Act" (that includes the FIU) "from making any further or other use of data or information provided or received by virtue of this Act, and from publicizing such data and information in any further or other way, than is required for the performance of that party's duties or than required pursuant to this act" (Article 22). Although, unlike for other provisions set out in the WWFT, there is no specific sanction for non-compliance with this obligation, the authorities pointed to Article 2.7.2 of the Criminal Code that provides criminal sanction for violation of confidentiality/secrecy rules and to Article 2:5 of the General Administrative Law Act, that also provides for sanctions for civil servants breaching secrecy requirements.

461. There are specific provisions concerning the UTR database, whose data, as explained earlier, is classified as "personal information" (as opposed to the STR-related data which is classified as "Police data" and falls under the Police Data Act). Article 14 of the WWFT states that the "FIU may process personal data for the purpose of the tasks referred to in Article 13 (which sets out the FIU's responsibilities). The Article goes on establishing, by way of cross reference to the Police Data Act, a series of safeguards with regard to the processing of the data and establishes that the MoJ is the authority responsible for collecting the data and sharing it (including abroad). It is not clear whether this responsibility is the same as the one envisaged by the Disclosure of Unusual Transaction Act, which

61 The authorities informed the mission that, as result of the new government in place since October 2010, the Ministry of Justice (renamed Ministry of Security and Justice) has the overall responsibility (including the managerial one) for the Police (and that includes the KLPD and the FIU). This change will likely affect the new management agreement which was signed on September 10, 2010, at a time in which the MoI had responsibility over the Police and the FIU.

clearly established the responsibility for the "administration" of the UTR database in the MoJ. There are also different views among the MoJ and the MoI on who should be responsible over the administration of the UTR database, particularly with regard to the responsibility of the MoJ in the classification of the data and on the security policy. The view of the MoJ is that the delegations to the MoI do not include the administration of the UTR database, whereas the MoI is of the opinion that the delegation of the "overall administration, organization and management" also includes the UTR database. While this is a sensitive point that authorities need to clarify—because it is also related to the classification of the UTR data as "personal" data under Dutch law (and not as "Police" data)—for the purpose of this assessment what is relevant is that, the MoJ is entitled to have access to the information contained in the UTR database. The assessors understand that this is also a consequence of the classification of the personal data as "personal" and of the MoJ's legal responsibility for the treatment of the data in compliance with the law (established by Article 14 (3) WWFT with a cross reference to the Police Act). The assessors also acknowledge that, when an FIU is placed within another institution, IT security is often the responsibility of non-FIU staff. Although the MoJ has access to the UTR database for IT security and for checking compliance with the rules concerning the processing/classification of such data in accordance with the law, the safeguards provided by Article 272 of the Criminal Code and Article 2:5 of the General Administrative Law Act would apply.

462. This concern is emphasized also by the circumstance that Police staff other than the staff of the FIU attempted to access to the UTR database (the 2008 evaluation study reports that there were attempts by KLPD to access the data). It is only the new management agreement, signed on September 10, which prescribes that access to the UTR database is permitted solely to the authorized staff of the FIU Netherlands. No such provision existed at the time of the onsite visit.

463. These circumstances suggest that control of the information and monitoring of access should be enhanced and raise concerns with regard to the effective implementation of security policies concerning access to information.

464. On the other hand, as noted earlier, the MoJ has determined that the UTR-related information is to be classified as "secret", which is a high standard and hinders the possibility of the FIU to request/have access to data it may need to properly undertake its functions, if the request implies that UTR-related information has to be disclosed.

465. With regard to physical security of the information, the various servers of the FIU (including the "UTR database") are stored in a room that is only accessible with the use of a special card by authorized FIU-NL staff only. However there are no other particular measures to ensure physical security (such as windows with bars). With regard to the hard-copy database (where files concerning UTRs which had been filed in hard copies or explanatory annexes to UTRs filed electronically are stored) security measures seemed low. At the time of the onsite visit to the FIU-NL premises the door (not reinforced) was open, although the assessors where explained that it is locked up every night.

466. With regard to IT security the FIU-Netherlands has comprehensive policies in place that require, inter alia, use of access cards, user IDs and passwords, firewalls, and dedicated workstations for contacts with the 'outside" (FIU.net, Egmont Secure Web and FATF.net).

Publication of Annual Reports (c. 26.8):

467. The FIU publishes a yearly report (available online in the FIU website, also in English). The report is very informative and well structured and, in addition to detailed statistics, typologies and trends, contains sanitized cases as well as information concerning the relation of the FIU and its main counterparts, and a description of the main activities carried out.

468. Membership of Egmont Group (c. 26.9) and Egmont Principles of Exchange of Information Among FIUs (c. 26.10):

469. The FIU of the Netherlands is one of the founding members of the Egmont Group and applies the Egmont Group principles for the exchange of information. In 2007, FIU-NL received 348 Egmont requests via the ESW, in 2008, 374 requests, and in 2009, 333 requests. Within the European Union, FIU-NL is the FIU that receives the largest number of EU FIU requests. These requests are made via the FIU.net and cover the years 2007 (707), 2008 (1 032), 2009 (874). A random check done during the on-site visit on a sample of requests received/responses provided through the Egmont Secure Web, indicated that the information is provided in a reasonable timeframe (an average of 5 days, 2 when the request was urgent). With regard to the information provided—from the sample of responses seen by the assessors—this was mainly related to whether the requested person was in the UTR database or information from the Commercial Register.

470. The authorities explained that the requests from foreign FIUs received through the FIU.net are saved in the FIU.net mailing box for an initial period of one year and a half, after which they are stored in hard copy for a period of five years. Requests received through the ESW are saved in the ESW mailing box for a period of one year and also kept in hard copy for a period of five years (legal retention period).

Analysis of effectiveness

471. The FIU receives the vast majority of UTRs in an electronic format. UTRs can be filed directly to the FIU with protected software that all reporting institutions can use, after registering in the website of the FIU. A minor percentage of the reports (less than 1 percent, mainly from DNFBPs) are received in hard copy. A team of 4 officials is in charge to check UTRs for completeness/accuracy of data. After this check the data is loaded into the UTR database. The database runs a daily automatic check for triggering matches of individuals with criminal-record related information in Police database (Referral Database Criminal Investigations and Subjects). The information is also run regularly with the information in the Execution of Confiscation Office (CJIB) database for matches. No other automatic way for triggering red flags are available (for example, in the area of UTRs that are filed based on a 'subjective' indicator), except for an automatic link between the reported transactions and the person, to look for hits in the UTR database.

472. Given the volume of the reports received (an average of 200 000 per year and 500 per day) the analysis is not for each and every UTR, except those coming from gatekeepers. Methods are employed to "prioritize" the investigations on the UTRs, such as a division per category of reporting entities (some of which, such as gatekeepers are considered to pose more risk), but it is not clear, for example, if reports submitted under "subjective indicators" are given priority in the analysis. In the context of a yearly assessment, certain sectors or professions can also be subjected to an enhanced scrutiny based on risk (for example the real estate sector). The use of codes to classify transactions/institutions/indicators at the stage of reporting/collection is a good tool that enhances the processing of the data, although it has to be noted that there is no specific indicator in the UTRs for FT-related transactions (consequently, there is no possibility of automatic red flags). The financial operational analysis consists mainly of matching the information the FIU receives with the information contained in the various database to which the FIU has access to.

473. Few reports were received with regard to FT, and those received (with the exception discussed later on) concerned persons/entities in the sanction list. In these cases, the FIU's analysis consists of establishing the identity of the reported person/entity and enhancing the information received. There are two dedicated analysts for FT-related cases; queries in the UTR database are conducted weekly to detect reported transactions that may be linked to terrorism.

474. Given the high volume of data received, the FIU could benefit from the development of a more automated way of generating red flags, which would help prioritize the analysis of the data in a more structured way. The circumstance that the databases used by the FIU only show the natural persons under investigation but not their associates hinders the capacity of the FIU to have a clearer picture of the whole scenario concerning a UTR. Also, the high standard for the classification of UTR-related information (personal/State secret) affect the effectiveness of the analysis performed by the FIU, in that it restrains the type of information the FIU can have access to, if the request of such information reveals UTR-related data (for example the FIU cannot request whether a person involved in a UTR has been subject to a prior conviction, because such request would imply the disclosure of the name of that person).

475. In addition to the UTRs received from the private sector, the FIU also receives other information that may be related to money laundering, in the form of requests of information, which are forwarded to the FIU by law enforcement agencies through the office of the public prosecutor. These requests are checked for relevance (information can be only provided with regard to "crimes" and if certain other requirements are met) and the information to-be provided classified as STR (so that the relevant information qualifies as "Police data" and can be disclosed).

476. In addition to operational analysis, the FIU also undertakes strategic analysis (there are 3 analysts dedicated to this task). This involves the systematic analysis of money flows cross-border-wise as well as country and region-wise. The analysis of international money flows leads to a "Money flow report" that contains an overview of the unusual and suspicious flows between the Netherlands and the countries in the region where the Netherlands maintain Police liaison officers. The analysis of regional flows leads to the so-called "financial weather reports," which contain sanitized data with respect to geographic "hot spots" in a specific region and an indication of potential trends/problems which may not be apparent/spotted in regional-based investigations. Pro-active analysis is done also with regard to FT. Another type of strategic analysis was undertaken in the context of the FinTer project. The FIU developed a financing/transaction model based on the study of academic researches, modus operandi of groups, terrorists behavior and operational financial analysis (financial behavioral patterns of persons/suspects from real cases) and built a financial transaction pattern model which was sent out to financial institutions for possible matches. The project resulted in 170 UTRs, out of which 49 where substantiated into STRs and lead to the identification of suspected terrorists.

477. The information gathered by the FIU can be stored only for five years (after which it must be deleted), whereas the information in the STR database have a retention period of 10 years. Considering that for the ML offenses stipulated by Articles 420bis and 420ter CC the statute of limitation is set at 12 years, the retention period does not appear to be appropriate and should be extended to 12 years.

478. Interviews with law enforcement authorities indicated that the quality of the information in the STR database, as well as the information pro-actively disseminated by the FIU to law enforcement is good; although, as discussed under R. 27 and 28, law enforcement authorities still do not fully make the most use of this information other than in existing investigations. In particular, according to law enforcement authorities, the number of new investigations prompted by an STR is still low. A June 2008 report of the Court of Audit notes the increase in the use of STR-related information by law enforcement authorities but stresses that they still make little use of the STR-related information, estimating that only 6% of the STRs are used in investigations and that law enforcement authorities initiate investigations on ML cases based on other information. This may also be a symptom that the quality of the STRs is poor. The past attempts by law enforcement to get access to the UTR database may also be indicative that the information available in the STR database may not be sufficiently developed or not entirely useful for the purpose of the criminal investigation.

479. More broadly, it cannot be determined how the information "disseminated" by the FIU effectively contributes to the opening of new ML/FT-related investigations. The statistics provided by the authorities only indicate the number of instances in which law enforcement authorities "consult" the STR database, which can be for any type of (ongoing) criminal investigation, not necessarily for ML or FT.

480. It is also not possible to determine what is the dissemination ratio to law enforcement for the UTRs that are "disseminated" only by way of transforming them into STR and loading them in the STR database accessible to law enforcement authorities (as opposed to the case in which the information on a case generated by the analysis of an UTR, is specifically brought to the attention of the competent law enforcement agency). Statistics for the years 2007, 2008 and 2009 show an increase in the number of instances in which an "official report was prepared on the basis of subject or transaction information" by the law enforcement authority after having accessed the STR database, but, as explained earlier these data refer to ML investigations as well as investigation for other crimes. Finally the increase is not in absolute terms (if compared with the increase of the number of UTR which were transformed in STRs). It is also not clear to what extent the FIU outcome has been used in prosecutions and, in particular, the ratio of dissemination of subjective indicator-triggered disclosures.

481. The FIU is aware of the need to increase the use of STR-related information by law enforcement and it seeking to enhance its pro-active approach to the dissemination of information. In this respect the organization of the work of "account managers" at the FIU, whose task is to bring the information at regional level (including assistance in the collection of evidence for the case), and the deployment of 4 FIOD liaison officers to the FIU have produced encouraging results. Given the minimal use of STR related information for triggering new criminal investigations/adding value to existing ones related to ML/FT authorities should reconsider the utility of a system in which "dissemination" mainly consists of loading information into the STR database.

482. While financial institutions were familiar with the reporting requirements, assessors noted a significant gap in the knowledge of such requirements by the DNFBPs, the majority of which, for example, seemed unaware of the modalities of reporting through the FIU website or of the MOT-explorer. The FIU has conducted a number of reaching out initiatives to these sectors when the WWFT was enacted; it should continue to engage to the private sectors, especially with the DNFBPs, with the view to provide more guidance on the reporting requirements and more examples of typologies and trends of ML/FT (in addition to the good examples provided in the annual report). Reporting entities in general referred to lack of feedback after they are notified that a UTR has been substantiated into an STR. The problem is that the FIU itself, once the information is disseminated to law enforcement has no information of the further course of action undertaken by law enforcement authorities.

483. Interviews with the FIU revealed that management is aware of the current problems (including the issues highlighted in a report issued very recently by the Court of Audit, which was critical of the AML/CFT chain) and of the existing weaknesses, but has also clear views and determination to overcome these problems.

484. Finally, the delays in the finalization of the merger between MOT and BLOM and the delayed approval of a new governance model have also affected the effectiveness of the FIU's performance vis-a-vis the responsibilities assigned to it by the law: the June 2008 Court of Audit report acknowledged that the FIU-Nederland has an important responsibility to signal trends based on the UTRs received and to share this information, but that this responsibility "is not yet lived up to" (because of the not completed reorganization, between MOT and BLOM). It is interesting to note that, according to the statistics provided for the year 2009, there is a decrease of 5 000 in the number of UTRs substantiated into STRs by way of FIU internal analysis only (as opposed by those substantiated because of automated matches with criminal investigation information, or generated by requests of law enforcement through the Public Prosecution).

485. In conclusion, the complexities related to the governance model (particularly the complexity/non-clarity of the reporting lines and the policy/management division of tasks among the various stakeholders), the long delays in the reorganization of the FIU-Netherlands and objective difficulties due to the "change of institutional environment", have an impact on the effectiveness of the FIU.

486. Despite these shortcomings assessors are of the view that, all considered, the FIU has the potential for performing better in the future. The long awaited finalization of the merger, and the clarification of pending legal issues (such as, for example, the transfer of responsibility to the MoI and those related to the administration/classification of the UTR data, which affects the power of the FIU to have access to all the information it needs), the streamlining of the analysis and dissemination of financial information to law enforcement authorities will most likely enhance further the effectiveness of the FIU.

Adequacy of Resources—FIU (R. 30)

487. The FIU's financial, human and technical resources are considered to be, overall, adequate. The FIU-NL staff consists of 56 officials divided in 3 units (MOT, BLOM and an administrative unit). The FIU is under the supervision of the MoJ for the policy-management and, for the organizational management. For discussion on the existing governance model and issues of operational independence see analysis under criterion 26.6.

488. Financial resources are made available to the FIU-NL by the MoJ and are partly supplemented by the MoI. The budget of the FIU is separated from the KLPD, although consent of the head of the KLPD is required to authorize FIU's expenditure. The budget is set (annually) in accordance with Article 12 (5) WWFT, according to which "the Minister of Justice shall determine the budget of the FIU, in agreement with the Minister of Finance." The Head of the FIU is part of the preparation of the budget. In 2009, the budget of FIU-NL was approximately EUR 4.8 million.

489. The staff of the FIU is screened and a confidentiality document is signed off by every official working in the FIU-NL. Access to the UTR database is given by authorization to a limited number of staff members by the head of FIU-NL only (since the adoption of the new management agreement) (although the 2008 evaluation study report indicates that there were attempts to access the UTR database by non-FIU staff, officials of the Police). The MoJ, as discussed earlier, has also access to the database to check compliance with security and classification of information rules.

490. The staff of the FIU is trained on a regular basis, including on specific training programs (for example in the case of the 2 staff assigned for FT). The training programs are both on a national and on an international basis and include financial analysis, legal issues, special investigator trainings and also FATF-evaluator trainings. Some staff members assist in training projects related to law enforcement activities.

491. The FIU is in the process of upgrading its database system.

Statistics (R.32)

492. The FIU maintains accurate and very detailed statistics on the number of UTRs received, including a breakdown of the type to financial institutions, DNFBPs, Police Districts. Statistics are also available for the UTRs that are substantiated into STRs, broken down per type of financial institutions/DNFPs, Police Districts and with an indication of criteria/percentage for the substantiation into STRs, the amounts involved, as well as a breakdown with reference to the dissemination process. Separate statistics are maintained and analyzed for money transfers. Statistics are publicly available in the FIU's website:

http://www.fiu-nederland.nl/index.php?option=com_docman&task=cat_view&gid=7&Itemid=50&lang=en/

493. Please refer to the analysis on R13 for statistics concerning STRs.

2.5.2. Recommendations and Comments

494. Authorities are recommended to:

- Complete the legal framework concerning the FIU-Netherlands.
- Implement a simplified governance model so that issues that affect the operational independence of the FIU are fully addressed.
- Streamline financial analysis, by developing automated-based systems for generating red flags and prioritizing the analysis of the data in a more structured way.
- Reconsider the whole "dissemination" system, with a view to emphasize a more streamlined provision of information to law enforcement, on a case-by-case basis, given the minimal role played by the current system of dissemination of STRs in generating new criminal investigations/adding value to existing ones.
- Enhance security of information held by the FIU (including the physical security of the information stored in hard copy).
- Ensure that the FIU has timely and full access to all data it requires to properly undertake its functions.
- Outreach to lawyers to clarify FIU's powers to request additional information.
- Extend the legal retention period to match statute of limitation envisaged for ML/FT.

2.5.3. Compliance with Recommendation 26

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.26	**PC**	• The FIU-NL has been a project organization for almost five years, and the Netherlands have undertaken steps towards the final merger between MOT and BLOM only after the onsite visit. The legal framework for the FIU-NL is not yet fully complete. • Instances in which access to data does not allow the FIU to properly undertake its functions. • Shortcomings in the secure protection of data. • Governance issues affecting the operational independence of the FIU. • Effectiveness issues concerning: o operational analysis (lack of prioritarization techniques in a context characterized by large amounts of reports); o dissemination of financial information to law enforcement (the role of the STRs' in triggering ML investigations and prosecutions, as well as in ongoing cases, is very minimal; authorities cannot establish how many of the STRs contribute to the opening of ML/FT criminal investigations; access to STR-information is available to law enforcement for investigation of any type of crime, not just ML/FT).

2.6 Law enforcement, prosecution, and other competent authorities—the framework for the investigation and prosecution of offenses, and for confiscation and freezing (R.27 and 28)

2.6.1 Description and Analysis

Legal Framework:

495. The responsibilities, rights and duties of the law enforcement and prosecution agencies are predominantly set forth in the WvSv (Criminal Procedure Code). Criminal financial investigations are directed by the public prosecutor, based on an authorization from the examining magistrate (Article 126 WvSv), and carried out by the police, or specialized services in case specific expertise is needed. The examining magistrate is an independent judge located at the district court's level. The public prosecution service is accountable to the Minister for Justice, who has political responsibility for the service's conduct and performance. The law enforcement agencies have to render account of their actions to one of the officers of the Public Prosecution Service (PPS). If necessary, the public prosecutor may authorize law enforcement agencies to apply coercive measures, after authorization by the examining magistrate for some of them, including special investigative techniques. It is important to underline that not every crime that comes to the PPS' knowledge has to be pursued for prosecution, since there is a discretional power based on the "rule of expediency".

Designation of Authorities ML/FT Investigations (c. 27.1):

Law enforcement authorities responsible for investigating ML/FT

496. The public prosecution service has an office in every of the 19 district courts. Each of these offices has a special prosecutor for money laundering cases. The national public prosecutor's office (*Landelijk Parket*–LP) and the financial, environmental and food safety offences office of the public prosecutor (*Functioneel Parket*–FP) are national organizations. The LP focuses on international forms of organized crime and coordinates efforts to combat terrorism. The FP is an office of the PPS with specific focus on tax fraud and the financial system. A national public prosecutor on ML is located at the FP and is directly linked to FIU-NL. Both organizations start complex and significant financial crime cases, based on intelligence coming from informants, open sources, administrative authorities, and the financial intelligence unit.

497. The police is composed of three levels, a national police agency (KLPD), interregional fraud teams, and the regional police. Among the specialized services, all working at national level, the most relevant for financial crimes is the FIOD, in charge of tax and economic crimes. To a lesser extent, the intelligence and investigation service of the ministry of social affairs and employment (SIOD), in charge of social legislation is performing some criminal financial investigations, as well as two other specialized services in the field of housing and agriculture. The Royal military and border police (KMAR) also performs financial criminal investigations, particularly in relation to its security tasks at Dutch airports.

498. The LP is the central authority responsible for terrorism in a broad sense, including TF. Within the LP, two specialized public prosecutors act as linking pin between the intelligence services and operational agencies and conduct investigations, which are carried out by a specialized unit in the National crime squad (DNR). Besides the LP, the ML prosecutor in the FP, is in charge of receiving FIU dissemination on TF. The FIOD is the special investigation division linked to the FP. Cases on TF will be investigated by the FIOD, and if necessary, the FIOD and DNR work closely together and may exchange personnel to efficiently use certain specialized knowledge. Besides the centralized organization of investigations concerning TF, every police region has, in principle, competence to investigate TF cases. If the case appears to be complex, it can be carried out jointly with, or transferred to, the DNR or the FIOD.

499. Regarding money laundering, the law enforcement agency in charge of investigations is determined by the complexity and geographical location of the case. Money laundering investigations can be conducted by the 19 district prosecutor as well as the LP and the FP, and are carried out by all law enforcement agencies in the country. Over the last years, around 80 percent of criminal investigations for ML or ML and another offense have been conducted by the regional police and around 12 percent by the FIOD.

Specificities of the designated investigation authorities

500. Regional police: The country is divided into twenty-five police regions with their own police forces. Financial investigation experts are located within the region's criminal intelligence divisions. For instance, the police region of Amsterdam-Amstelland has a bureau for financial investigation (BFER) which employs almost 80 full time employees.

501. Interregional groups: The police have created interregional groups to deal with cases related to different regions or which require specific skills regarding their complexity. Out of the six active interregional groups, two are specialized on financial crimes.

502. DNR: The National crime squad (DNR) is part of the Netherlands police agency (KLPD). It has responsibility for organized crime related to drug trafficking (cocaine, heroin, cannabis and synthetic drugs), firearms and explosives, human trafficking and people smuggling, financial and economic crimes, as well as terrorism. The DNR is composed of two teams in charge of financial crimes (19 full time employees each), and a specialized team for intelligence related to financial crime (approx. 5 full time employees).

503. FIOD: Located within the Tax and Customs Administration, the FIOD investigates financial crimes and particularly fraud against the financial interests of the Dutch state (i.e.: tax fraud, bankruptcy fraud, financial regulation of markets, insider trading, real estate, private sector corruption) and money laundering. It is also involved in investigations against organized crime and terrorism through the mapping of criminal funds, and assists the DNR in large and complex organized crime cases or in relation to terrorism financing.

504. KMAR: A specialized unit of the Royal Netherlands Military Police (KMAR) is specialized in financial crime and is mainly active in the Schiphol airport district. This unit is particularly in charge of investigating financial crimes related to drug trafficking both by passengers and air freight. It often operates in cooperation with the FIOD.

505. Other law enforcement agencies: Similarly to the FIOD, three other agencies specialized in criminal investigations in the field of social security law, agricultural law and housing law may perform ML investigations in relation to predicate offenses that are in their scope of activity.

Process of allocation of new ML/FT investigations

506. While the LP is the competent authority for terrorism, including financing of terrorism, the process of allocation of ML investigations by the PPS to law enforcement agencies has to be differentiated between national and local level.

507. At national level, the selection of cases is based on a structured intelligence process, with information coming from a variety of sources: information from informants, open sources, FIU, administrative authorities. All this information is gathered together for an analysis to identify relevant cases and meetings are conducted between the LP or FP and law enforcement agencies to decide on the cases to be investigated.

508. At district courts' level ML investigations are more often ancillary to the existing investigation on the predicate offence. According to the 2008 general instruction on investigation and prosecution of money laundering, law enforcement agencies should, as a matter of principle, investigate all cases involving lucrative forms of crime. In addition, new investigations can also start from local intelligence, including from Regional information and expertise centers (RIECs), established to support and advise municipalities and local authorities in implementing an administrative approach against crime. The national public prosecutor for ML coordinates the action of the 19 district public prosecutors.

Ability to Postpone/Waive Arrest of Suspects or Seizure of Funds (c. 27.2):

509. While the authority to postpone or waive the arrest of suspected persons, or the seizure of the money or both, is not expressly found in a law or similar measures, law enforcement and prosecutorial authorities implement these measures in practice. Decisions to arrest or seize, or to do both, are subject to tactical considerations and could be postponed to enable further investigations or to avoid interfering with the prosecution of a crime. Immediate seizure is only required when the objects are forbidden and there is a danger for public health or they are a threat to the public safety, which will not apply to financial assets.

510. The public prosecutor may decide at what point in time during a criminal financial investigation (CFI) the issuance of a warrant of arrest is appropriate, or at what time it requests to have such an order repealed. In addition, the ability to postpone the arrest of suspects or the seizure of property can be exercised in the context of controlled deliveries or undercover operations.

Additional Element—Ability to Use Special Investigative Techniques (c. 27.3):

511. The code of criminal procedure (Article 126 WvSv) provides a special framework for criminal financial investigations (CFI). This framework consists of extended powers to obtain documents and other information, or to seize goods or assets. These powers come in addition to the usual powers to investigate serious crime including special investigative techniques, which may still be used.

512. A number of special investigative techniques are permitted since the special powers of investigation act (*Wet BOB*) came into effect in February 2000. Special investigative techniques can only be applied to investigate and settle criminal cases in a criminal court. The use of a special investigative technique is subject to permission by the public prosecutor. Prior authorization by the examining magistrate or the board of procurators general is required in some instances. These powers cannot be used to gather information covered by professional secrecy and consequently cannot be directed or related to the activities of lawyers and notaries, except in specific circumstances: When the lawyer or notary is a suspect or an accomplice; with respect to objects that form part of the criminal act or that have served to commit such act; in very exceptional circumstances (Supreme Court March 2, 2010-LJN BJ9262). The existing special investigative techniques are listed below.

- Surveillance: It consists in systematically following persons or systematically observing their whereabouts. Surveillance of private homes is not permitted. Other locked premises such as office buildings or warehouses may be placed under surveillance in ML or TF investigations.

- Infiltration: It consists in participating or co-operating with a group of people that is believed to be planning crimes or to have committed crimes. As an infiltrator, the investigating officer cannot incite a person to commit criminal offences other than the one already planned. The infiltrator can also be a civilian, but in this case the prosecutor has to obtain consent from the board of procurators general.

- Pseudo purchases/services: It consists in the purchase of goods from, or the supply of services to the suspect and can take place separately from an infiltration.

- Systematically gathering intelligence under cover: It means that a police officer systematically obtains intelligence on the suspect through under cover activities such as frequenting the suspect's haunts without being apparent that he is acting as a police officer. As it poses fewer risks to the integrity and security of the investigation than infiltration and pseudo purchases/services, this power is bound by less serious conditions.

- Power to enter locked premises: It enables to enter locked premises (but not private premises) without the owner's permission.

- Recording confidential information: It relates to recording conversations and telecommunications in a closed network such as a company network. Prior authorization of the examining magistrate is required to exercise this investigative technique.

- Investigating telecommunications: This involves telephone taps and claiming data concerning telephone traffic and has to be authorized by the examining magistrate.

- Use of informants: An investigative officer can use a civilian to systematically acquire information on a certain person, once the public prosecutor has issued a warrant, for the duration of the warrant.

- Ban on laissez passer: In case a serious investigation is at stake, the public prosecutor can decide not to seize harmful or dangerous substances (controlled delivery). This decision has to be authorized by the board of general procurators. The same procedure also applies to the entry to individuals.

Additional Element—Use of Special Investigative Techniques for ML/FT (c. 27.4):

513. No statistics are kept on the use of special investigative techniques for combating ML, TF and underlying predicate offences. But law enforcement authorities indicated that they generally use all available investigative techniques to investigate crime.

Additional Element—Specialized Investigation Groups and Conducting Multinational Cooperative Investigations (c. 27.5):

514. In addition to special investigative techniques, there are permanent groups specialized in investigating the proceeds of crimes. At the national level, this task is performed by the FIOD and the DNR's financial crime units. At the interregional level, two of the six interregional groups are specialized on financial crimes. Finally, at the regional level, the BFERs are specifically in charge of economic and financial investigations.

515. While not having been specifically used for ML/TF or in relation to proceeds of crimes, joint-investigation teams (JIT) have already been used several times for other offences with different countries such as the United Kingdom, France, Germany and Belgium. These JITs are based on Article 13 of the Convention on mutual assistance in criminal matters between the Member States of the European union of May 29, 2000, and the Council framework decision of June 13, 2002 on joint investigation teams. The main objective of a JIT is to obtain information and evidence about the crime for the investigation of which it has been established.

Additional Elements—Review of ML and TF Trends by Law Enforcement Authorities (c. 27.6):

516. Law enforcement agencies work together in the FEC which performs studies with regard to issues related to the integrity of the financial sector on a regular basis. The FEC has performed studies on non-profit organizations, boiler rooms and real estate. Currently the FEC is working on a national threat assessment on money laundering (NTA), as well as on criminal use of money transfers, mortgage fraud, cyber crime and investment fraud. In addition, the annual report of the FIU is public and includes trends. The KLPD, including the FIU, also directly informs law enforcement agencies, on a case by case basis, of new trends and typologies. Finally, law enforcement agencies also contribute to a national threat assessment on serious and organized crime, which includes the threat that comes from money-laundering.

Analysis of effectiveness (R.27)

517. While investigations of TF are practically limited to a few numbers of agencies, namely the DNR and the FIOD, a large number of law enforcement agencies are involved in investigations of ML. This derives from the direction taken by both the Ministry of Interior and the Ministry of Justice to try to prosecute ML and deprive offenders of the proceeds of crime during each investigation related to lucrative crimes, even if the proceeds are low. This approach is illustrated by the relatively high number of prosecutions and convictions for ML, or ML and other offences.

518. Law enforcement agencies met by the assessors generally share the convictions that financial investigation can make an important contribution to the fight against serious organized crime and fraud. In practice, this means that in every investigation, a financial criminal investigation should be an integrated part. This is done using two parallel and complementary approaches. On the one hand, the number of skilled financial investigators is increasing and, on the other hand, 'ordinary' police officers should focus on financial aspect of criminal behaviors they may come across.

519. Even if ML investigations are relatively developed in the country, some difficulties remain in four areas related to coordination, training, use of FIU information and investigations related to foreign proceeds.

520. First, regarding coordination, the 2008 Court of Audit report concluded that there was a fragmentation of knowledge, information and skills detrimental to the conduct of financial investigations. This was explained by the organization of the PPS with different sections of the public prosecutor's office having authority over the different investigative services. The FIOD is clustered to the Functional public prosecutor (FP), the DNR to the national public prosecutor (LP), and the regional police services to the different regional prosecutors. Steps have been taken to enhance coordination inside the PPS and between law enforcement agencies through consultation and meetings. Regarding ML, the national prosecutor for ML aims at coordinating the efforts of the PPS.

521. Second, human resources remain an issue. On the first hand, the level of training of some police officers and their ability to deal with complex cases was critically assessed by members of the judiciary met during the interview. They raised the issue that law enforcement agencies and prosecutors often bring forward cases without sufficient proof, merely based on typologies. On the other hand some law enforcement experts underlined that members of the judiciary who are not specialized in financial investigations are not always skilled enough to deal with ML investigations. The problem of resources is reflected in the 2008 NTA which says that "investigations into money laundering and other forms of financial/economic crime are unpopular within the police and the public prosecution service. Rather than conducting financial investigations, the police seem to prefer the more traditional forms of investigation. Financial investigations require specific knowledge and skills that are often lacking." The NTA also

mentioned that "financial investigations are extremely labor-intensive and when people and resources are scarce, that will be an important consideration when deciding whether an investigation is to be launched".

522. Third, the use of FIU information may be enhanced. While the use of STR data for ongoing investigations is generally considered helpful by prosecutors and law enforcement agencies, there are only few instances where an investigation is only triggered by information disseminated by the FIU. Aware of this situation, the FIU is trying to better tailor its dissemination to the needs of specific law enforcement agencies and obtained some recent success related to the fight against human being trafficking. Still, the FIU lacks feedback on the use of its information in order to better tailor its analysis and disseminations. In 2008, it was estimated that 1.2 percent of the UTRs received by the FIU have been used for prosecution, including in ongoing investigations.

523. Finally, prosecutors and law enforcement agencies seem to focus more on the proceeds of domestic crime, than on the foreign proceeds of crime laundered in the Netherlands. This could be explained by a number of factors, including the ones already mentioned related to the constraint in human resources and the limited use of FIU information to trigger new criminal investigations. It may also be related to the approach taken by the authorities to include an AML component in each investigation on lucrative crimes. This "crime to finance" approach is different from the "finance to crime" approach that would often be needed in relation to the laundering of proceeds of foreign crimes in the Netherlands.

524. Draft legislation on confiscation aims at making financial investigations easier and would contribute to lower their labor intensity. This may both increase the use of FIU information and the number of investigations on the laundering of foreign proceeds. The draft legislation provides for statutory presumption based on evidence regarding the origin of assets belonging to the defendants. These presumptions would concern assets acquired over a period of up to six years, on the balance of probabilities.

Ability to Compel Production of and Searches for Documents and Information (c. 28.1):

525. Law enforcement authorities can obtain any documents and information for use in their investigations, as soon as a criminal financial investigation (CFI) has been authorized (Article 126 WvSv) by the examining magistrate. Financial institutions secrecy laws do not inhibit access to documents and information (see section 3, Recommendation 4).

526. Pursuant to Article 126a WvSv an investigating officer in charge of the CFI is entitled, on presentation of a copy of the CFI's authorization, to order an institution or natural person to:

- Report, or allow inspection, or provide with a copy of documents or data, to the exception of data referred to in Article 126nd, second paragraph, third sentence (personal data concerning one's religion, philosophy, race, political views, health, sexual orientation or membership in a trade union).
- State whether, and if so, which assets belong or have belonged to the subject of the investigation.
- Seize the written documents thus provided.

527. Article 126nc WvSv allows an investigating officer in charge of a CFI to request information on an unknown bank account belonging to a specified person. Identification of operations from and to a specified bank account is possible under Article 126nd WvSv. This option applies to offences, as described in Article 67a, paragraph 1 WvSv which are roughly offences punished with a maximum of four years imprisonment, hence including ML and TF. In the case of minor offences the measure requires prior

authorization of the examining magistrate. Under the same conditions, monitoring of future operations is possible based on Article 126ne WvSv. The measure may have a duration of four weeks, which can be extended.

528. Pursuant to Article 126b WvSv, the public prosecutor may demand that for the purpose of seizure, the examining magistrate searches a location. The examining magistrate is also allowed to order the delivery for seizure of letters that may serve to demonstrate the benefits illegally obtained by the subject of the investigation.

529. Pursuant to Article 126c WvSv, the public prosecutor may, in the event of imperative necessity, for the purpose of seizure, search any location, as well as habitation, without the permission of the occupant or an office of a person if any documents or data as referred to in Article 126a or objects as referred to in Article 94a are suspected to be at this location.

530. New draft legislation on confiscation (Parliament Documents II, 31 194), clarifies that the financial investigation can continue until the confiscation order has become final. Furthermore, in case of non-payment of the confiscation order, an investigation may be conducted to establish the assets of the convicted person. If there are any indications that the convicted person actually does have assets despite the fact that payment is not forthcoming, a CFI can also be conducted after the confiscation order has become final. Thus, assumed hidden assets can be recovered.

Document production and legal privilege

531. Competent authorities' ability to obtain documents and information for use in investigations and in prosecutions from professions covered by legal privilege has prompted interesting and perhaps unprecedented discussions during the assessment. On the one hand, law enforcement authorities and prosecutors met by the assessors repeatedly indicated difficulties in accessing information from persons with professional secrecy obligations. In the assessors view this position likely reflects the maturity of the Dutch AML system where a large number of ML investigations are conducted and where investigative work naturally generates interest in information traditionally maintained by or involving lawyers, notaries, accountants, and other professionals. Such issues may not have arisen or matured in countries whose AML frameworks are less developed or less integrated into the day-to-day work of police and prosecutors. On the other hand, the Ministry of Justice has asserted, first, that questions concerning the scope and application of professional privilege are beyond the scope of R.28, which by its terms is focused on the powers of the authorities to locate and trace assets, and, second, that in any case the way legal privilege and the related safeguards are implemented in the Netherlands is not different from neighboring countries and is in line with international law.

532. Assessors appreciate that an examination of the scope of legal and professional privilege in the context of R. 28 raises fundamental questions concerning the tension between the interests of security and human rights, and that it is difficult, if not impossible, to articulate a universal norm in balancing these competing interests. Nevertheless, the assessors do not agree with the position of the Ministry of Justice that the inquiry is beyond the scope of legitimate inquiry under R. 28 as i) the text of R. 28 requires competent authorities to be able to obtain information, while in the Netherlands the ability to obtain information is hindered by insufficient powers; ii) the Dutch legal framework is more restrictive than what would be permitted by relevant international law including obligations aiming to protect the rights to fair trial and to privacy; iii) feedback received from law enforcement authorities indicates concrete implications of their limited powers to access information; and iv) the issue of the scope of legal privilege has been mentioned as a factor underlying the ratings in the recent MERs of Argentina,[62] Austria,[63] and Germany.[64]

62 In relation to R.28 "Lawyers and notaries cannot provide information relating to acts that came to their knowledge through their office or profession."

The following paragraphs describe and analyze the Dutch legal framework, give an overview of the European context, and provide an assessment of the effectiveness of the system in place.

Dutch legal framework

533. Under Dutch law, lawyers, and civil-law notaries have the right to refuse to give evidence, to the extent that the provision of information would violate their professional privilege and the obligation of confidentiality arising from it (Article 218 CPP[65]). Within the context of a criminal investigation, search and seizure can take place at the addresses of lawyers, and civil-law notaries (Articles 110, 97.1, and 98 CPP). An order to produce documents ('production order') can also be directed against these professions, but these are not required to comply with such orders if and to the extent that the production of documents would violate their obligation of secrecy (Article 96a.3 CPP).

534. In practice, seizure of documents from lawyers or civil-law notaries is subject to procedural protections designed to ensure that professional secrecy obligations are honoured but not abused. Seizures are effected by means of a search supervised by an examining magistrate (in urgent cases, a search supervised by a Public Prosecutor is also possible; see Article 97.1.b. CPP). The examining magistrate will be accompanied by the local Dean of the Netherlands Bar Association or the local chairman of the Dutch Royal Notarial Association. They can serve a role as an intermediary during the selection of documents to be seized. In many cases, the examining magistrate will provisionally seize a large number of files and documents and take the final decision on seizure later in his office. It is primarily up to the lawyer or civil-law notary to assert what matters come under the scope of his right to refuse to give evidence. The examining magistrate will subsequently consider whether the right to refuse to give evidence applies.

535. The right to refuse to give evidence is not absolute and there are several important exceptions. If the examining magistrate is of the opinion that the right to refuse to give evidence should not be applied, he will make the documents available to the Public Prosecutor. These exceptions arise in the following circumstances:

- When the party observing confidentiality (lawyer or civil-law notary) can be designated as the suspect of a crime (Article 126nc CPP), or complicit in the crime committed by his client, as indicated in Supreme Court May 19, 2009, (LJN BH7284) and Supreme Court June 14, 2005 (LJN AT4418).

- With respect to objects that form part of the criminal act or that have served to commit such act (Article 98.2 CPP).

- In very exceptional circumstances, the interest of finding the truth prevails over the right to refuse to give evidence (Supreme Court March 2, 2010-LJN BJ9262). Since this is an exception to the main rule, this may not go any further than strictly necessary in order to reveal the truth of the relevant offence (Supreme Court June 29, 2004-LJN AO5070).

63 In relation to R.28 “Strict conditions for obtaining/compelling information subject to banking secrecy and scope of legal privilege hinder the possibility for law enforcement authorities to locate and trace property.”

64 In relation to R.12 “Professional secrecy provisions are interpreted broadly by the liberal professions, and pose a significant impediment to their ability to provide records as evidence for prosecution of a crime (as called for under c.10.1.1.) or keep findings available for competent authorities (as called for under c.11.3).

65 Article 218 CPP : “Others with exemption from giving evidence or answering certain questions are persons who are bound to secrecy by virtue of their position, their profession, or their office, but only with respect to the knowledge which has been entrusted to them”. This article also applies to tax accountants.

536. The concept of 'very exceptional circumstances' is not defined, but is determined on a case-by-case basis. A 2002 Supreme Court decision (*February 12, 2002–LJN AD9162*) is particularly interesting in the specific context of the lawyer-client privilege. The case discusses the authorities' ability to seize a letter sent from the Bahamas to the Netherlands in 1998, in the context of a criminal investigation. The recipient of the letter was a lawyer. A witness had stated that the letter mentioned a number of persons alleged to be "beneficial owners" of a Bahamian company. The persons mentioned in the letter were suspected to have participated in an organization whose aim was to commit crimes, including forgery and tax fraud. During a search this letter was taken, but the lawyer asked a lower court to order it returned to him. The lower court agreed, and the prosecutor appealed to the Supreme Court. The Supreme Court sided with the attorney indicating that showing the letter would have lead to a breach of the professional privilege. The Supreme Court indicated that there was no evidence that the letter itself was the object of the criminal act, or that it had been used to commit that act.

537. In another 2002 decision (*June 18, 2002–LJN AD5297*), the Supreme Court narrowly interpreted the absence of right to refusal when the holder of confidential information is a suspect. The Court explained that "the mere circumstance that an attorney is designated as a suspect is definitely not sufficient to breach through his privilege. (…) However the case may be different when there is suspicion of a serious criminal fact, such as an attorney engaging in criminal cooperation with a client."

538. Moreover, in the March 2, 2010 decision (*LJN BJ9262*), the Supreme court decided that for the assessment of the claim on the right to refuse to give evidence by a lawyer, the location where the documents are found (*i.e.* on the premises or in the possession of the person with the right to assert professional privilege or with a third party) is not decisive.

539. While the CPP provides for cases where the holder of confidential information may be compelled to give evidence to competent authorities despite their professional secrecy obligations, these provisions have been restrictively interpreted by the Supreme Court. In this connection, and drawing by analogy on the compromise reached in this area in connection with R. 16, the assessors are particularly concerned about instances where the confidential information was not related to the defense or representation of a client in or concerning proceedings. Consequently, the assessors believe the current legal framework limits competent authorities' ability to obtain documents and information for use in investigations, prosecutions and related actions on ML, TF and other underlying predicate offenses.

European context

540. The protection of confidentiality is assured through very different mechanisms in national European laws. In countries with a common law tradition, the protection of confidentiality is seen as part of a broader concept of "professional privilege," being a fundamental principle of justice, that grants protection from disclosing evidence and is seen as a right that attaches to the client and not to the lawyer and so may only be waived by the client. In other jurisdictions, as in The Netherlands, the privilege is considered as belonging to the lawyer.

541. While the assessment is conducted against the FATF standard, it is useful to consider if the compliance with the standard is constrained by treaties the Netherlands are bound to, and particularly European Union law and the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).

542. Neither the EU treaties nor the ECHR refer explicitly to professional privilege of lawyers but both the Luxembourg and the Strasbourg Courts did examine the question of confidentiality and professional privilege protecting the lawyer-client communication particularly through Article 6 (protecting the right to a fair trial) and Article 8 (protecting the right to privacy) of the ECHR. The

European Court of Human Rights (ECtHR), which has jurisdiction over violations of the ECHR, has dealt with the issue of professional privilege from the angle of Articles 6 and 8 of the ECHR, mostly in relation to the client-lawyer relationship in the context of a legal proceeding.

543. According to the ECHR's case law, the concept of 'a fair trial' referred to in Article 6 of the ECHR consists of various elements, which include, among others, the rights of the defense, the principle of equality of arms, the right of access to the courts, and the right of access to a lawyer both in civil and criminal proceedings.[66] Lawyers would be unable to carry out satisfactorily their task of advising, defending and representing their clients if they were obliged, in the context of judicial proceedings or the preparation of such proceedings, to cooperate with the authorities by passing them information obtained in the course of related legal consultations.

544. In relation to Article 8 ECHR, the Court indicated that the mere existence of professional privilege is not, as such, an absolute obstacle to interference with the right to privacy, especially if the interference is, pursuant to Article 8.2 ECHR, in accordance with the law and necessary in a democratic society including in the interests, among others, of national security or the prevention of disorder or crime[67]. The Court has consistently held that the contracting states have a certain margin of appreciation in assessing the need for an interference, but that it goes hand in hand with European supervision. The exceptions provided for in Article 8.2 are to be interpreted narrowly, and the need for them in a given case must be convincingly established.[68] In a recent decision, related to legal privilege but where the seized documents were not related to litigation, the Court indicated that domestic law can authorize searches in a law office as long as they are accompanied by special safeguards.[69]

545. The Court of Justice (ECJ) of the European Communities has developed less abundant case law on legal privilege than the ECtHR, but one case is particularly interesting as it is related to AML requirements.[70] In this case, Belgian bar associations were considering that the provisions of a Belgian law which extended to lawyers both the obligation to inform the competent authorities if they come across facts which they know or suspect to be linked to money laundering and the obligation to transmit to those authorities additional information which the authorities consider useful, unjustifiably impinge on professional secrecy and the independence of lawyers, that is to say on principles which are a constituent element of the fundamental right of every individual to a fair trial and to the respect of his rights of defense. As the Belgium law was a transposition of the Second EU AML directive, the Supreme Court referred the case for a preliminary ruling to the ECJ. The Court noted that in the Second EU AML directive, "the obligations of information and cooperation apply to lawyers only in so far as they advise their client in the preparation or execution of certain transactions—essentially those of a financial nature or concerning real estate, as referred in Article 2a (5) (a) of that directive—or when they act on behalf of and for their client in any financial or real estate transaction. As a rule, the nature of such activities is such that

66 See Golder v. United Kingdom (App. No. 4451/70); Campbell and Fell v. United Kingdom (App. No. 7819/77 and 7878/77); Borgers v. Belgium (App. No. 12005/86).

67 Article 8 ECHR – Right to respect for private and family life: 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

68 Crémieux v. France (App. No. 11471/85, 1993).

69 Da Silveira v. France (App. No. 43757/05, 2010).

70 Ordre des barreaux francophones et germanophones a.o. v. Council of Ministers, Belgium, (Nrs. 3064 and 3065, 2008.

they take place in a context with no link to judicial proceedings and, consequently, those activities fall outside the scope of the right to a fair trial."[71]

546. Consequently, European courts endorsed the 2nd European directive's obligation that in the preparation or execution of certain transactions, essentially those of financial nature or concerning real estate, lawyers have to cooperate fully with the authorities responsible for combating money laundering "by furnishing those authorities, at their request, with all necessary information, in accordance with the procedures established by the applicable legislation" (Article 6.1.b). Hence, the Dutch authorities appear to have room to improve the ability of law enforcement authorities to obtain information and documents from lawyers, notaries and tax accountants".

547. In addition, it does appear practically possible for a European country subject both to EU law and the ECHR to put fewer limitations on the authorities' powers. For example, in the United Kingdom, an original document not brought into existence for privileged purposes and so not already privileged, does not become privileged merely by being given to a lawyer for advice or other privileged purpose[72], which appeared to be the situation of the Bahamian letter mentioned in the Dutch Supreme Court decision above (February 12, 2002–LJN AD9162). In addition, in the United Kingdom, when advice is given or received in circumstances where litigation is neither contemplated nor reasonably in prospect, except in very limited circumstances communications between [the lawyer] and third parties will not be protected under the advice arm of legal professional privilege".[73]

Power to Take Witnesses' Statement (c. 28.2):

548. The WvSv arranges calling witnesses by the examining magistrate (Articles 210-226 WvSv), the public prosecutor (Article 260 (1) WvSv), the suspect (Article 260 (2) WvSv) and the judge of the court hearing (among other Articles, Article 280 WvSv). As a result of case law, the calling of witnesses by the law enforcement agencies, which has not been arranged by law, has become common practice.

549. The competent investigative authorities may draw up official reports, among which witness statements, because money laundering is an offence which may independently be penalized pursuant to the WvSr. This report may serve, pursuant to Article 344 (1) (2) WvSv, as evidence. In that sense investigators may testify about their findings in writing, but they may also question witnesses and have this laid down in a statement drawn up under oath of office. The investigative officer may be called upon to be questioned as a witness during the court hearing.

Analysis of effectiveness (R.28)

550. Although no statistics are available, CFIs appear to be widely used and the law enforcement agencies met by the assessors did not mention difficulties in timely accessing the documentation they need, for investigations relating both to money laundering or predicate offenses. The only exception is related to professions covered by legal privilege, namely, the lawyers, notaries, and tax accountants (see above).

551. The authorities consider professions covered by legal privilege, namely, the lawyers, notaries, and tax accountants, often play a key role in money laundering mechanisms. In October 2008, a special committee of the Dutch House of Representatives researched the inter-relations between the legitimate

71 This ECJ decision has been used by the ECtHR in André v. France (App. No. 18603/03, 2008).
72 Law Society of England and Wales, Anti-money laundering practice note, October 29, 2009, Section 6.4.4.
73 Id. Section 6.6.1.

business and the underworld.[74] The report described a trend of lawyers and notaries being increasingly involved in money laundering and other similar crimes.

552. Moreover, as indicated above, law enforcement authorities and prosecutors met by the mission repeatedly indicated difficulties in accessing information they need from persons asserting professional privilege. These difficulties have manifested themselves in very practical terms. As a typical example that is occurring with increasing frequency, the authorities indicated that where an email taken during a search to the premises of an alleged criminal has been copied to a lawyer, the lawyer must be given the opportunity to indicate whether it falls under his right to refuse to give evidence. Based on the somewhat restrictive legal framework analyzed above, the authorities indicated that the limitation to their ability to access information they need to obtain evidence, is an increasing concern, and has had an adverse impact on past investigations.

553. The instruction on the supply of information by financial service providers (2004A002) should be mentioned here as it refers to reimbursement arrangements of expenses involved in the surrender of objects and supply of information by financial institutions. The fact that law enforcement agencies have to pay for the production of documents is potentially an issue in an environment where i) the authorities want financial investigations to be a standard component of most of the criminal investigations, ii) the cost of services performed by financial institutions is increasing, and iii) law enforcement agencies budgets are under constraint. Consequently, even if the powers to obtain documents and information are wide, the cost related to accessing the information may lead to set a too high threshold for the law enforcement agencies to compel production of documents.

554. The Netherlands do not have a central national database with data of all banks account, but information regarding accounts in financial institutions of all natural and legal persons resident in the Netherlands is held by the tax authority. This information is considered very useful by police forces but may only be accessed by law enforcement authorities, other than the FIOD, upon authorization by the Prosecutor.

Statistics (R.32)

555. The only statistics provided to the assessors are the total number of prosecutions for ML and ML related offences (see below). There are no statistics on the number of investigations, or the number of investigations resulting from an STR.

Total number of prosecutions for ML or ML and another offense per law enforcement authority (January 1, 2006–June 30, 2009)	
Law enforcement authority	**Number of prosecutions**
Regional Police	3 279
FIOD	586
KMAR	356
KLPD	287
Interregional fraud team	126
Other	38
TOTAL	**4 672**

74 Dutch House of Representatives, "Verwevenheid van de bovenwereld met de onderwereld", http://www.tweedekamer.nl/images/Eindrapport_verwevenheid_onder_bovenwereld_118-173243.pdf

Adequacy of resources to Law Enforcement and other AML/CFT investigative or prosecutorial authorities (c.30.1)

556. The adequacy of resources is assessed for the AML/CFT investigative and prosecutorial agencies in the country. A number of measures have been taken in recent years to enhance the resources of investigative and prosecutorial authorities, including after the 2008 Court of Audit report mentioned the limited capacity and proficiency of some actors in the chain.

Public Prosecution

557. The public prosecutor service employs more than 4 500 people, including 700 public prosecutors. The mission met with the LP and the FP which seem to be adequately structured, funded, staffed and provided with sufficient resources. The FP counts 63 specialized prosecutors on fraud cases (including ML) and 72 legal aids.

558. Based on the interviews conducted, questions are raised by law enforcement agencies and judges regarding the adequate direction of investigations at the local level by district prosecutors. While prosecutors at the local level are specialized in fraud, there may not always be sufficient expertise to deal with ML cases.

559. The budget of the relevant sections of the public prosecution service is shown in the table below.

Budget of the relevant sections of the Public Prosecutions Service (2009).	
Section of the Public Prosecution Service	**Budget 2009 (million)**
District Public Prosecutor's Offices	308
Court of Appeal Jurisdiction	39
FP	28
LP	18
BOOM	10

Police

560. The police forces count approximately 54 000 members. At the national level the KLPD has specialized staff involved in financial investigations and includes three specialized DNR teams dealing with financial crimes.

561. The police authorities met by the mission did not mention particular difficulties in relation to staffing, funding and resources. But the 2008 Court of Audit report indicated a lack of capacity in the regional police units to effectively investigate financial crime. The current FINEC program (2007–2011) seeks to step up capacities in criminal financial investigations. The program currently focuses on 5 of the 25 police regions and the staffing of financial investigators should increase by 100 staff over the period.

FIOD

562. The FIOD employs approximately 1 100 people, including 800 investigators. While all FIOD investigators may perform ML investigations, two units are specialized on ML cases, in Amsterdam and in Harlem. Both have around 20 staff. The unit in Amsterdam specialized in real estate and the unit in Harlem is competent to work on signals coming from the NL-FIU. Out of the approximately 500 criminal investigations carried out by the FIOD in 2009, 146 included money laundering, to compare with 127 prosecutions in 2008 and 92 in 2007. The FIOD officials met by the assessors did not mention any specific issues related to funding, staffing and sufficient resources.

Integrity of competent authorities (c.30.2)

563. Regarding professional standards and integrity, public prosecutors and law enforcement agents are subject to a screening at the time of entrance and every five years. They have to abide to their respective codes of conduct. Inspections could be conducted by their relevant ministry or by the national police internal investigations department. This department is part of the PPS and falls directly under the management and authority of the Board of Procurators Generals. It investigates cases of illegal activities by persons or organizations that threaten the integrity of public authorities, and investigates government officials as well as legal persons and individual citizens. During the period 2005–2009, there has been an annual average of 90 cases of corruption cases involving police officers.

Training for competent authorities (c.30.3)

564. Law enforcement agencies and the Public Prosecution Service are participants in the FEC (see section 6.1). The FEC provides for traineeships within all cooperating organizations. Therefore it is possible for an employee of a law enforcement agency to work, for a short or longer period time, at, for instance, a supervisory agency or at the ministry of Finance or Justice.

Prosecutors

565. For outsiders who join as a substitute public prosecutor and secretaries who join as substitute public prosecutor, the public prosecution service organizes a course which comprises, among other things, a module on financial detection and a module on searches and seizure. On a voluntary basis, there are also courses on money laundering and on the confiscation of assets. These courses are also provided on a voluntary basis as ongoing training for the members of the prosecution service and in some cases to clerks.

Police

566. The Dutch National Police Academy offers training and education specially aimed at financial investigation. Specialized instructors and trainers are employed at the academy. All police regions can enroll staff in training and re-training programs to maintain up-to-date knowledge and expertise in field of financial crime to keep up with developments and to acquire useful knowledge of financial investigation techniques. All existing general police education programs have been or will soon be made FINEC-proof. In the academic field, the Police Academy has created the position of a professor of financial crime, with the objective of conducting scientific research in this field and of informing stakeholders of important developments in the domain of financial crime.

FIOD

567. The FIOD organizes a wide range of different training programs and seminars in the field of AML. These programs are mandatory for both managers and financial investigators. For example, there is a specialized training program for tax auditors and financial investigators and a yearly seminar on money laundering (sharing information, knowledge of new developments in the field of ML, discussion about best practices etc). The personnel of the FIOD are also informed of new developments through a special (internal) website.

Additional element—Special training for judges (c.30.4)

568. Trainings for prosecutors referred to in the description of c.30.3 can also be attended by judges and judicial secretaries on a voluntary basis. In addition, the judges have developed knowledge centers at

the level of the five courts of appeal. The knowledge center of the court of appeal of Amsterdam is specialized on financial crimes and provides lectures and courses for judges all over the country.

2.6.2 Recommendations and Comments

569. Regarding Recommendation 27, the authorities should consider improving the focus of ML investigations and the amount of investigations conducted in relation to transnational organized criminal activities where the proceeds are generated abroad and laundered in the Netherlands.

570. In relation to Recommendation 28:

- When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain from lawyers, notaries, and tax accountants, documents and information for use in those investigations, and in prosecutions and related actions. The assessment team considers that the current framework on legal privilege in the Netherlands limits the authorities' powers unreasonably. The authorities should review the scope of professional secrecy and privilege obligations, and consider amending the CPP to improve the authorities' ability to obtain documents and information, having regard to the possibilities enabled by the European treaties.

- Maintain statistics on the number of investigations and on the use of powers to conduct ML or TF investigations.

2.6.3 Compliance with Recommendations 27 & 28

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
R.27	**C**	• This Recommendation is fully observed.
R.28	**LC**	• Scope of legal privilege hinders the ability for law enforcement authorities to locate and trace assets and property. • Absence of statistics on investigations does not enable to fully assess effectiveness.

2.7 Cross-Border Declaration or Disclosure (SR.IX)[75]

2.7.1 Description and Analysis

Legal Framework:

Mechanisms to Monitor Cross-border Physical Transportation of Currency (c. IX.1):

571. As a member of the EU, the Netherlands applies EC and domestic rules in the case of cross border transportation of currency and negotiable instruments. The EC regulation 1889/2005 "on controls of cash entering or leaving the community", which is directly applicable in the Netherlands as an EU member, establishes the rule of obligatory declaration for "cash" of EUR10 000 or more carried by any natural person entering or leaving the European Community. Article 2 of the Regulation defines cash as including currency and bearer negotiable instruments that are either in bearer form, endorsed without

75 This assessment was conducted on the basis of the requirements in place at the borders into and out of the Netherlands. FATF agreed in February 2009 that a supra-national approach could be applied for EU countries. However, the supra-national approach has not been used to rate this assessment at the request of the authorities and also because further discussions are needed about how to implement a supra-national assessment.

restriction, made out to a fictitious payee, or otherwise in such a form that title thereto passes on delivery, as well as incomplete instruments (such as promissory notes and money orders) signed but with the payee's name omitted. Throughout the analysis of this Recommendation the term "cash" will be used to include both currency and bearer negotiable instruments.

572. The EC regulation is complemented by the Dutch General Customs Code (*Algemene Douanewet*, hereinafter ADW). Article 3 (2) of the ADW requires that the declaration be made in writing on entering or leaving the EU territory. Among the things that must be declared are the name of the person (including the case of a company and the "intended recipient" if the traveler is carrying cash on behalf of a third person) and the intended use of the cash and its origin.

573. There are no declaration requirements, in the EC regulation or in the ADW, in the case of shipment of currency through containerized cargo or in the case of mailing of currency or bearer negotiable instruments by a natural or legal person.

574. Authorities stated that crew and travelers on vessels can declare cash through a shipping agent (shipbroker). The shipping agent can make a declaration himself when, under the captain's orders, he takes cash on board or takes cash off the ship. In such cases Customs perform a broad inspection

575. Prior to the introduction of the EC regulation, there were no declaration requirements in the sense envisaged by SRIX; in July 2007 the Dutch authorities started to work in order to implement the EC Regulation. The authorities explained that prior to 2005 Customs could have (and still can) used powers stemming from the General Tax Code (*Algemene wet inzake rijksbelastingen*, hereinafter AWR) in the case of levy-related taxes for doing searches: if cash was discovered "cash notifications" were made to the FIOD. It is not clear how the powers envisaged by the AWR could be (can be) used in a situation in which there is no levy, such as the case of cross-border transportation of cash.

Request Information on Origin and Use of Currency (c. IX.2):

576. Customs have the authority to perform controls pursuant to the ADW (or, if they suspect tax-related offences, also pursuant to the AWR), which, in the case of the declaration requirement, consist at a minimum of checking the traveler's identity. The traveler subjected to the declaration obligation has also the obligation to provide proof of identification on demand (Article 1.34 of the ADW). Upon the discovery of a false declaration or in the case of failure to declare Customs authorities undertake so-called "in-depth" controls, in which the Customs official is entitled to ask for additional information, including with regard to the origin of the cash and its intended use. These data, as mentioned above, must be indicated in the declaration form. In this case Customs use a special standardized procedure with the aim to establish whether the information provided is correct and if there is any suspicion of ML.

Restraint of Currency (c. IX.3):

577. In the case of a lack of declaration or false declaration, Customs officials are authorized to detain the cash (Article 4.2. EC Regulation 1889/2005 in combination with Article 3:3 (1) (2) ADW), but only as long as the person subjected to the declaration requirement does not provide the information required for the declaration (Article 3:3 (3) ADW). Although this may not provide, per se, enough time to ascertain evidence of ML or TF, the authorities stated that this goal is achieved by means of the "in-depth control" that is always applied in cases of lack/incomplete/incorrect declaration. The in-depth control, as explained by the authorities, consists of checking the cash, inspecting the luggage and making a copy of the identity documents and other relevant documents. Customs authorities are also entitled to conduct a body search, pursuant to Article 1:28 ADW

578. The situation is more complex if there are suspicions of ML or TF. Authorities stated that Customs have been empowered by the *Besluit buitengewoon opsporingsambtenaar Belastingdienst/Douane* (hereinafter referred to as 'BOA decision') to use investigative powers for a list of designated crimes, which includes ML but not TF (since TF is not an autonomous offence in the Netherlands). From discussions during the onsite mission it was clarified that a situation of suspicion of ML would not per se trigger the application of these powers, unless Customs suspects tax-related offences. However, in the case in which the traveler complies with the declaration requirements and there is a suspicion of ML, the case would be transferred to FIOD as the competent law enforcement authority, but only a seizure pursuant to the Criminal Procedure Code (see discussion under Recommendation 3) could be applicable. In the period 1/1/2010-6/30/2010 there were 11 cases of suspicions of ML.

Retention of Information of Currency and Identification Data by Authorities when appropriate (c. IX.4); Access to Information by FIU (c. IX.5):

579. The declaration forms contain a series of data that must be filled in, which include, inter alia, the amount of the cash and the identification data of the bearer. At the end of each working day all declaration forms are sent to the Tax and Customs Administration/Central Administration (*Belastingdienst/Centrale Administratie*, hereinafter B/CA). B/CA enters the hand-written information on declaration forms into an automated system and processes them using a classification system for the information contained in/related to the declaration. This classification is based on various codes (for example these codes indicate whether the declaration was false/incomplete/missing; if the case has been forwarded to FIOD). The retention period of the processed data is of period of two years. The retention period for declarations is five years, except in the cases of incomplete/false/missing declarations, in which case the retention period is seven years. Pursuant to a memorandum of understanding signed in 2007 between the FIU and the Customs, the information contained in the declarations is also sent on a weekly basis to the FIU. However, in February 2010, the provision of this information had been discontinued until August 2010, as the Customs were upgrading their database. The information flow has resumed. The FIU also noted that, at times, the quality of data is poor and inaccurate and often not fully reliable (because the information is manually entered from hand-written declaration forms into the Customs system, hence the occurrence of errors). Authorities stated that as a result of a meeting called specifically to address this issue, FIU-Netherlands and Customs have agreed to improve the quality of the declaration forms/reports in order to improve the analysis of the data and the reporting of suspicions of ML.

Domestic Cooperation between Customs, Immigration, and Related Authorities (c. IX.6):

580. The Customs cooperate with the FIU by virtue of an agreement which entered into effect in July 2007. The agreement stipulates the way the declaration data should be provided to the FIU and envisages an annual assessment of the process. Since the agreement was signed this assessment took place once, and revealed the issues noted under criterion IX.5 regarding the quality/reliability of the data. Customs cooperate also with the Border Police (with whom they can request in real time information about travelers identities, including for suspect lists, suspected terrorists and sanction lists) and with the FIOD, which can be called in the case in which there are suspicions of ML. Although cooperation with the FIU is good, Customs indicated that they would like to receive a more "substantive" feedback from the FIU, other than the communication that an UTR has been developed into an STR, including more information on ML trends and typologies.

International Cooperation between Competent Authorities relating to Cross-border Physical Transportation of Currency (c. IX.7):

581. Articles 6 and 7 of EC Regulation No. 1889/2005 allow for the exchange of information with other EU Member States and non-EU Member States. Article 6 applies to the exchange of information

between EU Member States and allows for the transmission of information gathered through the declaration or disclosure process when there are indications that the sums of cash are related to any illegal activities associated with the movement of cash. As a member of the EU, the Netherlands also apply EC Regulation 515/97 on mutual assistance in customs matters. Article 7 (above) further provides for the exchange of information with non-EU Member States upon certain conditions.

582. At EU level there are also several mechanisms for exchanging of information that can be used also for the purpose of detecting money launderers or terrorist financiers and cash couriers, such as FIDE (Customs Files Identification Database), which can be used to check whether a person or company is or has been subject to criminal investigation or subjected to criminal sanctions; CIF (Customs Information System), which include also information on cash detained/seized; and the Risk Information Form (RIF) a system whereby customs administrations can exchange concrete risk information in a standardized format. These risks can relate to different fields of customs supervision, *e.g.* import of goods, transit of goods but also aspects related to cash controls. On the basis of these information customs administrations can decide to target these aspects and perform further controls.

583. Although the Netherlands have signed several Agreements on customs cooperation and mutual assistance with non-EU States, many of these agreements were established at a time in which there was no declaration obligation for cross border transportation of cash and, therefore, they would not set forth specific arrangements for the sharing of information recorded pursuant to criterion IX.4

Sanctions for Making False Declarations/Disclosures (applying c. 17.1-17.4 in R.17, c. IX.8; Sanctions for Cross-border Physical Transportation of Currency for Purposes of ML or TF (applying c. 17.1-17.4 in R.17, c. IX.9):

584. Article 10:5 of the ADW provides that those who make an incorrect or incomplete declaration or are obliged, by virtue of Customs legislation, to provide information details or indication and fail to provide it, or provide it incorrectly or incompletely are subjected to detention not exceeding 6 months or a fine of third category. The sanctions are differentiated taking into account whether the violation was done with intent or gross negligence; the amount of the sum; and the type of violation (failure to declare; incorrect or incomplete declaration), and range between a minimum of EUR250 to a maximum of 10 percent of the amount not declared, in any case the fine cannot exceed EUR19 000. Authorities explained that the case of recidivism would trigger a suspicion of ML by default. Authorities provided statistics for sanctions issued for the period January (when the database was established)–May 2010 as follows: there were 157 cases (the overall amount of the currency involved was EUR2 494 650) of non-declaration and 2 cases of incomplete/incorrect declarations (currency involved: EUR94 700). The average amount of the fines issued is between EUR1 000 and EUR2 000. The authorities stated that the maximum fine imposed in a case of non-declaration was EUR5 235.

585. There are no additional sanctions other than those provided for in the Penal Code for money laundering (terrorist financing is not an autonomous offence in the Netherlands but in some situations could be considered as “preparation” of a terrorist act or “participation in a terrorist organization” and, under the terms discussed under SRII it could be theoretically possible that a cross border transportation of cash be considered as a “preparation” for a terrorist act or “participation in a terrorist organization”).

586. Sanctions appear to be proportionate and dissuasive. From a sample of issued sanctions provided by the authorities (see table below) it appears that in several instances sanctions are too low compared to the non declared amounts, hence, issues of effectiveness.

Reference	Amount of currency involved (converted to EUR)	Imposed fine
52000310001	EUR 28 410	EUR 250
52000610055	EUR 11 750	EUR 1 000
52000610049	EUR 33 563	EUR 2 000
52000210002	EUR 13 000	EUR 1 000
52000210004	EUR 13 711	EUR 1 000
52000310014	EUR 24 100	EUR 250
52000210003	EUR 12 073	EUR 500
52000110002	EUR 12 000	EUR 1 000
52000210005	EUR 15 780	EUR 1 000
52000310010	EUR 17 490	EUR 500
52000110006	EUR 14 680	EUR 500
52000610056	EUR 10 075	EUR 1 000
52000810003	EUR 13 100	EUR 1 000
52000310013	EUR 10 070	EUR 1 000
52000310012	EUR 15 050	EUR 1 000
52000310018	EUR 11 742	EUR 1 000
52000510041	EUR 10 425	EUR 1 000
52000310052	EUR 31 000	EUR 2 000
52000710002	EUR 10 000	EUR 1 000
52000710001	EUR 10 200	EUR 1 000
52000310057	EUR 42 325	EUR 2 000
52000310031	EUR 60 040	EUR 3 000
52000710006	EUR 17 390	EUR 1 000
52000710005	EUR 17 670	EUR 1 000
52000310032	EUR 50 780	EUR 3 000
52000110008	EUR 10 610	EUR 500
52000310034	EUR 12 175	EUR 500
52000210017	EUR 25 600	EUR 2 000
52000210018	EUR 13 235	EUR 1 000
52000710013	EUR 14 080	EUR 500
52000810010	EUR 15 500	EUR 1 000
52000710009	EUR 12 000	EUR 500
52000410005	EUR 11 052	EUR 1 000
52000410006	EUR 38 837	EUR 2 000
52000810018	EUR 14 900	EUR 250
52000710026	EUR 20 657	EUR 1 000
52000410008	EUR 21 810	EUR 2 000
52000710028	EUR 12 065	EUR 1 000
52000110037	EUR 17 902	EUR 500
52000410014	EUR 11 458	EUR 1 000
52000410013	EUR 39 075	EUR 250
52000810025	EUR 10 000	EUR 250
52000310083	EUR 11 381	EUR 1 000
52000510032	EUR 14 360	EUR 1 000
52000410016	EUR 16 133	EUR 1 000
52000310089	EUR 101 643	EUR 3 000
52000810026	EUR 10 900	EUR 1 000

Reference	Amount of currency involved (converted to EUR)	Imposed fine
52000110022	EUR 29 420	EUR 1 000
52000410017	EUR 13 000	EUR 500
52000110026	EUR 11 485	EUR 1 000
52000310108	EUR 12 535	EUR 1 000
52000310109	EUR 26 889	EUR 1 000
52000110029	EUR 11 180	EUR 1 000
52000710034	EUR 10 928	EUR 500
52000410034	EUR 39 574	EUR 2 000
52000410032	EUR 11 240	EUR 500
52000410029	EUR 21 569	EUR 2 000
52000210047	EUR 19 640	EUR 2 000
52000410043	EUR 12 500	EUR 1 000
52000410042	EUR 10 000	EUR 500
52000410041	EUR 16 070	EUR 1 000
52000710036	EUR 11 550	EUR 250
52000510046	EUR 11 950	EUR 500
52000410050	EUR 10 000	EUR 1 000
52000210121	EUR 19 000	EUR 1 000
52000410053	EUR 11 020	EUR 1 000
52000110040	EUR 10 115	EUR 1 000
52000710039	EUR 31 327	EUR 2 000
52000510050	EUR 14 294	EUR 1 000
52000410059	EUR 18 774	EUR 1 000
52000410064	EUR 15 314	EUR 1 000
52000110046	EUR 35 030	EUR 2 000
52000410076	EUR 10 928	EUR 1 000
52000110048	EUR 44 000	EUR 2 000
52000110047	EUR 14 000	EUR 1 000
52000510103	EUR 29 514	EUR 250
52000310165	EUR 28 150	EUR 500
52000110056	EUR 15 725	EUR 1 000
52000510059	EUR 12 423	EUR 250
52000810037	EUR 15 000	EUR 1 000
52000210074	EUR 20 000	EUR 2 000
52000210075	EUR 21 280	EUR 2 000
52000310198	EUR 35 000	EUR 2 000
52000810043	EUR 100 000	EUR 1 000
52000810040	EUR 30 000	EUR 2 000
52000510074	EUR 10 587	EUR 1 000
52000310122	EUR 52 320	EUR 5 232
52000410090	EUR 22 359,	EUR 2 000
52000310143	EUR 12 486	EUR 1 000

Confiscation of Currency Related to ML/TF (applying c. 3.1-3.6 in R.3, c. IX.10; Confiscation of Currency Pursuant to UN SCRs (applying c. III.1-III.10 in SR III, c. IX.11):

587. Provisional measures and confiscation (as described under R.3) can be applied also in the case of cross border transportation of cash that are related to ML. For the applicability of confiscation in the case of FT, in the absence of an autonomous offence of FT, seizure and confiscation could be theoretically possible if the cash were considered within the "preparation" of a terrorist act or "participation in a terrorist organization" offenses. Authorities provided statistics on the number of cases which were transferred to FIOD for seizure for the period January–May 2010.

588. Funds and assets of persons and entities that are used for TF are frozen according to EC Regulation No. 881/2002 of May 27, 2002 and EC Regulation No. 2580/2001 of December 27, 2001 and, with regard to EU-internals, according to domestic designations pursuant to the Sanctions Act. Customs indicated that, through the border Police they would have access to suspect lists (that includes suspect for terrorism). In the case of EU/UN designated persons, the Customs Manual indicates the procedure to follow in the case in which a person's name matches with the lists.

Notification of Foreign Agency of Unusual Movement of Precious Metal and Stones (c. IX.12):

589. Within the EC, the reporting of cash and other means covers precious metals and stones. That is not the case for controls at the EC external frontiers. However, a customs declaration is required in any event when these goods are imported even if their value does not exceed the threshold value. In these cases information is exchanged with other countries under conditions set out in IX.7.

Safeguards for Proper Use of Information (c. IX.13):

590. Authorities stated that the system for reporting cross border transactions is subject to national security provisions which apply to the entire Tax and Customs Administration (*Voorschift Beveiliging).* The national security policy provides for physical protection of the terminals in use (locked rooms, restricted access to premises) and the restriction on personal access. Only designated officers have access to the systems (via authorizations by system owner). The sharing of information is restricted: the AWR and the ADW provide in what cases information can be shared with (governmental) third parties. The data which is collected is considered 'entry data'; when the data is processed it is considered as "personal" or "Police" data (in the latter case, for example, when the data is processed with investigative information) and subject to the rules on personal and Police data.

Training, Data Collection, Enforcement and Targeting Programs (c. IX.14):

591. Customs authorities receive regular training regarding the implementation of the declaration-related requirements, inspection procedures and targeting cash couriers. Dedicated training sessions on cash couriers have been held for the customs officers working at Schiphol airport and other airports in the Netherlands. The customs officials monitoring cross-border cash movements are provided with the knowledge and information they require to complete their tasks. They are also regularly provided with practical cash information updates, which contain case-specific information *e.g.*, about possible methods of concealment. For all Customs Authorities officers an electronic learning environment has been developed, including several hours of practice.

Additional Element—Implementation of SR.IX Best Practices (c. IX.16):

592. The Netherlands apply a EUR10 000 threshold for reporting of cross-border movement of currency and bearer negotiable instruments. To detect potential false declarations or disclosures and possible ML, the competent officers carry out controls, also in the form of "in-depth controls", described

earlier on. The controls are performed either randomly or on a targeted risk-based approach. Authorities stated that the data collected is also processed with a view to develop risk profiles and operational intelligence, which is shared with the local Customs offices. As mentioned under criterion IX14, the customs officials monitoring cross-border cash movements are provided with the knowledge and information they require in order to complete their tasks. There are three specially-trained cash detection dogs.

Additional Element—Computerization of Database and Accessible to Competent Authorities (c. IX.17):

593. Customs authorities maintain a computerized database. See analysis under criteria IX.4 and IX.5. The database is not accessible to the FIU, which only receives the raw data of the declarations on a weekly basis.

Statistics (R.32)

594. Only since a more sophisticated database was established in January 2010 are Customs authorities maintaining more comprehensive statistics that, in addition to overall value of cross border cash movement to/from the Netherlands (provided for 2007, 2008 and 2009, see first table below), would also include a breakdown per port of entry (with the indication of various codes for the results of the in depth controls, see second table below).

Cross-border cash movement (1889/2005-reports) in year 2007 (since June 15th 2007)			
Type of Report	**Number**	**Amount**	**Average amount**
cash to the Netherlands	595	EUR 22 990 000	EUR 39 000
cash from the Netherlands	175	EUR 5 463 000	EUR 32 000
Total	**770**	**EUR 28 453 000**	**EUR 37 000**

Cross-border cash movement (1889/2005-reports) in year 2008			
Type of Report	**Number**	**Amount**	**Average amount**
cash to the Netherlands	1 148	EUR 59 385 000	EUR 52 000
cash from the Netherlands	659	EUR 18 538 000	EUR 28 000
Total	**1 807**	**EUR 77 923 000**	**EUR 43 000**

Cross-border cash movement (1889/2005-reports) in year 2009			
Type of Report	**Number**	**Amount**	**Average amount**
import cash to the Netherlands	824	EUR 49 106 000	EUR 60 000
export cash from the Netherlands	23	EUR 25 379 000	EUR 28 000
transit of cash through the Netherlands	891	EUR 41 196 000	EUR 46 000

Cash declarations–January 1, 2010 to May 19, 2010			
Number of declarations	**Value**[1]	**Entry**	**Outgoing**
1103*	EUR 51 897.202	EUR 40 554 537	EUR 11 342 663
Code 1[2]		28	10
Code 2		74	83
Code 3		2	0
Code 4		0	1
Code 5		2	7
Schiphol (airport)	970	682	288
Maasvlakte (harbour)	97	26	71
Amsterdam (harbour)	26		26
Vlissingen (harbour)	3		3
Eindhoven (airport)	6		6
Moerdijk (harbour)	1		1
Total	**1 103**	**708**	**395**

* There were no declarations of other negotiable instruments, only cash declarations.

[1] Authorities indicated that this figures include also the amount seized, but could not provide more detailed information.
[2] Code 1: in depth control / no irregularities
Code 2: in depth control / no declaration
Code 3: in depth control / false or incomplete declaration
Code 4: detention of cash
Code 5: suspicion of money laundering

Adequacy of Resources—Customs (R.30)

595. Customs authorities appear to be adequately resourced.

596. The Customs Administration is part of the Tax and Customs Administration of the Ministry of Finance. The Director-general for the Tax and Customs Administration (*DG Belastingdienst*) leads this service. It is placed as one of the Directorates at the Ministry of Finance besides the Directorate for Fiscal Affairs, DG Budget and the Treasury. The number of staff for the whole Tax and Customs Administration is 33 260. For operational issues the Customs Administration is organized in a National Office in Rotterdam and 9 regional offices throughout the country (Schiphol PAX, Schiphol Cargo, Amsterdam, Rotterdam, Rotterdam Harbour, Roosendaal, Eindhoven, Nijmegen and Groningen). The General Director for customs is thereby responsible for prioritizing and coordinating operational customs affairs. The total staff of the Customs Administration is 5 350. At national office-level 475 staff is employed. In Rotterdam Harbour and at Schiphol (PAX and Cargo) the majority of the operational staff is located.

597. The total budget for the Tax and Customs Administration allocated for 2010 amount to EUR277 612 000 for expenditure related to staff and EUR43 600 000 for materials, which is considered adequate. There is no separate budget for Customs. At the time of the onsite visit the Customs Administration had at their disposal 3 fixed scanners, 1 re-locatable scanner, 1 extended scan-lane, 2 mobile scanners (container size cargo), 1 mobile backscatter-scanner and 3 mobile scanners. Some of these scanners can also be deployed for cash-control purposes. As mentioned earlier there are 3 sniffing dogs which are specially trained to detect cash.

Analysis of effectiveness

598. Although the introduction of the declaration requirements is relatively recent, Dutch authorities have put in place a system that works relatively well. The lack of an autonomous offence of TF could affect the implementation of some SRIX requirements (such as seizure and confiscation). The quality of the data that is shared with the FIU, which at times, has proved to be inaccurate, also affects the effective use of the information by the FIU.

2.7.2 Recommendations and Comments

599. Authorities are recommended to:

- Extend the requirements envisaged in the Dutch system to the case of shipment of currency through containerized cargo or in the case of mailing of currency or bearer negotiable instruments by a natural or legal person.
- Establish TF as an autonomous offence, and extend Customs' responsibilities also in this area.
- Consider enhancing Customs authorities powers to stop or restraint the currency, when there is a suspicion of ML and when the person has fulfilled the declaration requirements.
- Consider updating the international agreements with foreign Customs which entered into force prior to the EC 1889/2005 to specifically provide for the exchange of information also in the area of AML/CFT, if needed.
- Improve the quality of the data shared with the FIU.

2.7.3 Compliance with Special Recommendation IX

	Rating	Summary of factors relevant to s.2.7 underlying overall rating
SR.IX	**LC**	• No requirements in the case of shipment of currency through containerized cargo or in the case of mailing of currency or bearer negotiable instruments by a natural or legal person. • Quality of the data made accessible to the FIU affects the effective use of such information by the FIU. • Sanctions are not always effective.

3. PREVENTIVE MEASURES—FINANCIAL INSTITUTIONS

Regulatory Framework (Laws, Regulations and Other Enforceable Means)

600. The framework that regulates Customer Due Diligence (CDD) requirements consists of the following laws, regulations and guidance:

- The Money Laundering and Terrorist Financing Prevention Act (*Wet ter voorkoming van witwassen en financieren van terrorisme* WWFT) of July 15, 2008 which came into force on August 1, 2008. Prior to the WWFT, the Provision of Services Act of 1993 (WID) and the Disclosure of Unusual Transactions Act of 1994 (WMOT) constituted the AML framework. The WID imposed the customer identification and CDD obligations while the WMOT obligated the disclosure of unusual transactions. When the new provisions of the Third Money Laundering Directive had to be incorporated into Dutch legislation, the WID and WMOT were first merged into a law (which remained in force for a very short time) which was subsequently integrated into a single piece of legislation, the WWFT.

- The Decree of July 15, 2008, no. 305 implementing the WWFT (*Uitvoeringsbesluit Wet ter voorkoming van witwassen en financieren van terrorisme*, UBWWFT). The UBWWFT introduced amendments to several laws following the passage of the WWFT and contains the list of indicators (subjective and objective) for the reporting of transactions to the Netherlands FIU.

- The Regulation implementing the WWFT of July 23, 2008 (*Uitvoeringsregeling Wet ter voorkoming van witwassen en financieren van terrorisme*, URWWFT).

- The Explanatory Memorandum to the WWFT. In the Dutch legal system, laws and regulations are accompanied by a memorandum that, inter alia, explains the aim of the law or regulation and describes in greater detail the scope of the various provisions and requirements. Courts refer to these explanatory memoranda when interpreting the laws and regulations to which these memoranda are associated. The authorities stated that supervisory authorities also refer to these memoranda.

- Guidance published by the DNB in "Open book on Supervision" in the form of "Questions and Answers" (hereinafter: Q & A).

- Joint guidance issued by the DNB and the Dutch Bankers Association on the Basel Committee on Bank Supervision's report *Customer Due Diligence for Banks* first published in 2001 and updated in 2006.

601. The WWFT along with the UBWWFT and the URWWFT provide the foundation for the Netherlands AML/CFT framework for financial institutions and DNFBPs. For the purpose of this assessment the UBWWFT and the URWWFT are considered as "regulation", as defined by the FATF, as they were authorized by a legislative body, impose mandatory requirements which can be sanctioned for non-compliance. References will be also made to the Explanatory Memorandum, the Q & A, and the

guidance issued regarding the Basel Committee, but they are not considered to amount to "other enforceable means". The Explanatory Memorandum has a mere interpretative nature (although it is interesting to note that in some instances, the Memorandum seems to establish additional requirements to the WWFT and its implementing regulations, not always consistently with these implementing regulations or with the Q & A) and it is not enforceable. Even when it would appear to set additional requirements, non-compliance with these requirements could not be sanctioned. The assessors also deem that the Q & A and joint DNB/ DBA guidance do not amount to "other enforceable means," because they are not enforceable.

602. The AML/CFT legal framework regulating CDD is also complemented by other laws and regulations:

- The Act on Financial Supervision (*Wet op het financieel toezicht*-Wft), which came into force in January 2007, consolidating the law on supervision of banks and, the law on the Supervision of Insurance Companies. The Wft, along with the Decree on Prudential Rules pursuant to the Act on Financial Supervision (*Besluit prudentiële regels Wet op het financieel toezicht* BPR-Wft) and the Decree on Supervision of the Conduct of Financial Enterprises pursuant to the Act on Financial Supervision *(Besluit Gedragstoezicht financiële ondernemingen Wet op het financieel toezicht* BGFO Wft) provide for further rules, particularly regarding the integrity measures. The relationship between the integrity requirements and the AML/CFT obligations is discussed in more detail in the assessment of Recommendation 15.

- *Regeling afgeschermde rekeningen Wft*, a regulation issued in 2006 by the DNB on protected accounts amended, after the onsite mission, by the DNB regulation N.V. of August 26,2010.[76]

Scope

603. The WWFT covers all financial institutions as defined by the FATF. The following table shows which type of activities fall within the scope of the WWFT:

Financial activity	WWFT
Acceptance of deposits and other repayable funds from the public	Article 1 (1) (a) 1°
Lending	Article 1 (1) (a) 1° and 2°
Financial leasing	Article 1 (1) (a) 1° and 2°
The transfer of money or value.	Article 1 (1) (a) 1°, 2°, and 4°
Issuing and managing means of payment (*e.g.* credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).	Article 1 (1) (a) 1°, 2°, and 17°
Financial guarantees and commitments.	Article 1 (1) (a) 1°, and 2°,
Trading in: (a) money market instruments (cheques, bills, CDs, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading.	Article 1 (1) (a) 1°, 2°, 6 and 7°
Participation in securities issues and the provision of financial services related to such issues.	Article 1 (1) (a) 1°, 2°, 6 and 7°
Individual and collective portfolio management.	Article 1 (1) (a) 1°, 2°, 6 and 7°
Safekeeping and administration of cash or liquid securities on behalf of other persons.	Article 1 (1) (a) 1°, 2°, 6 and 7°
Safekeeping and administration of cash or liquid securities on behalf of other persons.	Article 1 (1) (a) 1°, 2°, 6 and 7°

76 Protected accounts are accounts in which the customer's identity is invisible or otherwise protected during the transaction processing in that only an account number, a number or a code word is used, whereas the customer's identity is known at the credit institution or credit institution's branch.

Financial activity	WWFT
Otherwise investing, administering or managing funds or money on behalf of other persons.	Article 1 (1) (a) 1°, 2°, 6 and 7°
Underwriting and placement of life insurance and other investment related insurance.	Article 1 (1) (a) (5)
Money and currency changing.	Article 1 (1) (a) (4)

Customer Due Diligence and Record Keeping

3.1 Risk of money laundering or terrorist financing

604. As discussed under criterion 5.9., the WWFT, following the EU third Anti-Money Laundering Directive lists institutions/products which are exempted from CDD (Articles 6 and 7 of the WWFT). In addition to these the WWFT provides that by order in council customers other than those designated by Article 6 can also be subject to the same regime. Article 7 (3) WWFT stipulates also that additional products or transactions to which CDD measures do not apply may be designated by council. Article 3 of the UBWWFT does so by providing that Article 7 (1) and (2) of the WWFT shall apply mutatis mutandis to Article 3 (3) of the Commission Directive 2006/70/EC of August 1, 2006[77] which designates additional products or transactions with are a low risk of money laundering or terrorist financing such as savings products for the benefit of children and certain forms of leasing agreements. Finally, pursuant to Article 3 (7) the Minister of Finance may grant temporary or permanent dispensations from the CDD measures envisaged by Article 3 (1) and (2). The authorities informed the mission that, to date, one dispensation was granted to a company which was established by the five largest Dutch public transport companies to implement a single payment system for public transport in the Netherlands, based on the low risk of ML/TF and the small amounts involved in these transactions.

605. European "equivalence"/ Third European Directive on AML/CFT

606. Throughout this section of the report there are references to the applications of exemptions or certain specific "low-risk" measures, designated within the WWFT, with respect to institutions, transactions, counterparties, etc, that originate from or are based in other EU Member States. These designations are derived from the EU-wide regulations and directives, which work on the presumption that all Member States have AML/CFT regimes of a minimum common standard, and can be treated, de facto, and sometimes de jure, by each Member State as being part of its domestic environment. While in certain very specific cases (*e.g.*, SR.VII), the FATF has recognized within its standards the validity of the single European framework, there is no presumption by the FATF that the treatment of all EU Member States as being equivalent is appropriate in terms of a country fulfilling the requirements of the FATF Recommendations.

607. In addition to EU Member States the Dutch AML/CFT framework provides that certain gateways, exemptions and "low risk" options also apply with respect to third countries outside the EU, on the basis that they are deemed to apply the FATF standards on an "equivalent" basis to those applied within the EU.

608. This stems from a common understanding between EU Member States on the criteria for the recognition of third countries equivalence under the EU 3rd Anti-Money Laundering Directive. This understanding was reached on the basis that a level playing field for credit and financial institutions on the method to be applied for the identification of third countries imposing requirements equivalent to those of

77 Laying down the implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis.

the Third Directive was required. According to the understanding, any FATF member that receives a Partially Compliant (PC) or above on FATF Recommendations 1, 4, 5, 10, 13, 17, 23, 29, 30 and 40 and Special Recommendations II and IV is considered 'equivalent.'

609. This list, which was voluntarily established, includes most (but not all) non-EU Member jurisdictions of the FATF as well as certain French and overseas territories of the Kingdom of the Netherlands and U.K. Crown Dependencies.

610. The Dutch authorities have not undertaken an independent and autonomous risk assessment of the countries on the list, although they have participated in the joint assessment of such countries undertaken at the EU-level. The Dutch authorities explained that this assessment was conducted by looking at the compliance of these countries to certain FATF Recommendations, mostly by looking at the countries' mutual evaluation and follow up reports. They also informed the assessment team that, at the EU-level, they are supporting a revision of the current list, including an express indication that the list constitutes only a refutable presumption, based on risk, for the application of simplified CDD.

611. During the assessment, the team did note that financial institutions carried out their own risk assessment which incorporated country risk, and that they therefore did not accept the exemptions as universally low-risk. Consequently, where relevant in this report, the assessors have taken the view that the generic categorization of all EU Member States and other FATF member jurisdictions as adequately applying the FATF standards is unreasonable, in the absence of a proper risk assessment by the authorities that takes into account the specific risks for the Dutch environment. It has also to be noted that a few Member States of the EU still fail to fully implement the provisions of the Third EC Money Laundering Directive, which provides the basis for Member States' comparability, and the assessment reports of other FATF member jurisdictions which have implemented the Directive show significant variations in the application of the standards.

612. It is also important to note that this assessment does not address the effective transposition of the Third EC Money Laundering Directive into national law by the Netherlands, but rather the level of compliance by the Netherlands with the FATF standards. Therefore, although there may be circumstances where the Dutch legislation and practice are entirely compatible with the Directive, the assessors have noted where, in their view, the provisions do not comply with the FATF standards.

3.2. Customer due diligence, including enhanced or reduced measures (R.5 to 8)

3.2.1. Description and Analysis

The principles-based approach in the Netherlands

613. Before analyzing in detail CDD measures envisaged by the Dutch legislation it should be noted that the Dutch system of preventive measures relies on the risk-based approach and the principles-based approach, which, according to the authorities, represent the foundation of the Dutch AML/CFT regime.

614. While the Netherlands formally introduced the risk-based approach in 2008 with the implementation of the WWFT, the concept of the risk-based approach to customer due diligence measures had been introduced by the 2001 Basel CDD report which was later developed into guidance for the Dutch financial sector through close coordination between the Dutch Banking Association (*Nederlandse Vereniging van Banken*–NVB) and the Dutch Central Bank.

615. The risk-based approach is complemented by the principles-based approach, which prescribes a specific outcome for CDD measures, which financial institutions must achieve. This approach does not provide a required path to reach the outcome such as how specifically financially institutions should meet

the obligations of identifying and verifying the identity of the customer. As long as the final outcome is achieved—for example, the customer is identified and his/her identity verified—the way in which this was achieved is irrelevant. This approach is intended to permit financial institutions to adopt measures for CDD which are not prescriptive or detailed and allow the financial institutions to develop an individualized approach to CDD.

616. The principles-based approach and the risk-based approach complement one another as both rely on financial institutions to implement AML/CFT provisions based on the circumstances of the individual institutions. A financial institution must meet the obligations set out on the WWFT (principles-based), but may use the risk based approach to implement the requirement. This combination is intended to provide financial institutions with flexibility to implement the risk based approach to achieve the desired outcome.

617. As a result of the implementation of the risk based approach in the Netherlands, financial institutions are expected to conduct a risk assessment of each customer at the start of a business relationship and the DNB has clearly set the expectation that this is the basis of implementing the risk based approach.

Prohibition of Anonymous Accounts (c. 5.1):

618. Although there is no explicit provision that prohibits financial institutions to keep anonymous accounts or accounts in fictitious names, this can be inferred from Article 5 of the WWFT, which states that an institution is not permitted to enter into a business relationship or carry out a transaction if it has not performed CDD as referred to in Article 3 (a) (b) and (c) when entering into a business relationship, conducting incidental transaction or if there are indications that the customer is involved in money laundering or terrorist financing.

619. Pursuant to Article 14 (2) BPR Wft, Article 12 (2) BGFO Wft and Article 26 (2) BGFO Wft, financial institutions have to establish procedures and measures with regard to determining the identity of clients and the verification thereof.

620. Although financial institutions cannot keep anonymous accounts or accounts in fictitious names, they are permitted to keep "protected" accounts. These are accounts in which the account holder, rather than by name, is referred to by a number or code word (that is not a fictitious name). The DNB issued the Regulation on protected accounts under the Wft on December 6, 2006 (*Regeling afgeschermde rekeningen* Wft) which defines a "protected account" as an account in which "a balance of money, securities, precious metals or other valuables may be held and in respect of which the customer's name and identifying information is unseen or otherwise protected during transaction processing in that only an account number, a number or a code word is used, whereas the customer's identity is known at the credit institution or credit institution's branch." The Regulation requires financial institutions to keep a central register for the protected accounts and appoint an administrator for the central register.

621. The Regulation further stipulates that the credit institutions and their branches "shall not open protected accounts for any purpose other than to protect the privacy and safety of customers or to prevent the abuse of inside information" and clearly establishes that the credit institution should comply with the CDD requirements envisaged by the law (by requiring that, at a minimum, the central register contain the data which is subject to registration under the law)[78]. At the time of the assessment, the CDD requirements which are referenced by the Regulation were those stipulated by the Identification Services Act, which was in force prior to the WWFT.

78 For the CDD requirements under the Identification Services Act, please refer to Articles 2 and 3 (identification) and 6 (record keeping).

622. The Regulation was updated subsequent to the onsite visit and now refers to some provisions of the WWFT (notably the notion of "customers' and the obligation of record keeping). While it is clear that the purpose of these protected accounts is only limited to the protection of the privacy and that existing CDD requirement are to be applied, authorities could fine tune the revised legal regime regarding: 1) the lack of a transitional regime to clarify what rules are applicable to protected accounts opened prior to the entry into force of the new regulation; 2) the circumstance in which the regulation references the definition of customer (which does not encompass the definition of the beneficial owner); 3) the shortcomings noted with regard to the transitional regime envisaged by the WWFT[79] and with regard to the record keeping obligation[80], all of which could pose a theoretical risk of ML. Of more concern is the fact that the regulations are silent with regard to access to data contained in the data register by the compliance unit (see also the issues noted under Recommendation 15 with regard to the power of the compliance unit to access to data). This point should also be clarified in the Regulation.

623. Although the possibility cannot be ruled out that there may be protected accounts for which the CDD related information may be incomplete (with regard to the verification of the customers or the identification or verification of the beneficial owners), discussions with the private sector revealed only a small number of protected accounts held by financial institutions, primarily for privacy of the customer who in some cases included the royal family. The financial institutions had either already eliminated the accounts or had plans in place to do so, except in the case of the royal family where they intended for privacy and security, to keep the accounts protected. Overall, there seemed to be recognition that there was no legitimate purpose to having protected accounts and financial institutions met by the team indicated that they are seeking to remove them accordingly and are not planning to open new protected accounts.

When is CDD required

624. The WWFT clearly lays out the situations in which CDD is required. Article 3 of the WWFT obliges financial institutions to undertake CDD in the following circumstances:

- When entering into a business relationship in or from the Netherlands (Article 3.3. (a)).

- If they conduct an incidental transaction in or from the Netherlands for the customer with a minimum value of EUR15 000, or two or more related transactions with a minimum joint value of EUR15 000 (Article 3.3. (b). The Q & A on the WWFT issued by the DNB provides guidance and examples of 'related transactions.' These are described as transactions that are related on the basis of the type of transaction and the amounts involved such as where a person performs several transactions in one day, or who within a couple of days deposits cash into an account for which he/she is not the account holder.

- If there are indications that the customer is involved[81] in money laundering or terrorist financing (Article 3.3. (c). Additionally, Article 3.3 (e) WWFT requires that financial institutions perform customer due diligence when the risk of an existing customer's involvement in money laundering or terrorist financing gives cause to do so.

79 The transitional provision of the WWFT basically exempts financial institutions from the application of the CDD related requirements introduced by the WWFT to existing customers that were identified under the previous AML/CFT regime (see discussion under criterion 5.17).

80 As noted under the analysis of R10 the record keeping requirements do not apply to beneficial owner-related CDD data.

81 The authorities explained that the term "involved" in ML or TF, with reference to "indications," describes a situation that comprises also a simple suspicion of ML or TF.

- If they doubt the reliability of customer identification information previously obtained from the customer.

625. In addition, under Article 5 (2) of the EU Regulation 1781/2006 which implements directly throughout the European Union the provisions governing wire transfers (see discussion of SRVII), a payment services provider, before transferring funds, has to identify all customers, and verify identity whenever the transfer is of a value of EUR1 000 or more.

626. It is important to note that, as mentioned earlier, the WWFT explicitly waives the broader customer due diligence requirements in a certain number of "low-risk" circumstances specified under Articles 6 and 7. These (and the potential difficulties arising from them) are described in more detail below when discussing the simplified due diligence arrangements.

Identification measures and verification sources (c. 5.3):

627. Article 3 (2) (a) WWFT requires financial institutions to identify the customer and verify the customer's identity. According to Article 1 (1) (b) WWFT the customer is the natural or legal person with whom a business relationship is established or on whose behalf a transaction is carried out. Article 1 (1) (c) WWFT and Article 1 (1) (d) WWFT clearly distinguish between "identification" (defined as "statement of a person's identity") and "verification of identity" (defined as "establishing that the identity stated corresponds with the actual identity").

628. While the definition of "customer" refers to both natural and legal persons it does not specifically encompass legal arrangements (such as trusts). A reference to trusts is to be found in the context of the obligation to verify the identity of the beneficial owner (under Article 3 (2) (b) WWFT). Dutch law does not provide for the establishment of domestic trusts or similar legal arrangements, however, the Netherlands has ratified The Hague Convention on the Law Applicable to Trusts and their Recognition on November 28, 1995 and therefore recognizes that trusts set up under foreign law have legal effect within the Dutch system. Foreign trusts are administered in the Netherlands and the private sector confirmed that some financial institutions hold foreign trust accounts, although in very low numbers. No reference was made by financial institutions met by the missions to funds maintained by other legal arrangements other than trusts.

629. Considering that the phenomenon appears limited and the practice of the financial institutions met by the missions (in general, foreign trusts were seen as high risk and as result some financial institutions did not accept foreign trusts as customers and others treated the customers as high risk and subjected the account to supplemental due diligence), this does not seem to be a material deficiency.

630. Article 11 (1) WWFT stipulates that the identity of the customer (when a natural person; a legal person incorporated under Dutch law having its registered office in the Netherlands) must be verified on the basis of documents, data or information from a reliable and independent source. Pursuant to Article 4 (1) of URWWFT the identity of a natural person may be verified *inter alia* on the basis of a valid passport. This includes national, foreign, diplomatic and service passports, as well as a valid Dutch identity card, driving license, or a card or driving license issued by a competent authority in another Member State. The travel documents of refugees and aliens and the aliens documents issued under the Aliens Act 2000 are also accepted. These documents are considered to be reliable, although the Explanatory Memorandum to the URWWFT seems to imply that a broader range of other documents can be used, as long as they are from an independent source. The Explanatory Memorandum clarifies that this list of documents is not exhaustive and that the verification may also take place on the basis of other documents, data and information from an independent source. While this approach stems from the principles-based approach

assessors think that a mandatory list of documents would be preferable to ensure that the documents used in the identification and verification process are both reliable and from an independent source.

631. Pursuant to Article 3 (2) (a) and (b) and Article 11 WWFT financial institutions must also identify and verify customers that are legal persons, although the type of documents, data and information that financial institutions are obligated to use in the process vary. In the case of (*i*) a legal person incorporated under Dutch law that has its registered office in the Netherlands, or (*ii*) of a foreign legal person based in the Netherlands, Article 11 (2) WWFT stipulates that the identity of the legal person must be verified on the basis of documents, data or information from a reliable and independent source. Article 4 (2) UR WWFT provides examples of the types of documents which may be used in these circumstances to identify and verify the identity of the legal entities mentioned under (*i*) and (*ii*):

- An extract of the Commercial Register kept by the Chamber of Commerce and Industry.
- A deed or statement drawn up or issued by a lawyer, civil-law notary, junior civil-law notary or comparable independent legal profession based in the Netherlands or in another EU Member State.
- For religious denominations and bodies, (a) a document showing that the institution is a member of the *Interkerkelijk Contact Overheidszaken (*CIO), through an on-line database; (b) a document classifying the organization as a public benefit organization as referred to in Section 6.33 (1)(b) of the Income Tax Act 2001.

632. As in the case of natural persons this list is not exhaustive, as clarified by the Explanatory Memorandum to the URWWFT and other documents from an independent source may be used.

633. Article 4 (3) of the URWWFT, as explained by its Explanatory Memorandum, refers to the case of partnerships and associations without legal personality. The provision requires that in these instances the identity of the customer may be verified on the basis of documents, data or information from a reliable and independent source.

634. The situation is different if the customer is a foreign legal entity not based in the Netherlands (or in the EU). In this case Article 11.3 requires the identity to be verified "on the basis of documents, data and information that are reliable and customary in international commerce, or on the basis of documents, data or information that have been recognized by the law as a valid means of identification in the customer's home State." There is no indication in the WWFT that when the customer is a foreign legal entity not based in the Netherlands these documents should be from an "independent" source. Moreover, there is no indication of the types of documents or data which may be presented, nor on how the legal status of the legal entity may be verified. Only for foreign legal entities based in the EU does the URWWFT refer to a deed or statement drawn up by an independent legal professionals based in the Netherlands or in another Member State.

Identification of Legal Persons or Other Arrangements (c. 5.4):

635. There are no provisions in the WWFT or in other laws or regulations which obligate financial institutions to verify that a person purporting to act on behalf of the legal entity is so authorized. This is confirmed by the fact that the record-keeping obligation does not encompass any provisions/acts regulating the power to bind the legal person or arrangement.

636. The obligation to identify and verify the identity of the person who is purporting to act on behalf of the customer can only be implicitly inferred from Article 33 (1) (a) (1), which sets forth record keeping

requirements: the provision states that an institution "that has identified the customer or business relationship and verified the identity" should keep various CDD-related data of the customer "as well as of the person acting on behalf of the customer" (for which financial institutions are required to keeps records concerning the "name and date of birth").

637. The obligation to verify the legal status of the legal person or arrangement can be inferred, to some extent, from the provisions that require identifying and verifying the identity of a customer that is a legal person, (discussed under criterion 5.3.) and the record-keeping requirements (Article 33). However, only in the case of legal persons incorporated under Dutch law does the identification obligation require a copy of the deed of incorporation and, for record-keeping purposes, the legal form and the address.[82] There are no requirements to obtain the name of trustees or directors or to obtain provisions regulating the power to bind the legal person or arrangements.

638. In practice, financial institutions found identifying and verifying the identity of the legal person and the status for legal persons formed outside of the Netherlands very difficult. In some cases, financial institutions sent foreign resident customers to notaries in the Netherlands to have them produce a statement to certify the identity and legal status of the legal person, which should imply that the notary conducts the additional due diligence required. The "outsourcing" of this obligation, made possible by the fact that the URWWFT allows financial institutions to verify the identity of customers that are legal person based on a statement produced by a notary, raises questions about the capacity of financial institutions as well as about the due diligence which can be conducted by notaries to provide the required certification in the case of foreign legal persons.

Identification of Beneficial Owners (c. 5.5; 5.5.1 and 5.5.2):

639. Article 3 (2) (b) WWFT obliges financial institutions, "where applicable, to identify the beneficial owner and take risk-based and adequate measures to verify the beneficial owner's identity" and, in the case of a legal person, a foundation or a trust,[83] "to take risk-based and adequate measures to gain insight into the customer's ownership and control structure".

640. Article 1 (f) WWFT defines the beneficial owner as the:

1. "Natural person who holds a share of more than 25 percent of the issued capital or can exercise more than 25 percent of the voting rights in the shareholders' meeting of a legal person other than a foundation, or can exercise actual control over this legal person, unless this legal person is a company subject to disclosure requirements as referred to in Directive 2004/109/EC of the European Parliament and of the Council of December 15, 2004 on the harmonization of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC (OJEU L 390), or to requirements of an international organization which are equivalent to that Directive.

2. Beneficiary of 25 percent or more of the assets of a foundation or a trust as referred to in the Convention on the Law Applicable to Trusts and on their Recognition (Treaty Series 1985, 141) or the party that has special control over 25 percent or more of the assets of a foundation or trust."

82 Interestingly, under the previous AML law there was a requirement for "foreign legal entity without a place of business in the Netherlands to obtain an extract/statement that would include, inter alia, the legal form, the corporate name, the address and house number, postcode and place of business (see Article 3, para 3 of the Act of December 16, 1993 and subsequent amendments).

83 As referred to in the Convention on the Law applicable to Trusts and their Recognition (treaty Series 1985).

641. The definition in the WWFT also refers to the person than can exercise actual control over the legal person (although there is no such reference for legal arrangements).

642. The definition of the beneficial owner in the WWFT falls short the FATF standard as it only refers to the beneficial owner of legal persons and trusts, and not, in the broader definition of the FATF, to "the natural person(s) who ultimately own or control a customer" which could also be a natural person. This element of the FATF definition specifically addresses the concept of a nominee who is the customer and may be acting on behalf of a natural person who exercises control. This issue is closely linked to financial institutions lack of obligation to determine whether a customer is acting on behalf of another person discussed later on. The definition falls short of the FATF standard also in that it does not include the person that can exercise ultimate effective control over a legal arrangement, as mentioned above.

643. The WWFT clearly establishes the obligation for financial institutions to identify the beneficial owner. With regard to the obligation to take adequate measures to verify the identity of the beneficial owner, the reference in Article 3 (2) (b) to "risk-based" measures to verify the identity of beneficial owners indicates that it might be sufficient simply to establish the name of the beneficial owner; and only in situations presenting a higher risk would the full establishment and verification of the beneficial owner's identity be made necessary. This is also confirmed by the Explanatory Memorandum where, with reference to Article 3 (2) (b) it states that the phrase 'risk-based adequate measures' "indicate that the obligation to verify the ultimate beneficial owner's identity concerns those cases which the institution believes involve a greater risk of money laundering or terrorist financing."

644. The authorities pointed out an amendment of the WWFT which was introduced in 2008 to better clarify the distinction between the obligation to "identify" the customer and the obligation to "verify" the identity, modification that was also introduced with regard to the beneficial owner. According to the authorities these amendments should be also interpreted as imposing an absolute requirement to verify (in all circumstances) the beneficial owner's identity. However this interpretation is not shared by the assessors, considering that the expression "take risk-based measures " with reference to the obligation to verify the beneficial owner's identity has remained unchanged by these amendments, and that the explanatory Memorandum is very clear in stating, as mentioned earlier, that the phrase 'risk-based adequate measures' "indicate that the obligation to verify the ultimate beneficial owner's identity concerns those cases which the institution believes involve a greater risk of money laundering or terrorist financing."

645. The Q & A re-states that the financial institutions "has to take risk-based and adequate measures to verify the identity" and that these measures should enable the institution to obtain sufficient information to verify the identity of the beneficial owner.

646. These provisions fall short of the FATF standards, which require that in all cases (unless there are specific low-risk situations), institutions take reasonable measures to verify the identity of the beneficial owners. The financial institutions met by the mission confirmed that only in greater-risk situation they would also verify the identity of the beneficial owners.

647. With regard to the FATF requirement that financial institutions, when identifying the beneficial owner and taking reasonable measures to verify the identity, should use relevant information or data obtained from a reliable source, see analysis of criterion 5.3 for an indication of the types of documents information. As for other CDD-related requirements, the WWFT purports to follow a "principles based approach" with regard to obligation to establish ultimate beneficial ownership and to identify and verify the identity of the beneficial owner. The Explanatory Memorandum stresses that there are no rules regarding "how" financial institutions "must organize the CDD requirements" and that only the "result that the institution must achieve from due diligence is described."

648. The same approach is followed with regard to the identification and verification of the beneficial owner, where the risks presented by the customers, product or transaction should be taken into account. However the guidance available for financial institutions is insufficient. For example, in the case of legal persons incorporated under Dutch law or for foreign legal persons based in the Netherlands the Explanatory Memorandum clarifies that the obligation to identify the beneficial owner can be fulfilled by obtaining an extract from the Commercial Register. However the Commercial Register would only contain the information about the ultimate beneficial owner in cases in which the company is wholly owned by one person or in those cases in which the information was registered on a voluntarily basis by the company. The Explanatory Memorandum acknowledges this by suggesting that for customers with a potentially high risk profile "the amount of information required about the ultimate beneficial owner goes beyond the data stated in the Commercial Register". This implies that, when the risk is low, the financial institutions relying on the extract on the Commercial Register would not necessarily have identified the ultimate beneficial owner.

649. The Q & A suggest that in order to verify the identity of the beneficial owner "institutions may use public registry agencies and other public sources; ask the client for relevant data; or collect this information in some other way," which is generic and, in the case of public registry, does not necessarily imply that the ultimate beneficial owner can be identified or verified.

650. There is no direct obligation in the WWFT or related legislation requiring financial institutions to determine whether the customer is acting on behalf of another person or to take reasonable steps to obtain sufficient identification data to verify the identity of that other person. For indirect requirements stemming from the record keeping obligation, see the discussion under criterion 5.4.

651. With regard to the FATF requirement to understand the ownership and control structure of the customer Article 3 (2) (b) WWFT obligates an institution, "where applicable" to take risk-based and adequate measures to gain insight into the ownership and control structure of a legal person, a foundation or a trust. This obligation is contained in the same paragraph and uses the same language as that to verify the identity of the beneficial owner, which additional guidance and conversations confirmed only applies in high risk situations

652. With regard to the obligation to determine the identity of the natural persons that ultimately own or control the legal person/arrangement, a requirement in this respect can be inferred by the definition of beneficial owner and the relevant obligation to identify the beneficial owner in the case of legal persons (the definition of beneficial owner refers to thresholds as well as the person who can exercise actual control). With regard to legal arrangements there is an indication of thresholds, which does not per se indicate a situation of ultimate beneficial ownerships.

653. Discussions with the private sector demonstrated a clear understanding that the ultimate beneficial owner must always be identified when the customer is a legal person. However the implementation of the obligation to identify the beneficial owner, as well as the obligation to take risk based and adequate measures to verify the identity of the ultimate beneficial owner, reflected uncertainty and unpredictable results. The discussions with the private sector indicated that there are circumstances in which financial institutions are unable to determine who the beneficial owner may be, and that that there was some confusion in determining how far up the chain of legal entities they must go in order to satisfy the threshold requirement. Despite the reference to the actual control, the private sector confirmed that in cases in which no natural person owned 25 percent, the name of any shareholder would be considered sufficient. In practice, the use of a threshold also results in an emphasis on ownership over control, undermining the requirement to determine who exercise ultimate effective control. Financial institutions appear to always seek to find a shareholder rather than the person who actually controls the entity which may be one without an ownership interest.

654. In the case of legal persons, financial institutions universally rely on information from the Commercial Register to identify the legal person. In cases which were viewed as high risk, which varied from institution to institution, the Commercial Register was often used to also verify the identity of the beneficial owner. However, as described above, the Commercial Register only contains the name of the shareholder in cases in which it was 100 percent owned by one person. If no one person held a minimum of 25 percent then any shareholder would be sufficient, although the on-line Commercial Registry would not contain this information. The on-site meetings with the private sector demonstrated that, in determining beneficial ownership, there was little or no comprehension of the importance of understanding the control structure of a legal person. As a result, a fundamental element of the FATF requirements on beneficial owners is not implemented in practice, and in the cases of complex legal structures in particular, the financial institutions may not pierce through the chain and identify the ultimate beneficial owner.

Information on Purpose and Nature of Business Relationship (c. 5.6):

655. According to Article 3 (2) (c) WWFT an institution is obliged to determine the objective and envisaged nature of the business relationship.

Ongoing Due Diligence on Business Relationship (c. 5.7; 5.7.1 and 5.7.2):

656. According to Article 3 (2) (d) of the WWFT an institution is obliged, "where possible, to carry out constant monitoring of the business relationship and the transactions conducted during the existence of this relationship, in order to ensure that these tally with the knowledge which the institution has of the customer and the customer's risk profile, and to check the source of the assets where appropriate." The authorities explained that the reference to "constant" should be intended as "ongoing" and that the applicability of the obligation "where appropriate" refers to situation is which there is an ongoing relationship (as opposed to the case in which the relationship consists of a one-time act).

657. There are no obligations for financial institutions to ensure that the data and information obtained under the CDD process, such as the client risk profile and contact information, is kept up-to-date and that relevant reviews are conducted, particularly for higher-risk customers or business relationships. In practice, most financial institutions conducted an annual review of all CDD which included the physical review of client files for customers categorized as high risk, although some held such reviews only every two years, even for high-risk customers.

Risk—Enhanced Due Diligence for Higher-Risk Customers (c. 5.8):

658. In addition to the CDD-related requirements envisaged by Article 3 (2) (3) (4), Article 8 (1) WWFT requires financial institutions to perform "supplementary customer due diligence if and as a business relationship or transaction by its nature entails a greater risk of money laundering or terrorist financing." This Article states that such business relationships/transactions "may be designated by order in council," however, none have been so designated by the Dutch authorities.

659. Article 8 WWFT aims at establishing a general requirement for financial institutions to apply enhanced due diligence measures in the case of greater risk of ML/FT and then lists three situations (*i.e.* non face-to-face business, correspondent banking and PEPs, which are discussed under R. 8, 7 and 6 respectively) in which the enhanced due diligence should apply. The authorities explained that the obligation to conduct enhanced due diligence is general and must be geared to the risk and that the three cases mentioned by the WWFT in which enhanced customer due diligence should apply are not exhaustive. This is confirmed by the Q & A issued by DNB, according to which the risk assessment conducted for each customer by the financial institution should identify additional circumstances in which supplementary due diligence is required and permit the financial institution to conduct appropriate due

diligence. However the Explanatory Memorandum's reference to Article 8 explains that this provision, "*lists* the various risks and the corresponding supplementary measures", suggesting that enhanced due diligence applies only to these three scenarios and thus weakening the general requirement of the WWFT that financial institutions pro-actively identify situation of greater risks that require enhanced due diligence.

660. Discussions with financial institutions reflected that, in practice, the risk profiles developed and applied by institutions effectively identified a range of high risk scenarios which went beyond the list in the WWFT as well as the examples in the guidance. In these situations of identified higher risk, financial institutions did conduct supplementary due diligence and were implementing the WWFT as the authorities intended.

661. In the description of the risk assessment financial institutions undertake for each client, the Q & A issued by the DNB also provides examples of some products which may be low or high risk. Savings products or consumer credits may have lower inherent risk because of the long term nature of the products, while back-to-back loans, trade finance, or real estate transactions may be higher risk because of their complexity or lack of transparency. However, there is no guidance regarding the measures financial institutions should take in these cases.

662. As for other CDD-related measures, including the case of enhanced CDD, the WWFT and the guidance issued pursuant to it relies on the principles - based approach which provides an intended outcome the supervisors expect financial institutions to reach. That's why, authorities explained, there was no indication (except for the three cases mentioned above) of what enhanced due diligence measures the financial institutions should undertake in situations of greater risk of ML/FT. The 2006 joint guidance issued by the DNB and the Dutch Bankers Association on the Basel Committee states that in normal and increased risk categories, the person who decides to accept the client should take place at "a more elevated level." The risk assessment should enable financial institutions to develop a risk profile incorporating a variety of factors including, among other elements, client, product and country risk. The profile results in the classification of a client into a risk category, the number of which varied from institution to institution, but all had a minimum of two rankings ranging from low to unacceptable.

663. In practice, the implementation of this provision varied based on the risk assessment conducted by the financial institution for each customer but seems satisfactory overall, although financial institutions could benefit from additional guidance, especially with regard to what constitutes appropriate measures to take in the case of enhanced CDD. PEPs were always considered high risk; however, correspondent banking relationships with institutions in an EU Member State or a State designated by the Ministry of Finance were considered low risk by some financial institutions as a result of Article 6 of the WWFT which exempts these institutions from CDD. Non face-to-face situations were also not seen as high risk in situations in which the introducer was in the Netherlands and the product was viewed as low risk. Financial institutions did consider additional circumstances as high risk, but it varied by financial institution. Small and medium sized legal persons, international private banking, energy commodity and trade, as well as countries that ranked high on the Transparency International Corruption Index were given as examples of criteria which would put a customer into a high-risk category and for which enhanced due diligence would be conducted. The elements of enhanced due diligence varied by risk and institution, but generally included a more in-depth customer profile which incorporated additional information about the customer and the intended financial activity.

Risk—Application of Simplified/Reduced CDD Measures when appropriate (c. 5.9; Risk—Simplification/Reduction of CDD Measures relating to overseas residents (c. 5.10):

664. Rather than identifying circumstances in which simplified CDD can be conducted, Article 6 WWFT provides a list of customers exempt from the CDD requirements stipulated by Article 3 (1) (the obligation to undertake customer due diligence, which, as the authorities confirmed, includes the measures detailed in paragraph 2 of the same article), Article 3 (3) (a)(b)(d) and (4) and Article 4 (1). These customers are exempt from the CDD provisions that address the key CDD components of identifying and verifying the customer's identity, identifying the beneficial owner and verifying its identity, determining the purpose and intended nature of the business relationship, and conducting ongoing monitoring of the relationship. Therefore, these are not reduced or simplified CDD measures as suggested by the standard, but exemption from any CDD except in the case in which there are indications that the customer is involved in money laundering or terrorist financing or where Article 8 (10) WWFT is applicable.

665. The following customers are exempt from CDD:

1. Credit and financial institutions, financial enterprises[84] money transfer offices, life insurers, investment firms, collective investment schemes and financial service providers (acting as a broker in respect of life insurance), which have their registered office in the Netherlands or in another EU state, as well as branch offices operating in the Netherlands of foreign institutions undertaking the activities mentioned above.

2. Institutions undertaking the activities mentioned above and their branches, which have their registered office in a non-Member State, if statutory regulations apply to the institution in that State which are equivalent[85] to the CDD provisions set out in Article 3 and to the enhanced CDD provisions set out in Article 8 (1).

3. Listed companies whose securities are admitted to trading in a Member State, as well as listed companies from a non-Member State that are subject to disclosure requirements consistent with EU legislation.

4. Third-party accounts of civil-law notaries, lawyers and other independent legal professionals in an EU Member State or, if the account holders are not based in a Member State, 1) there must be statutory regulations to prevent money laundering and terrorist financing that are equivalent Dutch law; 2) the information on the identity of the customers is available on request to the institution concerned.

5. Dutch government bodies and bodies that are entrusted with public functions pursuant to EU-related treaties, whose identity is known, whose activities and accounting practices are transparent; and that are accountable to a Community institution or to authorities of a Member State, or in respect of which appropriate check-and-balances procedures exist to control their activities.

84 These are companies undertaking activities listed in section 14 of Annex I to the EC Directive 2006/48/EC.

85 Article 6 (4) empowers the Minister of Finance to designate the states referred to in Article 6(1)(b). The ministerial designation was made with the URWWFT, which, in Article 3 has designated the following States as having "equivalent" statutory regulations: Argentina, Aruba, Australia, Brazil, Canada, French Polynesia, Guernsey, Hong Kong, Japan, Jersey, the Isle of Man, Mayotte, Mexico, the Netherlands Antilles, New Zealand, the Russian Federation, Singapore, Saint Pierre and Miquelon, the United States of America, Wallis Archipelago and Futuna Island, South Africa and Switzerland.

666. Article 7 WWFT provides additional exemptions for business relationships and transactions that concern life insurance agreements, products relating to pensions, and electronic money. These exemptions are subject to a variety of limits in terms of amount, type of counterparty, residence of counterparty and type of business[86] (for the details of these exemptions, see Article 7 of the WWFT).

667. Article 6 (2) obligates institutions to gather sufficient data in order to establish whether the exemption should apply and authorities explained that in all circumstances financial institutions are expected to gather enough information to assess whether the customer meets the criteria for exemption. The Q & A issued by the DNA provide guidance regarding what information is deemed sufficient in order to ascertain whether a customer is exempt, in particular an extract from the Commercial Registry or entries in public register or other official public documents.

668. Authorities also explained that this exemption does not override the risk assessment conducted on behalf of customers. The DNB issued Q & A clarify situations in which a client's country of residence may play a role in applying simplified due diligence. It states that this provision does not nullify Article 8 of the WWFT which require supplementary due diligence if and as a business relationship or transaction entails a greater risk of money laundering or terrorist financing. The guidance also refers to the FATF warnings on specific countries and explains that institutions are free on the basis of their own risk assessment, not to apply simplified due diligence. However, as clarified earlier, this guidance is not enforceable.

669. In practice financial institutions were able to confirm an exemption based on publicly available information, however circumstances in which a company had to demonstrate the exemption based on additional documents were more challenging.

670. Authorities also pointed to the explanatory memorandum to the URWWFT, which states, with regard to the countries that are considered to be "equivalent" that an institution is free—based on its own risk assessment—not to apply the exemptions to institutions that have registered office in a state considered "equivalent", but this does not amount to a legal obligation. Meetings with the private sector confirmed that, in practice, the general trend is to consider these customers exempted by default.

671. This approach raises a number of issues about the impact on the integrity of some of the CDD measures. The list of exemptions has been taken directly from the Third EC Money Laundering Directive, which allows exemptions for listed companies, beneficial owners of pooled accounts held by notaries, domestic public authorities or customers meeting the technical criteria established in Directive 2006/70/EC, including customers who are credit or financial institutions with the EU, or in third countries that impose requirements equivalent to those of the Directive. As explained in section 3.1 of this report, the Dutch authorities have participated in the risk analysis conducted by the European Union but have not undertaken any formal risk analysis to determine whether the circumstances are appropriate to the local environment.

672. The exemption from all CDD for the listed institutions raises a number of fundamental concerns about the CDD process. The FATF standard does allow for reduced or simplified due diligence, however this assumes some level of CDD in all circumstances. The WWFT provides for a blanket exemption from

86 These exemptions specifically apply to three categories:

- life insurance agreements, whereby the annual premium owed is €1 000 or less or whereby the one-off premium is €2 500 or less;
- products related to a pension as referred to in Section 1 of the Pensions Act;
- or electronic money whereby if the monetary value stored on the electronic carrier or stored remotely in a central accounting record 1) cannot be reloaded the maximum amount does not exceed €150; 2) can be reloaded the total amount of the transactions that can be conducted during a calendar year does not exceed €2 500.

all CDD measures in Article 3 WWFT. In the circumstances provided under the WWFT, it is apparent that, in the defined set of "low-risk" circumstances, institutions are specifically exempted from the vast majority of the key elements of the CDD process. Although Article 6 para. 2 of the WWFT requires financial institutions to gather "sufficient data" to determine whether a customer qualifies for the application of the exemptions, there is no further clarification on what "sufficient data" means and the provision's scope seems limited to the process of determining whether the customers qualifies for the exemption.

673. More specifically it has to be noted that the removal of the obligation for institutions to undertake ongoing monitoring of the accounts to ensure that the transactions are consistent with the institution's knowledge of the customer, can affect the requirement to identify unusual transactions. Another area of particular concern is the fact that the exemption applies even in cases where there are doubts about the veracity or adequacy of the information identifying the customer or beneficial owner. It might be argued that there is some logic in this exemption since an institution would not have reliable information in the first instance, but the overall tone of the provision runs counter to the concept that institutions should have core accurate information on their customers, whatever the risk.

Risk—Simplified/Reduced CDD Measures Not to Apply when Suspicions of ML/TF or other high-risk scenarios exist (c. 5.11):

674. Simplified CDD is not permitted when there are indications that the customer is involved in money laundering or terrorist financing. Article 6 (1) WWFT and article 7 (1) WWFT specifically exclude article 3 (3) (c) and (e) WWFT).

675. Additionally, according to Article 8 (1) WWFT enhanced CDD is required if and as a business relationship or transaction by its nature entails a greater risk of money laundering or terrorist financing.

Risk-Based Application of CDD to be consistent with Guidelines (c. 5.12)

676. Article 3 (4) WWFT stipulates that an institution "may gear the customer due diligence to the risk sensitivity of the type of clients, business relationship, product or transaction to money laundering or terrorist financing." The guidance issued by the DNB as Q & A provides greater clarification of this obligation by stating that on the basis of Article 3 (2) under (d) WWFT, "institutions have to draw up a risk profile of their clients." The Q & A provides specific examples of types of customers, products, and sectors to which different risk may be assigned and consequently the varying due diligence applied.

677. Discussions with financial institutions confirmed the implementation of an approach to establishing a risk profile for every customer which resulted in categorizing them in one of three to five categories of risk ranging from low risk to unacceptable depending on the institution. The nature and extent of CDD appeared to vary according to the risk profile, as is appropriate.

Timing of Verification of Identity—General Rule (c. 5.13)—Treatment of Exceptional Circumstances (c.5.14 and 5.14.1):

678. Article 4 (1) WWFT requires that the customer and the beneficial owner are identified and their identities verified before the business relationship is established or an occasional transaction is carried out. However, this provision also goes on to state that the verification of the customer/beneficial owner may be completed while the business relationship is being established "if this is necessary for an uninterrupted provision of services and if the risk of money laundering or terrorist financing is low" (Article 4 (2) Life insurance companies are permitted to identify the beneficiary of a policy and to verify the identity after the business relationship has been established, although in this case the identification/verification must take place at or before the moment of payment (or when the beneficiary wants to exercise the rights of the policy).

679. Finally, a credit institution is permitted to open an account before the customer's identity has been verified, "if it ensures that this account cannot be used before verification has taken place" (Article 4 (4) WWFT).

680. There are no explicit requirements or guidance to adopt risk management procedures for situations in which the customer is permitted to utilize the business relation prior to verification, although this can be inferred by the requirement that this is only applicable provided that the risk of money laundering and terrorist financing is low.

Failure to Complete CDD before commencing the Business Relationship (c. 5.15 Failure to Complete CDD after commencing the Business Relationship (c. 5.16):

681. According to Article 5 WWFT, a financial institution is not permitted to enter into a business relationship or carry out a transaction if it 1) has not performed customer due diligence pursuant to Article 3 WWFT, or if 2) the "customer due diligence review did not produce the result referred to in Article 3 (2) including the identification and verification of the customers, and where appropriate, the beneficial owner, as well as determining the objective and envisaged nature of the business relationship.

682. Article 5 (1) WWFT obligates financial institutions to terminate an existing business relationship if the financial institution cannot comply with the provisions of Article 3 (1) and (2), opening words and (a), (b) and (c) WWFT (obligation to conduct customer due diligence, including the identification and verification of the customers, and where appropriate, the beneficial owner, as well as determining the objective and envisaged nature of the business relationship).

683. The Explanatory Memorandum suggests that in these circumstances the financial institution would file an STR if there was suspicion of money laundering or terrorist financing. However, there is no obligation in WWFT Article 5 or elsewhere in the WWFT to consider filing a suspicious transaction report on the basis of failure to satisfactorily complete CDD or of terminating the relationship.

Existing Customers—CDD Requirements (c. 5.17):

684. There are no provisions in the WWFT obligating financial institutions to apply CDD to existing customers and to conduct due diligence on such existing relationship at appropriate times. A transitional provision (Article 38 of the WWFT) states that Article 3 (1) (the provision that requires financial institutions to perform customer due diligence) does not apply to customers that have already been identified under the earlier AML law "or in respect of whom there was no identification requirement." However the previous AML law did not contain any requirement with regard to verification of identity or beneficial owner-related CDD requirements. The Explanatory Memorandum explains that the identification of the customers that took place under the previous AML law will remain valid, and seems only to refer to the "identification".

685. Authorities explained that this FATF requirement is addressed by the obligation to conduct ongoing monitoring of the business relationship and by the obligation to apply CDD in the case in which there are indications that the customer is involved in ML or TF, but this interpretation was not fully supported by the practice. The financial institutions visited by the team reflected a mix of policies, some of which extended beyond the legal requirement including, in some cases, an entire review of all client files to update the information. However, some have not applied the CDD requirements to customers taken prior to the entry into force of the WWFT. Some financial institutions indeed pointed out that reliance is placed on Article 3 (3) (e) WWFT requiring that financial institutions perform customer due diligence when the risk of an existing customer's involvement in money laundering or terrorist financing gives cause to do so. Others indicated that Article 3 (2) (d) WWFT may also be applied for the monitoring obligation during the

business relationship, however there is no guidance regarding what types of activities should result in applying CDD to existing customers. Overall it cannot be concluded that financial institutions consistently apply CDD requirements to existing customers on the basis of materiality and risk and conduct due diligence on such existing relationships at appropriate times.

Existing Anonymous-account Customers—CDD Requirements (c. 5.18):

686. There are no anonymous accounts or accounts in fictitious names. With regard to protected accounts, see analysis under criterion 5.1. The new regulation on protected accounts does not have a provision for the transitional regime, and the WWFT has one (discussed above) which provides that customers which were subject to CDD under the previous AML/CFT laws are exempted from carrying out the CDD obligations stipulated by Article 3 (1) of the WWFT.

Foreign PEPs—Requirement to Identify (c. 6.1); Foreign PEPs—Risk Management (c. 6.2; 6.2.1); Foreign PEPs—Requirement to Determine Source of Wealth and Funds (c. 6.3); Foreign PEPs—Ongoing Monitoring (c. 6.4):

687. In accordance with Article 8 (4) WWFT financial institutions must have risk-based procedures in place to identify politically exposed persons (PEP), and conduct enhanced due diligence when it enters into a business relationship with, or conducts a transaction for, a PEP not residing in the Netherlands. Once a potential client has been identified as a PEP, a financial institution that enters into a business relationship with a PEP not residing in the Netherlands shall also ensure that:

1. The decision to enter into that relationship or conduct that transaction is taken or approved by persons whom the institution has authorized to do so.

2. It takes adequate measures to establish the source of the assets used in the business relationship or transaction.

3. It applies ongoing monitoring to the business relationship.

688. The approval procedures refer to ‘individuals whom the institution has authorized to do so,’ and the Explanatory Memorandum further explains that the individual is expected to be a person designated by the executive board of the institution and that the implication is that the person establishing the relationship will hold a senior position in the financial institution. The 2006 joint guidance issued by the DNB and the Dutch Bankers Association on the Basel Committee states that in normal and increased risk categories which include PEP accounts, the decision to accept the client should take place at “a more elevated level.” This is more in keeping with the language from the WWFT which does not obligate this person to be senior management. Discussions with the private sector confirmed that in practice, senior manager approval was required to establish the business relationship.

689. There is no obligation in the WWFT addressing circumstances in which a customer or beneficial owner becomes a PEP or is found to be PEP during the course of an already established business relationship. This may be addressed through the application of the risk-based approach to monitor possible PEP status of customers envisaged by Article 8 (4). However there is no requirement to obtain senior management approval to continue the business relationship, which falls short of the FATF standard. Moreover the obligation for financial institutions to have risk based procedure to determine whether a customer is a PEP, does not extend to the case of the beneficial owner (as the WWFT’s definition of “customer” does not entail the one of “beneficial owner”).

690. Section 8(4)(b) WWFT obligates financial institutions to take measures to establish the “source of assets used in the business relationship or transaction, however the FATF standard obligates financial

institutions to establish the source of wealth and source of funds, without any reference to a specific transaction or business relationship. The authorities clarified that the Dutch term "*vermogen*" indicates also "wealth." However, Article 8 (4) (b) falls short of the FATF standard by focusing on the assets/wealth related to the relationship or transaction, rather than requiring financial institutions to take reasonable measures to establish the source of the overall wealth of the individual (in addition to the source of funds). In practice, the team found that financial institutions with a large private banking client base seemed more comfortable with the purpose and rationale for identifying the source of wealth, however for others for whom private banking was not their core business, the obligation to determine source of assets would be more strictly interpreted as referring to the funds intended to be used in the transaction/business relation.

691. There is an obligation to conduct ongoing due diligence of the business relationship and of the transactions conducted during the existence of the relationship in Article 8 (4) (c) WWFT, The Explanatory Memorandum explains that financial institutions must apply the rules of enhanced due diligence in a risk-oriented manner, but only "when entering into a business relationship with a PEP." The Explanatory Memorandum also explains that for PEPs financial institutions must 'make assessments in its internal procedures about the risks of certain product procured by the PEP.' It also states that in the event that a PEP procures a high risk product, such as private banking, the institution is obligated to subject the PEP to stricter monitoring. The majority of the private sector financial institutions the team met with confirmed that on-going PEP monitoring took place, that the shift of a client to a PEP would change their risk profile, require enhanced due diligence and require senior management approval to continue the relationship.

692. The WWFT defines a PEP by referencing to the Implementing Directive for Third EC Money Laundering Directive, and it defines a PEP "natural persons who are or have been entrusted with prominent public functions," unless the person has not held the position referred to in that paragraph for one year or more (the WWFT references to Article 2.1. of the Implementing Directive for a list of PEP categories), as well as "immediate family members, and close associates of such persons, within the meaning of Article 2 (2) and (3) of the Implementing Directive." However the obligations for financial institutions in the case of PEPs, stipulated by the WWFT and described earlier on are restricted to "PEPs not residing in the Netherlands" (Article 8 (4) of the WWFT), which falls short of the FATF standard.

693. The definition of PEP does not capture PEPs who have not been in office at least one year. The FATF plenary has concluded in the context of other EU Member State's mutual evaluation that the one-year limit as a threshold is not a material deficiency when there is a general obligation to apply enhanced due diligence to customers (including PEPs) who still present a higher risk of ML or TF regardless of any timeframe. As mentioned earlier, Article 8 (1) of the WWFT includes such an obligation, however it also suggest that additional "categories of business relationships and transactions that by nature entail greater risk of money laundering or terrorist financing may be designated by order and council." To date, none have been designated. The expectation is that the financial institutions' risk assessments will categorize the appropriate customers as high risk and conduct supplementary due diligence.

694. With regard to close associates, the Explanatory Memorandum clearly states that "this Bill does not require an institution to conduct active investigations to discover these relationship" and that "enhanced customer due diligence for this group will only be required insofar as the relationship with this person and the PEP is in public domain" or where the institution has reason to "assume" such a relationship exists. This explanation of the requirement is not consistent with FATF Recommendation 6, which does not limit the application of enhanced due diligence to close associates that are publicly known to be associates and implies a pro-active effort by financial institution to establish whether the customer is a close associate of the PEP. The definition of close associate contained in the WWFT (Article 1 (1) (e)—although it references to Article 2 (2) (3) of the Implementing Directive which refers to "person known to be close associates"—does not qualify close associates as "known in public domain."

Domestic PEPs—Requirements (Additional Element c. 6.5):

695. There is no obligation for financial institutions to identify PEPs residing in the Netherlands including non-Dutch PEPs. The Dutch approach relies on the implementation of the risk-based approach to identify circumstances with increased risk of money laundering or terrorist financing. In practice, financial institutions use commercially available software which includes all PEPs, including Dutch PEPs residing in the Netherlands or elsewhere.

Domestic PEPs—Ratification of the Merida Convention (Additional Element c. 6.6):

696. The Netherlands have signed the United Nations Convention against Corruption in 2003; ratification took place in 2006.

Cross-Border Correspondent Accounts and Similar Relationships—Introduction

697. Article 1 (1) (l) WWFT defines a correspondent bank relationship as a "regular relationship between banks in different countries for the settlement of transactions or the execution of orders." Article 8 (3) WWFT requires enhanced CDD when a bank enters or has entered into a correspondent bank relationship with a bank in a non-Member State. There are no specific provisions in place regarding correspondent relationships for financial institutions within the EU.

Requirement to Obtain Information on Respondent Institution (c. 7.1) Assessment of AML/CFT Controls in Respondent Institution (c. 7.2), Approval of Establishing Correspondent Relationships (c. 7.3), Documentation of AML/CFT Responsibilities for Each Institution (c. 7.4), Correspondent Relationship involving the maintenance of "payable-through accounts" (c.7.5):

698. Article 8 (3) WWFT specifies the procedures that banks must adopt when engaging into a correspondent bank relationship with a non-EU-based bank. It requires that banks:

1. Gather sufficient information about the bank concerned to obtain a complete picture of the nature of its business operations, and assesses the reputation of the bank and the quality of the supervision exercised over the bank on the basis of information in the public domain.

2. Assess the procedures and measures of the bank concerned to prevent money laundering and terrorist financing.

3. In the case of a new correspondent bank relationship, the decision to enter into that relationship is taken or approved by persons whom the bank has authorized to do so.

4. The responsibilities of both banks are laid down in writing.

5. The bank concerned has identified the customer and verified the customer's identity, and furthermore constantly monitors those customers who have direct access to transit accounts and is able to provide the former bank with the relevant customer data on request.

699. As with the other enhanced due diligence requirements, the term 'senior management' from the FATF standard is not applied, rather approval is required "by persons whom the bank has authorized to do so." The Q & A on the WWFT published in Open Book on Supervision on August 1, 2008 addresses this by explaining that the person authorizing the relationship should be in senior management, however, the person does not need to be a member of the board of management, but a person one level up from the one requesting the authorization, assuming that this meets the senior management requirement. In practice, the

approval for correspondent relationships varied by size of financial institutions in which smaller institutions required the approval of senior management while larger institutions did not require the same level of approval but nonetheless satisfied the requirement of the standard.

700. The Q & A on the WWFT published in Open Book on Supervision published a response to clarify payable through accounts (PTA). The response explains that Section 8(3)(e) of the WWFT means that 'a bank in the Netherlands with a correspondent relationship with a foreign bank (in a non-EU Member State) should ensure that the foreign bank has conducted equivalent customer due diligence on the clients and can provide the relevant information to the Dutch bank if that foreign bank gives its clients direct access to the account. However, this guidance is not enforceable and therefore it does not meet the FATF standard for criterion 7.5.

701. The implementation of this provision varied from financial institution to financial institution. The financial institutions the team meat with that had correspondent banking relationships and developed a risk assessment which included country risk. Smaller financial institutions were well aware of the heightened risk of correspondent relationships and either conduct enhanced due diligence, regardless of the jurisdiction and institution, or avoid the relationships entirely. However some of the larger financial institutions for which correspondent banking is a significant business, based their country risk profile on the exemptions from EU Member States and therefore did not conduct enhanced due diligence as required by the FATF standard. Those institutions that did not apply a blanket exemption did conduct independent due diligence on the respondent institution based on publicly available information including Transparency International's Corruption Perception Index and FATF Mutual Evaluations and on the supervisory authority based on Bankers Almanac or similar sources.

702. As mentioned earlier, correspondent relationships with banks in an EU State are not subject to enhanced due diligence unless there is heightened risk of money laundering or financing of terrorism. The specific measures relating to enhanced due diligence for correspondent relationships apply only in the context of non-EU respondent banks, on the basis that respondent institutions headquartered in the EU are low risk, as specified in the Third EC Money Laundering Directive. This approach does not meet the FATF standard, since correspondent banking is considered a high risk activity that requires enhanced due diligence in all cases.

Misuse of New Technology for ML/TF (c. 8.1):

703. There are no specific regulations to address the risks associated with new technologies. Instead reliance is placed on the application of Articles 8 (1) and 8 (2) of the WWFT which obligate financial institutions to perform enhanced customer due diligence if the business relationship or the transaction entails a greater risk of money laundering or terrorist financing or if the customer is not physically present for identification.

Risk of Non-Face-to-Face Business Relationships (c. 8.2 and 8.2.1):

704. There is no general obligation for financial institutions to have policies in place to address any specific risk with non-face to face business relationships or transactions but there are requirements for specific procedures in cases in which a customer is not physically present for identification. In these cases Article 8 (2) of the WWFT requires financial institutions to take the following measures to compensate for the greater risk:

1. Verifying the customer's identity on the basis of additional documents, data or information.

2. Verifying the authenticity of the documents submitted.

3. Guaranteeing that the first payment relating to the business relationship or transaction is made into or from an account of the customer with a bank that has its registered office in a Member State, or in a State designated by the Minister of Finance, and that has a license to conduct its business in that Member State or designated State.

705. The Q & A on the WWFT published in Open Book on Supervision supports the requirement to identify a customer not physically present, in particular due to on-line banking. In line with the risk-based approach, financial institutions may take additional steps beyond the obligations in Article 8 (2) to verify the identity of the customer. The Q & A provides additional examples including extra documents, bank statements, salary slips, employment contracts, or utility bills. It further provides guidance on methods to confirm the authenticity of the documents by asking the clients to have copies authenticated or submit the originals.

706. As stated above, Article 8 (2) of the WWFT obligates financial institutions to conduct one of three procedures in cases in which a customer is not physically present for identification (although a financial institution may choose to apply more than one). Situations in which financial institutions apply only the third item—*i.e.* guaranteeing that the first payment be made into or from an account of the customer with a bank that has its registered office in a Member State or a State designated by the Minister of Finance—is problematic. This provision alone is not sufficient because of the exemption from CDD provided to banks in an EU Member State or in a State designated by the Finance Ministry. Therefore reliance solely on the third provision may result in a Dutch financial institution accepting non face-to-face customers who may have not been subject to proper CDD. This minimum level of diligence was also reflected in discussions with the private sector. For non face-to-face business, financial institutions had policies in place; however, the institutions relied on the first payment being from an account in the Netherlands and, in some circumstances, other states. Additional identification measures varied and did not reflect the additional elements listed above or others listed in the FATF standard. Most problematic was the lack of understanding by some financial institutions that this type of business presented a unique risk. As a result, the verification of the beneficial owner, which in the Netherlands is risk-based and only required in high-risk scenarios, was not viewed as an obligation for this type of transaction.

Analysis of effectiveness (overall CDD measures)

707. Throughout the teams' discussions with the private sector and associations, the financial institutions demonstrated that they were comfortable explaining the risk based and principle-based approaches which underpin the Dutch AML/CFT regime, however the implementation of the principles-based approach was in some cases confusing for financial institutions, particularly in challenging areas such as identifying and verifying the beneficial owner and PEP accounts. Knowledge of the legal framework varied, although the implementation of preventive measures generally exceeded the legal requirements despite relatively high level laws and limited guidance the result of which is more of a framework than a road map to financial institutions. This seems to be a result of 1) a sophisticated financial sector in which institutions with a global presence seek guidance from other jurisdictions in which they operate or employ staff with considerable experience which included overseas postings and 2) regular contact with the DNB to discuss potential solutions to challenges.

708. In some circumstances there appeared to be a correlation between the size, age, and type of institution and the capacity of the institution to understand and meet the minimum standard as set out in the WWFT. In these cases, the lack of a legal obligation and clear guidance resulted in less than the FATF standard. For example large, multinational banks were best placed to fill in the gaps through resources, expertise and global contacts and had compliance policies in place that were often based on global best practice and therefore exceeded the Dutch standard of the WWFT and met the FATF standard. However, smaller and newly formed banks, although often closely supervised by DNB, were looking for more

assistance and specific advice and were meeting neither the standard set out by the WWFT nor the FATF standard. Insurance companies, large and small, seemed to be struggling with the overall AML obligations and also would be benefitted from more specific guidance. Money transfer offices and money exchanges receive in depth assistance from the DNB and, through these close relationships have learned to implement the obligations of the WWFT. Financial services providers such as insurance agents and brokers, although less closely supervised, in part due to the enormity of the sector, seemed to have a good understanding of their obligations.

709. During the onsite meetings, it became clear that representatives of the private sector understood the principles-based approach to allow for considerable latitude in the attainment of the desired outcome; however, given the varying degrees of implementation of the standards, the assessors determined that such a clear understanding of the end goal was not always present. The interviews with financial institutions indicated that standards were on a mix of regulations and guidance which resulted in uneven implementation.

710. During discussions with the private sector during the onsite visit it became clear that a particular area of confusion for financial institutions related to the obligation to take adequate and reasonable measures to verify the identity of the ultimate beneficial owner of a legal person. In most cases, financial institutions only verified the identity in high risk situations which was based on different risk assessments implemented by each institution. Although the standard permits a financial institution to take adequate measures, most institutions did not attempt to verify the identity of the beneficial owner as they did not understand this to be the obligation. There was also confusion about the difference between verifying the legal status of the legal person and verifying the identity of the beneficial owner of the legal person. In most cases an excerpt from the Commercial Register seemed to tick the box for both requirements, regardless of how many shareholders may be present and whether a name may be available on the shareholder list. There was also a universal focus on ownership rather than control and a number of circumstances, such as when no one person held at least 25 percent, that any one shareholder would meet the requirement.

3.2.2. Recommendations and Comments

711. The AML/CFT legal framework for CDD in the Netherlands as laid out by the WWFT and explained by the Explanatory Memorandum to the WWFT provides a very broad outline of what financial institutions should do to meet the minimum requirements. However a number of the CDD provisions either fall short of the FATF standard or leave too much discretion to the implementing institution. This is partly a result of the WWFT, which prescribes the result to be produced by the customer due diligence review, but not how this review must be carried out. Generally, financial institutions are doing more than the minimum required, although given the nature of the supervisory authorities which demonstrates a light touch, it was unclear to the assessors on what basis this standard exists. Large, international financial institutions are better positioned to fill the lack of guidance with experience, however smaller and less experienced institutions or compliance officials clearly voiced their preference for more formal guidance from the DNB.

712. In order to comply fully with Recommendations 5–8, it is recommended that that the authorities:

In respect to Recommendation 5:

- Clarify the issues related to the applicability of the CDD requirements envisaged by the WWFT (in particular those concerning beneficial ownership) to protected accounts opened prior to the entry into force of the updated Regulation on protected accounts.

- Make it clear in the Regulation on protected accounts that the compliance officer must have access to the data in the central register of protected accounts.

- Clarify that the notion of "customers" is intended to cover also trusts and other legal arrangements.

- Consider providing a list of examples of the types of documents that can be used to identify and verify the customers and beneficial owners.

- Clarify the obligation (documents should be from independent source) and provide guidance for the verification of the identity of non-Dutch based foreign legal entities (indicate examples of documents that can be used to verify identity).

- Require financial institutions to obtain information regulating the power to bind the legal person or arrangement (including the name of trustees and directors); including, in the case of foreign legal persons, the legal form and address.

- Bring the definition of beneficial owner in line with the FATF standard (by referring it to the customer and by providing a reference to "actual control' also in the case of trusts and other legal arrangements).

- Clarify the obligations to identify and to take reasonable measures to verify the ultimate beneficial owner and to understand the ownership and control structure of the customer in all circumstances regardless of risk, and provide guidance as to how this can be conducted in particular for legal persons formed outside of the Netherlands.

- Obligate financial institutions to determine whether the customer is acting on behalf of another person.

- Obligate financial institutions to verify that a person purporting to act on behalf of the legal entity so authorized.

- Provide further guidance on all CDD measures to financial institutions, including on additional circumstances which may be considered high risk as well as examples of the type of enhanced due diligence measures that could be implemented.

- Address the exemptions for low-risk customers as adopted from the Third EC Money Laundering Directive to ensure that all transactions are based on a risk assessment regardless of the location, type of client or product and that regardless of the classification that all transactions are subject to monitoring and periodic review.

- Oblige financial institutions to ensure that data and information obtained under the CDD process, such as the client risk profile and contact information, are kept up-to-date.

- Introduce an express obligation to consider fling an STR in the case of failure to satisfactorily complete CDD/terminating business relation.

- Repeal the transitional provision of the WWFT that deems the identification and record keeping requirements under the previous AML/CFT law as if it were duly fulfilled under the WWFT.

In respect to Recommendation 6:

- Require institutions to ascertain source of wealth and funds in all circumstances and not limited to business relations/transactions.
- Review the PEP-related requirements to include non-Dutch PEPs resident in the Netherlands.
- Introduce a requirement to obtain senior management approval to continue business relationship when a customer/beneficial owner becomes a PEP or is found to be a PEP during the course of an already established business relationship.
- Extend the obligation for financial institutions to have risk based procedure to determine whether a customer is a PEP, also to the case of the beneficial owner.
- Clarify that the notion of close associate is not limited to close associates who are publicly known.

In respect to Recommendation 7:

- Extend enhanced due diligence to all correspondent relationships regardless of the location of the respondent.
- Introduce enforceable requirements in the case of payable-through accounts.

In respect to Recommendation 8:

- Extend enhanced due diligence required to all non face-to-face relationships.
- Reconsider the option envisaged by Article 8, para 2 c) of the WWFT, as it may not ensure effective CDD procedures in the case of non face-to-face transactions.
- Create specific obligation to prevent the misuse of new technologies.

3.2.3. Compliance with Recommendations 5, 6, 7, & 8

	Rating	Summary of factors underlying rating
R.5	**PC**	• There is no direct obligation in the WWFT or related legislation requiring financial institutions to determine whether the customer is acting on behalf of another person. • For foreign legal persons "not based in the Netherlands", there is no indication that documents used to verify the identity of a legal entity should be from an "independent" source. • The WWFT does not obligate financial institutions to verify that a person purporting to act on behalf of the legal entity is so authorized. • There is no requirement to obtain a "foreign legal person's" address and legal form or to obtain the name of trustees or directors or to obtain provisions regulating the power to bind the legal person or arrangements. • The definition of the beneficial owner falls short the FATF standard as it only refers to legal persons and trusts, and not, more broadly, to the natural person(s) who ultimately own or controls "a customer". The definition does not refer to the person that can exercise ultimate effective control over a legal arrangement. • The requirement to verify the identity of the beneficial owner and to understand the ownership and control structure of the customer are subject to a risk based

	Rating	Summary of factors underlying rating
		approach and are only applicable in high risk scenarios. • Rather than identifying circumstances in which simplified CDD can be conducted, Article 6 WWFT provides a list of customers/scenarios exempt from the CDD requirements stipulated by Article 3(1) (the obligation to undertake customer due diligence, which, as the authorities confirmed, includes the measures detailed in paragraph 2), Article 3 (3) (a)(b)(d) and (4) and Article 4 (1). • There are no obligations for financial institutions to ensure that data and information obtained under the CDD process, such as the client risk profile and contact information, are kept up-to-date. • No enforceable obligation to consider filing a suspicious transaction report in the case of failure to satisfactorily complete CDD/terminate business relationship. • There are no provisions in the WWFT obligating financial institutions to apply CDD to existing customers. Transitional provision exists that consider by default the customers identified under the previous AML/CFT regime as identified under the WWFT. • Effectiveness issues in the implementation of preventive measures, regarding: the identification and verification of the beneficial owner
R.6	**PC**	• There is no requirement for institutions to ascertain source of wealth and to identify the beneficial owner when the source of wealth is a PEP. • The PEP-related requirements do not apply to non-Dutch PEPs resident in the Netherlands. • The obligation for financial institutions to have risk based procedure to determine whether a customer is a PEP, does not extend to the case of the beneficial owner. • There is no requirement to obtain senior management approval to continue business relationship when a customer/beneficial owner becomes a PEP or is found to be a PEP during the course of an already established business relationship. • The notion of close associate in the Explanatory Memorandum is limited to those who are "publicly known".
R.7	**LC**	• Enhanced due diligence does not apply to correspondent relationships involving financial institutions headquartered in an EU Member State. • No enforceable requirements in the case of "payable-through accounts".
R.8	**LC**	• The option envisaged by Article 8, para 2 c) of the WWFT may not ensure effective CDD procedures in the case of non face-to-face transactions. • No specific obligation to prevent the misuse of new technology.

3.3. Third Parties and Introduced Business (R.9)

3.3.1. Description and Analysis

Legal Framework:

713. In the Netherlands financial institutions are permitted to rely on third parties to perform some of the elements of the CDD process. Article 9 (1) WWFT in conjunction with Article 5 (1) WWFT and Article 3 of the WWFT permit the following institutions to conduct CDD in an equivalent manner:

- Those institutions as referred by in Article 1 (1) (a) 11°-13° (*i.e.* independent legal professionals such as a chartered accountant, external accounting consultant or tax advisor, lawyer or notary having a registered office in the Netherlands or in another EU Member State).

- Those institutions as referred to by Article 1 (1) (a) (1°)-(3°) or (5°)-(10°), (*i.e.* financial and credit institutions, life insurers, investments firms, collective investments schemes, financial

services providers, or trust offices, including from non-EU Member countries, but no money transfer offices).

714. Unlike in the case of impendent legal professionals, there is no indication that the financial institutions that can be relied upon be based in the Netherlands or in the EU. This constitutes a problem because there are no specific provisions that Dutch-based financial institutions must apply when accepting third party performed-CDD, and no additional guidance is provided.

Requirement to Immediately Obtain Certain CDD elements from Third Parties (c. 9.1) & Availability of Identification Data from Third Parties (c. 9.2):

715. There is no specific obligation for financial institutions relying on third parties to immediately obtain the necessary information from the institution that is being relied upon. Rather than obliging institutions which are relying on a third party to immediately obtain the necessary information concerning the CDD process from that party (as required by the FATF standard), Article 9 (2) WWFT places the obligation on the institutions that are being relied upon to carry out certain elements of the CDD process to provide, at the request of the "relying" financial institution, with the identification and verification data and other data and documents regarding the identity of the customer or the beneficial owner. This provision—which transposes Article 18.1 of the Third EU Directive—is not consistent to the FATF standard and appears also difficult to enforce (especially in the case of foreign institutions being relied upon). There is also no explicit requirement or relevant guidance for Dutch financial institutions to satisfy themselves that copies of data and documentation relating to CDD will be made available from the third party without delay. The authorities have indicated that, by imposing the obligation onto the third party, there is an implicit obligation on the Dutch institution to satisfy itself that the third party will be able and willing to fulfil its responsibilities and that, ultimately, it is the responsibility of the Dutch relying institution to have the CDD data in its files to comply with the record keeping requirements (and that failure to do so would result in a fine being applied by the competent supervisors).

Regulation and Supervision of Third Party (applying R. 23, 24, and 29, c. 9.3)-Adequacy of Application of FATF Recommendations (c. 9.4):

716. While the eligible third party introducers are clearly defined, there is no obligation for financial institutions relying on third parties to carry out some of the CDD process to be satisfied that the third party is regulated and supervised and has measures in place to comply with requirements set out in Recommendations 5 and 10.

Adequacy of Application of FATF Recommendations (c. 9.4):

717. Article 9 (1) (b) WWFT does not stipulate specific countries in which the third party introducer can be based (see discussion above regarding the difference between independent legal professionals, which in order to be relied upon, should be either in the Netherlands or in another EU Member State, and financial institutions, for which no restriction is placed based on residence) nor has guidance been published.

Ultimate Responsibility for CDD (c. 9.5):

718. The Explanatory Memorandum to the WWFT refers to the Directive 2005/60/EC which states the ultimate responsibility for customer due diligence lies with the institution where the client is introduced, however the enforceability of the guidance is unsubstantiated.

Analysis of effectiveness

719. In practice, the banks and insurance companies the team met, accepted CDD from third party introducers based almost exclusively in the Netherlands and which are therefore subject to Dutch supervision.

3.3.2. Recommendations and Comments

720. The authorities are recommended to:

- Revise the obligation that is currently imposed on the third party to provide the information concerning the CDD process, so that this information is immediately obtained by the FI that is relying on the third party should be redrafted to impose the obligation on the financial institution.

- Introduce a requirement for financial institutions to satisfy themselves that a third party located within the EU and EEA is regulated and supervised (in accordance with Recommendations 23, 24 and 29), and has measures in place to comply with the CDD requirements set out in R.5 and 10. Alternatively, the authorities could consider conducting a thorough assessment of the supervisory framework and of the CDD measures in place in the concerned countries where the third parties are located and limit the location of third parties to those countries that have satisfactory supervisory framework and CDD measures.

- Introduce enforceable requirements that place the ultimate responsibility for customer identification and verification with the financial institution relying on the third party.

3.3.3. Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	**NC**	• No direct obligation for financial institutions to: o immediately receive necessary customer information and; o satisfy themselves that copies of CDD documents and data will be available without delay. • No obligation for financial institutions to satisfy themselves that the third party is regulated or supervised. Presumption that all EU and EEA countries adequately apply the FATF Recommendations. • No enforceable requirement that ultimate responsibility for CDD should remain within the FI relying on the third party.

3.4 Financial Institution Secrecy or Confidentiality (R.4)

3.4.1. Description and Analysis

Legal Framework:

721. The duty of financial entities to protect the confidentiality of the information provided to them by their customers is normally dealt with in the contract between the entities and their customer. In addition, Article 8 of the Data Protection Act restricts the distribution of personal data, but allows for exemptions such as when disclosure is necessary to meet a legal obligation.

722. Powers to obtain information from regulated financial entities, notwithstanding any confidentiality duty, are provided by Articles 5.11 to 5.20 of the General Administration Act (Awb) which are applied to the supervisory authorities by provisions in the WWFT (Article 24), Articles 1:73, 1:74, of

the Law on Financial Supervision–Wft–(which applies to most regulated financial entities) and Article 8 (5) of the law on Money Transaction Offices–Wgt–(which applies to bureaux de change). The powers relating to money transfer offices were originally given in the Wgt but an amendment to the Wft in November 2009, prompted by the Payment Services Directive, resulted in the licensing and other powers for money transfer offices being included within the Wft. Powers relating to bureaux de change, however, remain in the Wgt.

Inhibition of Implementation of FATF Recommendations (c.4.1):

723. Overall, the provisions governing confidentiality of records, when taken with the powers for the authorities to obtain and share information do not inhibit the implementation of FATF Recommendations.

724. Articles 5.11 to 5.20 of the Awb give powers to statutory authorities to compel a person to give information. The powers are available to those statutory bodies charged with monitoring compliance with statutory obligations. These are statutory powers that override contractual duties. They also create a legal obligation and thus allow disclosure, by regulated financial entities, under Article 8 of the Data Protection Act. However, the powers in the Awb are only available when specifically applied by the legislation creating the statutory duty to monitor compliance. This is done in the WWFT, Wft, and other laws as detailed below.

725. Article 24 of the WWFT gives the Ministers of Finance and Justice the power to designate the authorities responsible for monitoring compliance with the Act by those institutions subject to the Act. The WWFT applies to all "institutions" defined in Section 1:1 of the WWFT. That definition encompasses all the activities in the FATF Glossary definition of "financial institution". The power to designate supervisory authorities was exercised in a joint order, on 18 July 2008, designating *De Nederlandsche Bank* (the Central Bank or DNB) and *Autoriteit Financiële Markten* (the Authority for the Financial Markets or AFM) as being responsible for monitoring regulated financial entities' compliance with their obligations under the WWFT. In addition, Article 24 of the WWFT directly makes the DNB responsible for monitoring compliance with EU Regulation 2006/1781 on wire transfers. Article 1:24 of the Wft gives the DNB supervisory powers over prudential matters relating to financial entities regulated under the Wft. Article 1:25 gives supervisory powers over conduct of business of such entities to the AFM. The power to supervise bureau de change is given in the delegation decree of the Wgt.

726. The information gathering powers in the Awb are given to the supervisory authorities as follows:

- Article 24 of the WWFT gives the DNB and AFM all of the powers in Articles 5.11 to 5.20 of the Awb.
- Articles 1:73 and 1:74 of the Wft gives the supervisor the information gathering powers in Articles 5.13 to 5:17 and Article 5:20 of the Awb.
- Article 8(5) of the Wgt gives the supervisors the information gathering powers in Articles 5:12, 5:13, 5:15, 5:16, 5:17 and 5:20 of the Awb.

727. Although the application of the provisions of the Awb is slightly different in the WWFT, the Wft, and Wgt, the key provisions are applied under both statutes:

- Article 5:16 of the Awb gives the supervisors the power to demand information.
- Article 5:17 gives the power to inspect, take copies of or remove business information and document.

- Article 5:15 gives the supervisor the power to gain entry to the premises of the supervised institution (by force if necessary).

- Article 5:20 creates an obligation on the supervised institution to provide all necessary assistance.

728. The provisions that are included in the WWFT but excluded from the Wft or Wgt are not of operational significance for the purpose of providing adequate information gathering powers to supervisors. Articles 5:11 and 5:12 of the Awb (which are not given to the supervisory authorities by the Wft) define an inspector and oblige such an inspector to carry appropriate authority and identity documentation. Articles 5:18 and 5:19 of the Awb (which are not given to supervisory bodies in either the Wft or Wgt) contain powers not directly relevant to regulated financial entities, such as the power to obtain samples of goods).

729. The requirement on supervisory authorities to protect the confidentiality of information obtained by them is set out in Article 22 of the WWFT, Article 1:89 of the Wft, Article 12 of the Wgt and Article 2:5 of the Awb. In each case, the duty to protect the confidentiality of information is subject to exemptions:

- Article 22 of the WWFT permits disclosure of data and information where this is required for the performance of duties under the WWFT or is required by the WWFT.

- Article 13 (g) of the WWFT gives the FIU the right to pass information to the supervisory authorities on the reporting behavior of entities subject to the Act.

- Article 25 of the WWFT and Article 13 of the Wgt require the supervising institutions to pass to the FIU any information suggesting suspicion of money laundering and terrorist financing.

- Article 17 of the WWFT empowers the FIU to request additional data from entities subject to the Act and DNFBPs that have submitted an unusual transaction report or that are involved in a transaction on which the FIU has gathered data.

- Article 1:51 Wft permits the disclosure of confidential information to supervisory authorities of Member States and Article 1:65 provides for disclosure to non Member States subject to conditions including the protection of the information and the use to which it will be put.

- Article 1:90 of the Wft permits disclosure of information from DNB to AFM (and vice versa) and to a supervisory authority of another Member State except where certain tests apply, such as that disclosure would not be compatible with Dutch law or the confidentiality or appropriate use of the information could not be assured.

- Article 1:92 of the Wft permits disclosure of confidential information to prosecutors.

- Other provisions in the Wft permit disclosure of confidential data to other persons of less direct relevance to the monitoring of AML/CFT obligations by regulated financial entities, subject to similar conditions.

- Article 14 of the Wgt allows disclosures to domestic and foreign government and supervisory authorities subject to certain conditions concerning the use to which information will be put.

- Article 2.5 of the Awb allows disclosure where required by law or arising from the nature of the duties of the inspector.

730. The DNB and AFM may use the information gathering and information exchange powers under either WWFT or Wft. Both supervisory authorities are given the powers under the Awb in both WWFT and Wft (and in the case of the DNB, given comparable powers over the bureau de change in the Wgt). They can therefore use whichever of the information gathering powers that are appropriate in any given circumstance.

731. The powers in the WWFT to exchange information (other than with the FIU) are implicit in that they must be assumed from the provision that disclosure is prohibited unless required for the performance of duties under the WWFT or directly required by the WWFT. There could be challenges about disclosures of confidential information to other supervisory authorities if based on such general provisions. However, there are more specific provisions in the Wft, on which the DNB and AFM may rely and in the Wgt, on which the DNB may rely. The ability to exchange confidential information and data with supervisory authorities in non Member States in Article 1:65 of the Wft is not constrained to information obtained under the Wft and therefore could also apply to information obtained using other powers, including the WWFT.

732. The ability to collaborate with supervisory authorities of Member States only applies where necessary for the performance of duties under the Wft. However, as discussed more fully below, the authorities state that the provisions of the Wft in Article 3:10 and 4: 15 with regard to integrity impose an obligation on regulated financial entities to take measures to prevent transgressions of the law and relations with clients that would undermine confidence. The authorities' position is that this effectively requires regulated financial entities to have procedures and measures to ensure compliance with WWFT. It is accepted in this assessment that the supervisory authorities have the right to supervise compliance with this obligation. Monitoring compliance with WWFT is, on this interpretation of the Wft, one of the duties of the supervisory authorities under the Wft and therefore the information exchange provisions in Article 1:51 (as elsewhere) may be used by the DNB and AFM in respect of compliance with WWFT. In the case of bureaux de change, Article 5 of the Wgt Regulations imposes a direct duty to have procedures and measures to implement the statutes that preceded the WWFT (and is therefore also presumed to require procedures and measures to ensure the implementation of the WWFT). The supervisory powers in the Wgt over bureaux de change including those relating to information exchange can therefore be used in respect of information concerning compliance with the provisions of the WWFT.

733. Article 1:79 of Wft permits the DNB and AFM to impose sanctions for violation of Article 5.20 of the Awb (that which obliges a person to co-operate with the supervisory authorities in the exercise of their information gathering powers). Article 1:79 of the Wft and Article 20 of the Wgt apply the sanctions provisions of the Awb. These can therefore be used to enforce the information gathering provisions described above.

Exchange of information between authorities:

734. As a result of the legal framework described above, the DNB and AFM are able to obtain any information from regulated financial entities that is necessary to monitor compliance with the WWFT regardless of the entities' duty of confidentiality to their clients or the Data Protection Act. The DNB and AFM may receive information from the FIU and must make disclosures of money laundering or terrorist financing suspicions to the FIU. The DNB and AFM are also able to share confidential information with each other and with foreign supervisory authorities (so as, for example, to share information on the performance of institutions in complying with their obligations).

735. The DNB and AFM state that they have no difficulty in obtaining information from regulated financial entities in practice and that they conduct a risk-based supervision program which results in their obtaining the required information. Regulated financial entities were also clear that they were required to

provide the supervisory authorities with information they wanted and confirmed that the authorities regularly demanded such information. This would include internal procedures and policies as well as customer data taken as samples to check the implementation of AML/CFT policies.

736. The supervisory authorities have made a small number of disclosures of unusual transactions to the FIU but, as would be expected, this is relatively rare as the primary obligation for such disclosures would fall upon the institutions themselves. The FIU provides information to the supervisors on the reporting behavior of institutions and, in some cases, on the treatment of certain unusual transaction reports.

737. The DNB and AFM have stated that they regularly share information with each other on compliance by regulated financial entities. There is no inhibition in practice. They have also stated that they are rarely asked for information by foreign supervisory authorities on compliance by such entities but that they regularly exchange confidential information on other matters with supervisory authorities in other Member States and elsewhere.

738. The FIU is also able to obtain information that is covered by financial or professional secret, from the subjects to the obligation to report unusual transactions. The FIU states, that, in practice, it has no difficulty in getting this information.

Exchange of information between regulated financial entities where required by R.7, R.9 and SR VII:

739. Article 8 of the WWFT states that a bank that allows direct access to its accounts by customers of a correspondent bank must provide the other bank with relevant customer data on request. Article 9 of the WWTF requires an institution subject to the Act to provide details on customer due diligence to another institution, when the latter institution has relied upon customer due diligence undertaken by the first person.

740. The Bankers Association has agreed a Code of Conduct that allows dissemination of customer information between banks, where there is some evidence of fraud or other wrongdoing, even where there is no conviction. The Code of Conduct is based on the provisions of the WWFT (which requires some exchange of customer information as noted above). The Bankers Association informed the mission that the exchange of information resulted in a list of customers about which banks should make further enquiries prior to opening accounts. The system is confined to banks. Other financial services providers noted that they did not have access to any such system. Thus, if a bank refused to do business with a customer introduced by a financial services provider such as a mortgage broker, the broker would not know the reason. Moreover, the broker might also be subject to some suspicion by the bank for introducing such a customer. The arrangement between the banks is a sensible initiative. There may be scope for extending the system to other financial services providers but such an extension would clearly have to be undertaken with great care.

741. The provisions of EU Regulation 1781/2006 on wire transfers apply directly in The Netherlands and all entities that can make payments by wire transfer are directly bound by it. The Regulation is described in more detail below. For the purpose of exchange of information between authorities relating to the Regulation, Articles 5 (1) and 7 (1) of the Regulation require the provision of complete payer information (name, address and account number) with wire transfers. When there is a domestic transfer or intra EU transfer where complete payer information might not be supplied, Article 6 of the Regulation requires that an institutions should make complete payer information available to the payment services provider of the payee on request within three days.

742. Each of the obligations to provide customer data is a legal obligation that, according to Article 8 of the Data Protection Act, overrides the confidentiality requirements in that Act. The statutory requirements would also override contractual confidentiality obligations. The requirements of the Recommendation 4 are therefore met.

Analysis of effectiveness

743. There is no inhibition on FATF Recommendation 4. The supervisory authorities have power to collect information and the power to share it domestically and internationally. The supervisory authorities can apply the penalty provisions in Articles 1:75, 1:79 and 1:104 of the Wft. These are discussed more fully in the context of Recommendation 29. The statutory provisions described above require regulated financial entities to exchange information between themselves where this is necessary for Recommendations 7, 9 and SRVII.

744. The authorities state that these provisions work effectively and that, in practice they share information with other authorities on the compliance by regulated financial entities with their AML/CFT obligations. Individual financial entities also share information between themselves where this is required by the WWTF and EU regulation 1781/2006

3.4.2. Recommendations and Comments

745. The provisions of the WWFT give only implicit power to the supervisory authorities to share information (except for making ML or TF disclosures to the FIU). Powers to share information under the Wft are much more explicit and clearly defined. They can be applied in respect of information obtained under the WWFT. In the case of collaboration between the Dutch supervisory authorities and their counterparts in Member States, Article 1:51 provides for this where necessary for the purposes of the Wft and this is assumed to encompass the obligations imposed by the WWFT for reasons discussed more fully below in the discussion of internal controls. Although this interpretation is accepted for the purposes of this assessment, it is possible that there could be a challenge to the right of supervisors to use the powers in the Wft to exchange confidential AML/CFT related information collected under compulsion under the WWFT.

746. The authorities are **recommended** to:

- Amend the WWFT (Article 22) to make explicit that supervisory authorities may share information collected for the purpose of Article 24 with other domestic authorities and foreign supervisors, where this is necessary for the administration and enforcement of obligations under the WWFT and to include appropriate provisions regarding the use and confidentiality of such information, as are currently provided for in the Wft.

- Consider with the Bankers Association the extent to which other regulated financial entities could have access to the customer information shared between banks according to the Code of Conduct.

3.4.3. Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	**C**	• This Recommendation is fully observed.

3.5 Record keeping and wire transfer rules (R.10 & SR.VII)

3.5.1. Description and Analysis

Legal Framework:

747. Article 52 (4) of the tax law (AWR) obliges any person who is obliged to keep records to keep those concerning financial and other matters for at least seven years. In addition, Article 10 of Title 2 of the Civil Code (*Burgerlijk Wetboek* or BW) imposes a general record-keeping requirement that includes a provision insisting on maintenance and retention of all business records by legal persons for seven years.

748. There are record-keeping and retention rules in Articles 33 and 34 of the WWFT (which apply to all regulated financial entities that are defined in the FATF glossary). There are further record-keeping and retention provisions in the implementing regulations for Wft which have the force of law. The prudential rules decree (BPR Wft) has record keeping and retention requirements in Articles 14 and 19. There are record-keeping provisions in Articles 6, 7, and 10 of the Wgt Regulation. The decree on conduct of financial enterprises (BGFO Wft) includes record-keeping and retention provisions in Articles 21 and 26. The record-keeping provisions on wire transfers are implemented directly by EC Regulation 1781/2006.

749. In the assessment of Recommendations 10 and 15, it is noted that the provisions in the Wft apply differently to different categories of regulated financial entity. The term “financial institution” is used in the Wft to denote a person, who is not a credit institution, but who provides certain financial services. The term “financial services provider” is used to denote a person who supplies a financial product other than a financial instrument (and often means, in practice, an insurance or mortgage broker). The natural meaning of terms such as “financial institution” or “financial services provider” are much broader than the narrow definition in the Wft. The term “financial institution” would normally mean any entity providing financial services. To avoid confusion, the assessment of Recommendations 10 and 15 use the terms financial institution and financial services provider as defined in the Wft. For references to a broader range of entity, the terms “regulated financial entity” or simply “financial entity” are used.

Record Keeping and Reconstruction of Transaction Records (c. 10.1 and 10.1.1):

750. Record-keeping and retention provisions cover most records and most institutions. However, the provisions do not necessarily cover all the institutions and all the records required by the FATF Recommendations.

751. Article 10 (1) of Title 1 of Book 2 of the Civil Code (BW) states that “The board of management is obliged to keep administrative records of the legal entity's financial position and everything relating to the work of the legal entity according to the requirements arising from that work and to keep the accompanying books, documents and other data carriers in such a way that the rights and obligations of the legal entity can be established at all times”. Article 10 (3) includes a requirement to maintain records for seven years. Article 52 of the AWR states that:

> *Persons obliged to keep records are obliged to keep records of their financial position and of everything concerning their company, independent profession or work, in accordance with the requirements of that company, that independent profession or that work,*

and that

Unless otherwise provided under or pursuant to the tax law, persons obliged to keep records are obliged to keep the data carriers referred to in the preceding paragraphs for seven years.

752. These provisions are written in broad terms and would encompass, amongst others, records on transactions. The BW provisions apply only to legal entities and not to natural persons. The AWR provisions apply to all legal and natural persons residing in the Netherlands with a fiscal obligation. Clearly, most regulated financial entities will, in practice be legal persons, (although there is no overriding requirement in the Wft, Wgt or the WWFT that regulated financial entities must be legal entities) and the authorities state that all will have a fiscal obligation. However, there is no direct requirement to keep such records that would permit a reconstruction of an individual transaction sufficient to be evidence for a prosecution (as stated in criterion 10.1.1). This is a high test that may not necessarily be met by the general record keeping and retention provisions in the Civil Code or the tax law.

753. Article 14 (5) of the BPR Wft imposes on credit insurers, life insurers, payment institutions[87] or branches a record keeping requirement in relation to the monitoring of client transactions and requires the regulated financial entity concerned to maintain that data for a minimum of five years after the services have been provided. The Article makes no distinction between domestic and international transaction and may be presumed to apply to both. Article 19 of the BPR Wft requires credit institutions, clearing institutions, payment service providers, insurers or branches to keep records on all rights and obligations. Article 21 (5) of the BGFO Wft requires a collective investment scheme to keep records on the monitoring of transactions and to keep them for five years. Article 26 (4) has comparable provisions for record keeping of the monitoring of transactions for investment firms.

754. The Wft defines various categories of regulated financial entity. One such category is a "financial institution" which is an entity, not a credit institution, which provides certain financial services. The provisions in the BPR Wft and BGFO Wft, quoted above, do not apply to financial institutions (as defined in the Wft), or to financial services providers. They do not apply to management companies, investment companies or depositories. The provisions refer only to records on the monitoring of transactions and not necessarily to the transactions themselves. The provisions do not require the reconstruction of individual transactions so as to be able to provide evidence for prosecution of criminal activity. As noted above, this is a high test and it would be unsafe to assume that it would be met by the record-keeping and retention requirement in the Wft.

755. Article 6 of the Wgt Regulation requires a bureau de change to record incidents. Article 10 states that individual transactions must be recorded in a timely manner. There are no record retention requirements in the Wgt, although bureau de change would be subject to the general provisions of the AWR and BW.

756. Article 34 of the WWFT requires a regulated financial entity to maintain records relating to a transaction that has been the subject of an Article 16 disclosure and requires that these records should include customer identity (including identity documentation), the beneficiary, the nature, time and place of the transaction, and the extent, origin and destination of the funds (or other property). This provision does not extend to transactions about which there has been no disclosure. Article 34 requires that the data be retained for five years from the time of disclosure.

87 This refers to the application of the BPR Wft to payment institutions on the assumption that the BPR Wft has been amended in line with amendments to the primary law–the Wft. No translation has been given of an amendment to Article 14(5) BPR Wft.

757. The general provisions in the BW and AWR will normally impose the seven-year record-retention requirement. However, it is strange to have a general seven-year retention requirement coexisting with specific retention requirements of periods less than this. The provisions in the Civil Code and tax law do not specifically require records that are sufficient to reconstruct individual transactions and to provide evidence for a prosecution, although the authorities state that this is implicit in the law and is achieved in practice. It is probable that the general provisions in the AWR and BW are sufficient to impose a record retention requirement of seven years on all regulated entities, however, such an entity may conclude either that the general requirements in the Civil Code or tax code should be narrowly interpreted or that the specific requirements in the WWFT, Wft, or Wgt could have no meaning unless they overrode the general requirements. If the general provisions in the AWR and BW were not sufficient, the specific statutory provisions in the WWFT, Wft, and Wgt, would not cover all the requirements in Recommendation 10. In particular:

- The provisions in the BPR Wft and BGFO require that data relating to the monitoring of transactions be retained but do not require transactions data itself to be maintained and there is no requirement that the records should permit reconstruction of transactions sufficient for prosecution evidence.

- The provisions in the BPR Wft and BGFO Wft do not apply to the Wft categories known as financial institutions, to financial services providers, or to management companies, investment companies or depositories.

- There are no record retention provisions in the Wgt and the requirement to maintain transactions records is not explicit that the records must be kept in a form that would allow reconstruction for the purposes of prosecution.

- There is no provision giving the competent authorities the power to extend the record keeping requirement in particular circumstances except in respect of information relating to wire transfers.

Record Keeping for Identification Data, Files and Correspondence (c. 10.2):

758. Article 10 of Title 1 of Book 2 of the Civil Code, quoted above is in very general terms and without specific guidance issued by the authorities, its precise meaning in the context of records of relevance to AML/CFT obligations is unclear. It would appear to encompass identification data, account files and business correspondence for legal entities. Similarly, the provisions in the tax code (AWR), also quoted above, are very general and cover everything concerning the company, profession or work of the entity concerned. This coverage meets the terms of the criterion. The requirement for retention of records for seven years does not say from when that period should start but the authorities state that the AWR requires the records to be kept for as long as they are necessary and that, in practice, the seven year period would start from a period no earlier than the time at which the business with a customer ceased.

759. Article 33 of the WWFT requires an entity subject to the law to maintain records of customer identity, including the full names, addresses and birth date of natural persons, the incorporation documents of legal persons (where incorporated under Dutch law), the verification information, and the nature of services provided. Other documentation is required for foreign companies. There is no requirement for the retention of data on the identification of beneficial owners (except where one natural person is acting on behalf of another), or of legal arrangements such as trusts. The Article is very specific and, since it does not require the retention of business correspondence and other account files, the natural reading of the Article is that no such requirement is created. The authorities state that these deficiencies will all be corrected when a proposed amendment, currently before Parliament, is enacted.

760. Article 33 of the WWFT states that the specified data on customers should be kept for five years after the business relationship is terminated or for five years after the transaction was carried out (presumably where the customer identification data was obtained for an occasional transaction).

761. Article 14 (5) of the BPR Wft applies to credit institutions, life insurers, payment institutions or branches. It requires data on the identification of customers and the monitoring of transactions to be maintained for a minimum of five years. Article 21 (5) of the BGFO Wft applies to collective investment schemes. It requires maintenance of data on client identification for five years. Article 26 (4) applies to investment firms and imposes a similar requirement. Article 35 (1) requires investment firms to record all data of all investment services, ancillary services and investment activities for the purpose of implementing the EU Directives on Markets in Financial Instruments (MiFID). Article 33 of the BGFO Wft applies to credit providers. It imposes the five year record retention rule to financial information used to assess credit applications. These provisions do not apply to the Wft category of financial institutions, to financial services providers, to management companies, to investment companies or to depositories.

762. There are no requirements in the Wgt for a bureau de change to keep customer identification records, except to the extent that they would be maintained as part of the transactions records required by Article 10 of the Wgt.

Availability of Records to Competent Authorities in a Timely Manner (c. 10.3):

763. Article 33 (1) of the WWFT states that information must be held in an accessible manner. Since authorities have the power to obtain this information under the provisions of the Awb already described, these provisions will ensure that the information should be accessible to the authorities.

764. There is no requirement in the Wft or the Wgt that records should be held in such a way as to be accessible to the authorities in a timely manner. The authorities consider that this is implicit in the general provisions to have procedures, policies, and controls to mitigate integrity risk but have not issued any guidance making this position clear. The WWFT (Article 33 (1 and 2)) requires records to be kept in an accessible manner and (Article 17 (2)) allows the authorities to set deadlines for the production of records and this will enable them to ensure that records are available in a timely manner. Article 14 of the EU Regulation requires payment services providers to respond fully and without delay to enquiries about information in the context of wire transfers.

Obtain Originator Information for Wire Transfers (applying c. 5.2 and 5.3 in R.5, c.VII.1):

765. The Netherlands are directly bound by the EU Regulation on wire transfers, EC 1781/2006. The Regulation applies directly to its addressees, without further implementation being required by Member States through their national legislatures. Article 24 of the WWFT makes the DNB responsible for monitoring compliance with EU Regulation 2006/1781 on wire transfers.

766. According to Article 3, the Regulation applies to transfers of funds, in any currency, which are sent or received by a payment services provider (PSP) established in the EU. This would mean that, in The Netherlands, it would apply to credit institutions, money transfer offices and any regulated financial entity able to make payments by wire transfer.

767. Under the terms of the Regulation, it does not apply in the following cases:

768. Transfers of funds carried out using a credit or debit card, provided that:

(a) the payee has an agreement with the PSP permitting payment for the provision of goods and services; and

(b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies such a wire transfer (Article 3 (2) of the Regulation).

769. Transfers of funds using electronic money covered by that derogation, except where the amount transferred exceeds EUR1 000 ($1 392) (Article 3 (3) of the Regulation).

770. Transfers of funds carried out by means of a mobile telephone or any other digital or Information Technology (IT) device, when such transfers are pre-paid and do not exceed EUR150 ($209) (Article 3 (4) of the Regulation)

Transfers of funds carried out by means of a mobile telephone or any other digital or IT device, when such transfers are post-paid and meet all of the following conditions:

(a) the payee has an agreement with the PSP permitting payment for the provision of goods and services;

(b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the wire transfer; and

(c) the PSP is subject to the obligations set out in the Third EU Money Laundering Directive (Article 3 (6) of the Regulation).

Transfers of funds:

(a) where the payer withdraws cash from his or her own account;

(b) where there is a debit transfer authorization between two parties permitting payments between them through accounts, provided that a unique identifier accompanies the wire transfer, enabling the natural or legal person to be traced back;

(c) where truncated checks are used;

(d) to public authorities for taxes, fines or other levies within a Member State; and

(e) where both the payer and the payee are PSPs acting on their own behalf.

771. According to Article 5 of the Regulation, the payer's PSP has to ensure that transfers of funds are accompanied by complete information on the payer. Article 4 defines 'complete information' as consisting, in principle, of the name, address, and account number. The address may be substituted with the date and place of birth of the payer, a customer identification number, or national identity number. Where the payer does not have an account number, the PSP has to substitute it with a unique identifier which allows the transaction to be traced back to the payer.

772. Under Article 5 (2), the PSP, before transferring the funds, has to verify the complete information on the payer on the basis of documents, data or information obtained from a reliable and independent source. This provision does not apply where the value of the transfer is less than EUR1 000, unless the transaction is carried out in several smaller transactions that appear to be linked. The requirement for verification is set out in Article 11 of the WWFT and the documents to be used are shown in Article 4 of the implementing regulation URWWFT.

773. Article 5 (3) of Regulation 1781/2006 states that, in the case of transfers of funds from an account, verification may be deemed to have taken place, if:

- A payer's identity has been verified in connection with the opening of the account and the information obtained by this verification has been stored in accordance with the obligations set out in Articles 8 (2) and 30 (a) of the Third EC Money Laundering Directive.

- The payer falls within the scope of Article 9 (6) of the Third EC Money Laundering Directive (*i.e.* he or she is a customer who existed prior to the implementation of the Directive's provisions, but has been subject to verification on a risk-based approach).

Inclusion of Originator Information in Cross-Border Wire Transfers (c. VII.2):

774. According to Article 7 (1) of the Regulation, transfers of funds where the payer's payment service provider (PSP) is situated outside the European Union must be accompanied by complete information on the payer (as defined in Article 4). Transfers from one European Union Member State to another Member State are not considered to be cross-border for the purposes of the Regulation, and, therefore, this provision does not apply in such circumstances. For the purposes of SRVII, the FATF has recognized that transfers within the EU may be treated as domestic transactions, and therefore this limitation is not considered to be a deficiency in this case.

775. For batch files from a single payer, where the payee's PSP is outside the EU, Article 7 (2) provides that complete information should not be required for each individual transfer, if the full information accompanies the batch and each individual transfer has an account number or a unique identifier.

Inclusion of Originator Information in Domestic Wire Transfers (c. VII.3):

776. For transfers within the EU, the Regulation states that only the account number or the unique identifier allowing the transaction to be traced back to the payer should accompany the transfer, provided that complete payer information can be provided within three working days of a request from the payee service provider.

Maintenance of Originator Information ("Travel Rule") (c.VII.4):

777. Under Article 12 of the Regulation, an intermediary PSP is required to ensure that all information received on the payer is maintained with the transfer.

778. According to Article 13 (1) and (2), an intermediary PSP inside the European Union, when receiving a transfer of funds from a payer's PSP outside the EU , may use a payment system with technical limitations (which prevent information on the payer from accompanying the transfer of funds) to send transfers of funds to the payment service provider of the payee. This provision applies, unless the intermediary PSP becomes aware that information on the payer required under this Regulation is missing or incomplete. In such circumstances, the intermediary PSP may only use a payment system with technical limitations if it is able to inform the payee's PSP of this fact, either within a messaging or payment system, or through another procedure, provided that the manner of communication is accepted by, or agreed between, both PSPs (Article 13 (3)).

779. In cases where the intermediary PSP uses a payment system with technical limitations, the intermediary PSP has to make available to the payee's PSP, upon request, all the information on the payer which it has received, irrespective of whether it is complete or not, within three working days of receiving that request (Article 13 (4)). The intermediary PSP has to keep records of all information received for five years (Article 13 (5)), as does the payee's PSP (Article 11).

Risk-Based Procedures for Transfers Not Accompanied by Originator Information (c. VII.5):

780. Article 8 of the Regulation requires the payee's PSP to have procedures for detecting whether the following information on the payer is missing:

- For transfers of funds where the payer's PSP is situated in the European Union, the information required under Article 6 of the Regulation.

- For transfers of funds where the payer's PSP is situated outside the European Union, complete information on the payer as referred to in Article 4, or where applicable, the information required under Article 13 of the Regulation.

- For batch file transfers where the payer's PSP is situated outside the European Union, complete information on the payer as referred to in Article 4 of the Regulation in the batch file transfer only, but not in the individual transfers bundled therein.

781. Article 9 gives instructions on what to do if there is incomplete information. The recipient service provider should ask for the information or reject the payment. Under Article 10, the payee's PSP has to consider missing or incomplete information on the payer as a factor in assessing whether the transfer of funds, or any related transaction, is suspicious, and whether it must be reported to the authorities responsible for combating ML or TF, in this case, the FIU-NL.

782. For a payer's PSP who regularly fails to provide information, the payee's PSP should (after giving warnings and setting deadlines) consider rejecting all transfers under Article 9 (2). Such termination should be reported. The fact that there is incomplete information is not itself a reason for reporting a transfer as suspicious or unusual per se. The absence of payer information is not listed as an indicator of an unusual transaction in the implementing regulation (UBWWFT) but the recipient service provider may have other reasons for reporting.

Monitoring of Implementation (c. VII.6):

783. According to Article 15 (3) of the Regulation, EU Member States have to appoint competent authorities to effectively monitor, and take necessary measures with a view to ensuring, compliance with the requirements of the Regulation. Article 23 (3) of the WWFT gives the DNB the responsibility for monitoring compliance with the EU Regulation. The authorities state that this is monitored through sample testing during on-site examinations.

Application of Sanctions (c. VII.7: applying c.17.1–17.4):

784. Article 15 (1) of the Regulation obliges Member States to lay down rules on effective, proportionate, and dissuasive penalties applicable to infringements of the provisions of the Regulation, and to take all measures necessary to ensure that they are implemented. Articles 26 and 27 WWFT give the power of sanction to the Minister, in respect of various offences, including the breach of the Regulation. The sanction power has been delegated to DNB by Article 5 of the WWFT implementing regulation UBWWFT. The sanction is a monetary penalty which appears to be proportionate and dissuasive.

Additional elements—Elimination of thresholds (c. VII.8 and c. VII.9) (c. VII.8 and c. VII.9):

785. The threshold of EUR1 000 only applies to payments made from within the EU to a third country. There is no provision with respect to incoming payments, except insofar as the payee PSP must have systems to detect incomplete information. There is no threshold for incoming payments. The

obligations on the payee PSP under Article 8 to detect missing information is not affected by the size of the payment. For outgoing payments, complete payer information must accompany payments from accounts but the threshold of EUR1 000 applies when the payment is not from an account.

Analysis of effectiveness

786. The requirements on wire transfer rules are comprehensive.

787. Some of the record keeping and retention provisions can only be found in the Wft and its implementing regulations. In order to regard the Wft provisions on these matters as applicable, it is necessary to accept the view that the definition of integrity in Articles 3:10 and 4:11 of the Wft encompass measures to mitigate ML and TF risk. This interpretation is discussed more fully below but is accepted for the purposes of the assessment. Nevertheless, it is not impossible that it should be subject to challenge and it would be unsafe to rely solely upon it.

788. The record-keeping and retention provisions in the Civil Code, the tax code, the WWFT, and the Wft taken together apply to most and very probably all of the records required for Recommendation 10. In practice, the authorities consider that all institutions are covered by the requirements and comply in a way that meets the Recommendation. Moreover, there is no suggestion that, in practice, there is any difficulty in obtaining the necessary information in a timely manner. However, the co existence of two general seven year record retention provisions (in the AWR and BW) along with specific provisions for five years is contradictory. Regulated financial entities might reasonably conclude that the specific retention requirements that are for five years or less could have no meaning unless they somehow overrule the general seven year requirements. The specific provisions in the WWFT and Wft do not currently unambiguously cover the requirements in Recommendation 10 (although amendments currently before Parliament will rectify a number of deficiencies). In particular:

- The provisions in the WWFT do not require the keeping or retention of records relating to account files and business correspondence.
- The provisions in the WWFT do not require the keeping or retention of records of beneficial owners other than in the case of one person acting on behalf of another.
- The provisions in the BPR Wft and BGFO Wft do not apply to the Wft category of financial institutions, to financial services providers, to management companies, to investment companies or to depositories.
- There are no provisions relating to records on customers in the Wgt.
- There is no provision giving the competent authorities the power to extend the record-keeping requirement in particular circumstances.

789. The supervisory authorities can enforce the requirements on record retention and wire transfers by applying the penalty provisions in Articles 1:75, 1:79 and 1:104 of the Wft, Chapter 7 of the Wgt and Article 26 of the WWFT. These are discussed more fully in the context of Recommendation 29.

3.5.2 Recommendations and Comments

790. The authorities are **recommended** to amend WWFT, Wft, and Wgt, so as to:

- Remove the ambiguity created by the different and conflicting record-retention provisions in the AW, BWR, WWFT, and Wft and make explicit that the record-retention requirements (including those in the BW and AWR) necessarily apply to all transactions and to business correspondence, account files, customer identification on all legal persons and arrangements and beneficial owners.

- Ensure that records of transactions are maintained in a way that permits reconstruction of transactions for the purpose of prosecution.

- Extend the record keeping requirement in the BPR Wft and BGFO Wft to the Wft category of financial institution, financial services providers, money transfer offices, investment companies, management companies and custodians.

- Give the authorities the power to extend the retention period if necessary in particular cases.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	**LC**	• The ambiguity caused by the contradiction between general record-retention requirements of seven years and specific requirements relating to financial entities that are of five years of less. • The record- keeping provisions do not explicitly require that records of transactions should be sufficient to permit reconstruction of transactions sufficient for a prosecution. • The authorities have no power to extend the retention period if necessary in particular cases. •
SR.VII	**C**	• This Recommendation is fully observed.

3.6 Monitoring of Transactions and Relationships (R.11 and 21)

3.6.1 Description and Analysis

Special Attention to Complex, Unusual Large Transactions (c. 11.1), Examination of Complex and Unusual Transactions (c. 11.2), Record Keeping of Findings of Examination (c. 11.3):

791. The obligations envisaged by Recommendation 11–which requires financial institutions to pay special attention to all complex, unusual large transactions, or unusual pattern of transactions, that have no apparent or visible economic or lawful purpose, and requiring that their background and purpose be examined, the findings of which should be recorded−are scattered in several provisions of the Dutch AML/CFT system, although, in certain instances, they are only implicit.

792. There are references to elements of R.11 in the context of the WWFT (concerning ongoing due diligence) and the BPR Wft (obligation to establish procedures with regard to transaction-monitoring):

- Article 3 (2) (d) WWFT obligates financial institutions, "where possible, to carry out constant monitoring of the business relationship ***and the transactions conducted during the existence of this relationship.***" This requirement is aimed at ensuring that transactions "tally with the knowledge which the institution has of the customer and the customer's risk profile, and to check the source of the assets where appropriate."

- Additional provisions for some financial institutions are addressed in the BPR Wft and the BGFO Wft. Pursuant to Article 14 (4) BPR Wft, financial undertakings, collective investment schemes and investment firms having registered office in the Netherlands are obligated to "establish procedures and measures with regard to the analysis of client information, also in relation to the products and services purchased, ***and with regard to the detection of deviating transaction patterns***."

793. The obligation to pay special attention to transactions is also presupposed by the obligation to report suspicious transactions (as discussed under R.13 in the Dutch system, these are called "unusual transactions"). Financial institutions are required to report unusual transactions, based on subjective and objective indicators. Some of the objective indicators obligate certain types of unusual transactions to be reported by imposing thresholds related to the nature of the transaction (for example financial institutions are obligated to report any money transfer in cash that equals or exceeds EUR2 000 under certain circumstances or cash transactions that equal or exceed EUR15 000 that involve a "cash exchange into a different currency or from small to large denominations); however these transactions, while "exceeding certain limits," do not appear to equate to "large" and may not necessarily be "significant transactions relative to a relationship."

794. The authorities explained that the transactions described by Recommendation 11 would be captured by the "Subjective indicator", which is provided for transactions for which the party with the duty to disclose has reason to presume that they may be related to money laundering or terrorist financing. Thus, an obligation to pay special attention to transactions in the circumstances required by criterion 11.1 can be deduced from the requirement to report unusual transactions based on subjective indicators and to the ongoing due diligence requirement. With regard to the "unusual patterns of transaction," this is expressly required by Article 14 (4) BPR Wft (which does not apply to all financial institutions).

795. The Explanatory Memorandum to Article 3 (2) (d) supports authorities' interpretation, as it states that "institutions can only detect unusual transactions if they have a good picture of the customer concerned. If certain transactions show that the customer is deviating from the profile, the institution has to investigate what risks are entailed in by this deviation".

796. There is no direct requirement for financial institutions to examine as far as possible the background and purpose of unusual transactions. The obligation to "examine" in the terms described above (not enforceable because of the nature of the EM) is implicit in the obligation to "report" unusual transactions based on subjective indicators. Likewise, while there is no direct requirement for financial institutions to set forth their findings in writing for the instances envisaged by Recommendation 11, this requirement could be implied by the record keeping requirements: provisions relating to retention of unusual transactions are found in Article 34 WWFT which obligates financial institutions to retain all information in Article 16 (2) WWFT (obligation to report unusual transactions) in an accessible manner for five years following the moment when the disclosure was made. Article 14 (5) BPR Wft, Article 21 (5) BGFO Wft and Article 26 (4) BGFO Wft have provisions pertaining to financial undertakings, collective investment schemes and investment firms respectively.

797. These provisions require the institutions to provide evidence of unusual transactions to be stored for up to five years after the services have been provided or up to five years after the termination of the relationship with the client. Authorities clarified that this also includes the requirement to make records available to auditors. However the rationale for requiring financial institutions to set forth their findings in writing and make them available for competent authorities, as envisaged by Recommendation 11, is different from the obligation to report suspicious transactions. Under Recommendation 11 financial institutions are to undertake these tasks even if the transaction will not be reported to the FIU.

798. In conclusion, while in the legal provisions referred above there are elements that address, for the most part in an indirect way, most of the requirements of Recommendation 11; the current legislative and regulatory framework could be streamlined to differentiate in a clearer way the obligations envisaged by Recommendation 11 from those pertaining to the reporting of suspicious (in the Dutch system "unusual" transactions).

799. Discussions with banks and insurance companies revealed that financial institutions are recording unusual transactions for customers even if it does not rise to a UTR filing under the subjective indicator. In several instances institutions were keeping these records in separate client files to prevent tipping off in the event a client asked to see their file. Therefore the obligation to "examine," "report," and set forth the findings in writing, appears to be, in practice, being met through the monitoring obligation set out by financial institutions. However, smaller banks, money transactions offices, money exchange and financial service providers, may not have the same monitoring systems available to detect unusual and large transaction patterns as larger institutions. Although these businesses are as likely to file subjective UTRs, the capacity to monitor unusual patterns and keep separate client files for UTRs and other unusual transactions is most likely limited. In some cases, money transaction offices, money exchanges and financial service providers ended client relationships in the event they filed subjective UTRs, although the record keeping requirement was implemented.

Special Attention to Countries Not Sufficiently Applying FATF Recommendations (c. 21.1 & 21.1.1):

800. There is no specific, enforceable provision requiring financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. The authorities explained that the Netherlands relies on the broader requirement envisaged by Article 8 (1) of the WWFT, which obliges financial institutions to perform enhanced due diligence "if and as a business relationship or transaction by its nature entails a greater risk of money laundering". The provision also states that such business relationships/transactions "may be designated by order in council," however, none have been so designated by the Dutch authorities.

801. Under the former NCCT-list procedures of the FATF, the DNB would send a circular to all institutions under its supervision with updates on the NCCT list notifying financial institutions that the countries in the view of the FATF are "insufficiently active in countering money laundering." The circular requested that financial institutions pay special attention to business relations with natural person and legal entities from the countries designated which have significant deficiencies in their AML/CFT regime.

802. The DNB also sent advisories to the Bankers Association in October 2007 and May 2008 requesting the Bankers Association bring the statement to the attention of its members to make sure that they can use it in their risk assessment.

803. In relation to those jurisdictions that have been the subject of public statements issued by the FATF since 2008, the DNB has continued its practice of issuing guidance, now on its website. The guidance indicates that "for the jurisdictions listed by the FATF, particularly those named in the public statement, the DNB and the MoF point out that maintaining business relations with residents of these jurisdictions, or carrying out transactions to or from these jurisdictions, poses a higher risk of ML or FT, which could lead to tighter measures". The guidance also states that "financial institutions are expected to consider the specific circumstances when deciding on the necessary CDD measures".

804. The DNB guidance addresses high-risk jurisdictions as set out by the FATF and outlines measures already taken by the authorities specifically related to Iran, "the importance of exercising vigilance in respect of all financial transactions with Iranian banks is underlined: the term "vigilance" is

elaborated on in stricter customer investigation, transaction monitoring and an obligation to report suspicious transactions." However this guidance is not enforceable.

805. After each plenary meeting of the FATF, the Ministers of Finance and Justice send a report to the Dutch House of Representatives (Parliament). This report contains the relevant issues discussed at the Plenary, including FATF public statements and relevant decisions and discussions. These reports are publicly available on the website of the House of Representative and therefore accessible for financial institutions.

806. The FIU-NL also posts the FATF public statement regarding the listing of countries with AML/CFT deficiencies on its website after each plenary, although no additional guidance is provided to financial institutions by the FIU. Private sector representatives indicated that they do not look at the FIU website nor receive any proactive information or guidance on these countries from the FIU-NL.

807. Although there are several measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries, these measures are provided through guidance, and therefore there is no direct and specific enforceable requirement for financial institutions to give special attention to the business relationships which fall short of the FATF standard for 21.1. The authorities explained that financial institutions would be expected to comply with the FATF requirement envisaged by criterion 21.1 as part of their general obligation to perform enhanced due diligence. However, there is no specific requirement for financial institutions to pay "special attention", as required by the standard. The DNB guidance, which is not enforceable, simply stresses that "maintaining" business relations or "carrying" out transactions in this context poses more risk, "which could lead to tighter measures", so it is not clear whether tighter measures are always required.

Examinations of Transactions with no Apparent Economic or Visible Lawful Purpose from Countries Not Sufficiently Applying FATF Recommendations (c. 21.2):

808. There are no specific provisions regarding countries not sufficiently applying FATF Recommendations, please refer to the analysis under criterion 11.2.

Ability to Apply Counter Measures with Regard to Countries Not Sufficiently Applying FATF Recommendations (c. 21.3):

809. With regard to the ability of the authorities to apply countermeasures it should be noted that, among the objective indicators that trigger a reporting of the transaction, one specifically deals with transactions with (legal) persons based in countries or areas that have been designated by the Minister of Finance and the Minister of Justice "as representing an unacceptable risk of money laundering or terrorist financing." Hence, authorities do have the ability to make such designations.

810. However, no such designation has occurred, so the relevant obligation has de facto not been implemented. Moreover, this requirement is limited to transactions (not to business relationships).

811. The authorities cite specific provisions of Council Regulations (EC) concerning restrictive measures against the Democratic People's Republic of Korea and Iran as the rationale for not having resorted to ministerial designations. They indicate that these regulations directly oblige financial institutions in The Netherlands to apply enhanced CDD and report transactions to the FIU. However, the provisions Council Regulations in question are not directly relevant to R.21 since their focus is on curbing proliferation financing rather than on taking measures vis-à-vis persons from or in countries that which do not or insufficiently apply the FATF Recommendations. The specific provisions largely call for action that is either already required by the FATF standard (*e.g.*, "continuous vigilance" or ongoing due diligence, and record-keeping) or not relevant for AML/CFT (*e.g.*, the reporting of suspicions of proliferation financing).

Although the authorities assert that, in practice, financial institutions report all transactions with these jurisdictions, they do not have a legal obligation to do so.

812. The DNB warns financial institutions about the FATF-listed jurisdictions/public statements and that maintaining business relationships and carrying out transactions with residents of such jurisdictions pose a risk of ML and TF, but this guidance is not enforceable.

813. The DNB website also states that provided in the case of Iran, Uzbekistan and Azerbaijan mentioned also that "any applications from banks for establishing branches in the Netherlands are subject to close inspection, with due account taken of developments in the adoption of new AML/CFT legislation". The authorities have explained that this statement is intended to be preventive in nature, but it is unclear though the relevance of such statement in guidance provided to financial institutions.

814. With respect to "limiting business relations and transactions with the identified country or country or persons in that country" this is only limited, according to the authorities, to "prohibiting the insurance services to new business". Authorities stated that these limitations are in force since December 2009.

815. Finally, authorities report that in the second half of 2010, DNB received an application for a license as a payment institution from a person who indicated that his financial activities would focus on offering transactions (money transfers) with Iran. Even though the formal license application requirements were all satisfactorily fulfilled and there were no problems regarding the fitness and propriety of the applicant, DNB decided not to grant the license because of the high risk involved with transactions with Iran. The authorities stated that the legal argument for not approving the license was based on the fact that the applicant could not organize his operations in such a way as to safeguard controlled and sound operations (art 3:17 Wft). Once DNB informed the applicant of the decision not to approve the license, the application was withdrawn.

816. Overall, for the reasons noted above, the countermeasures adopted by the Netherlands seem limited in scope, since, in the majority of cases, they are neither enforceable nor implemented.

3.6.2 Recommendations and Comments

With respect to Recommendation 11

- Streamline the legislative and regulatory framework, eventually by introducing a separate obligation for all financial institutions to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions that have no apparent or visible economic or lawful purpose, autonomous from the obligation to report suspicious transactions. Introduce an explicit obligation for financial institutions to examine as far as possible the background and purpose of unusual transactions.

With respect to Recommendation 21

- Consider re-introducing the practice of issuing detailed circulars to financial institutions after each FATF Plenary.

- Introduce an enforceable obligation for financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations.

- Introduce more specific provisions to implement all aspects of R21.

3.6.3 Compliance with Recommendations 11 & 21

	Rating	Summary of factors underlying rating
R.11	**LC**	• Some elements of the obligation are implicit and do not apply to all financial institutions. • No enforceable requirement for financial institutions to examine as far as possible the background and purpose of unusual transactions and to keep the findings in writing.
R.21	**PC**	• No specific enforceable obligation for financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. • No requirement for financial institutions to examine as far as possible the background and purpose of unusual transactions. • The existing countermeasures are limited in scope.

3.7 Suspicious Transaction Reports and Other Reporting (R.13-14, 19, 25 and SR.IV)

3.7.1 Description and Analysis

Legal Framework:

817. The reporting requirements are set out in Articles 15 and 16 WWFT. Implementing elements are contained in Article 4 and the annex of the UBWWFT. Sanctions are provided in Articles 26 and 27 of the WWFT.

Requirement to Make STRs on ML and TF to FIU (c. 13.1, c.13.2 and c.IV.1):

818. Pursuant to Article 16 of the WWFT, "an institution shall notify the FIU of an unusual transaction already conducted or of an intended unusual transaction within 14 days of establishing the unusual nature of the transactions." This Article applies uniformly to all financial institutions listed in Article 1 of the WWFT.

819. As required by Article 15 WWFT and following Article 4 UBWWFT, indicators of "unusual transactions" are set out in the annex to the UBWWFT. When met, they trigger the reporting of an unusual transaction. The annex to the UBWWFT refers to subjective and objective indicators. There is only one subjective indicator, the same for all financial institutions: "Probable money-laundering transactions or terrorist financing: Transactions in which the party with a duty to disclose has reasons to presume that they may be related to money laundering or terrorist financing". According to the explanatory memorandum to the WWFT, the institution will have to ask itself whether to report a certain transaction because it may involve money laundering or terrorist financing. Objective indicators relate, for example, to specific transactions exceeding a certain threshold or undertaken with designated countries. While these indicators have been drafted in relation to ML/FT risks, an objective UTR has to be reported without a suspicion that funds are the proceeds of a criminal activity. Consequently, for the purpose of assessing compliance with the requirements of Recommendation 13, only UTRs reported on the basis of the subjective indicator will be considered.

820. According to the explanatory note to the WWFT, the maximum 14-day period given for reporting unusual transactions only applies to transactions that must be disclosed on the basis of a subjective indicator. At the time of last AML/CFT assessment in 2004, unusual transactions had to be reported without any delay. The FIU explained that this change has been requested by the financial sector, but

recommends in its reporting regulation to report UTRs promptly. In addition, the explanatory note introduces the notion of "strong suspicion" of money laundering of terrorist financing where "the obvious course to take is to disclose the transaction as soon as possible." In this case the report has to be filed to the Police with a copy to the FIU.

821. Notwithstanding the absence of criminalization of TF as a separate and autonomous offence, the WWFT requires the reporting of transactions related to TF, as defined in the WWFT. Pursuant to Article 1 (1) (i) (3) WWFT, the definition of TF includes "the provision of financial support, as well as deliberate fundraising in aid of an organization of which the object is to commit crimes as referred to in Section 83 of the criminal code".

822. Sanctions for breaching the reporting obligation are found in Articles 26 and 27 WWFT. Based on Article 26, the Minister of Finance may impose an order for incremental penalty payment, and based on Article 27, the Minister of Finance may impose an administrative fine. (See section 3.10 for the distinction between a fine and an incremental penalty payment, and a discussion on the effective, proportionate and dissuasive character of these sanctions).

823. The reporting obligation differs from of the requirements of the FATF standard in three key areas. First, the obligation relates to the act of ML itself and so does not link the obligation directly to suspicions that funds are the proceeds of crime. Second, while the WWFT definition covers most of the funds which should be reported to the FIU in case of suspicion of TF, it does not cover the funds related to those who finance terrorism. However, these two differences have been considered technical and no impact on financial institution's reporting behavior has been found. In the Dutch context, there is no difference for reporting entities between a suspicion of ML and suspected proceeds of crime as the acquisition, possession, transfer, conversion or use of any proceeds of crime by itself already constitutes ML (see Article 420 bis, Penal Code). Therefore any suspicion of such acquisition, possession, transfer, conversion or use of proceeds of crime should automatically trigger a suspicion of ML. Regarding terrorism financing, if it is known or suspected that a person is financing terrorism, the subjective reporting requirement in the Dutch system will always apply to funds related to that person, since that knowledge or suspicion about that person would always trigger the 'reasonable grounds to suspect TF'.

824. A third difference relates to the requirement to report within 14 days of establishing the unusual nature of the transaction. This is not in line with Recommendation 13 requiring to promptly reporting any suspicions to the FIU.

No Reporting Threshold for STRs (c. 13.3):

825. Article 16 WWFT specifically mentions that attempted transactions fall under the scope of the WWFT. The rules that apply for performed transactions, also apply for attempted transactions. During the period 2007–2009, FIU-NL received an annual average of 1 800 reports that referred to attempted transactions. Based on Article 16 WWFT and the definition of a subjective UTR in Article 4 UBWWFT, transactions should be reported regardless of the amount of the transaction.

Making of ML and TF STRs Regardless of Possible Involvement of Tax Matters (c. 13.4, c. IV.2):

826. There is no impediment to the reporting of subjective unusual transactions based on thought that, among other things, the transaction involves tax matters. FIU-NL regularly receives reports that are related to tax matters.

827. In addition, Dutch law does not exclude the reporting of unusual transactions that are related to tax matters and Dutch case law indicates that the requirement to report suspicious transactions also includes tax matters. In October 2008, the Dutch Supreme Court (*Hoge Raad*) ruled that tax fraud can be

considered as a predicate offence for money laundering, in accordance with Article 420bis WvSr (see 2). Thus, the suspicion that a transaction may be related to the laundering of tax fraud falls into the subjective indicator that a transaction may be related to money laundering or terrorist financing and should be reported to FIU-NL.

Additional Element—Reporting of All Criminal Acts (c. 13.5):

828. The requirement to report, based on the subjective indicator, includes the laundering of the proceeds of all criminal acts that would constitute a predicate offense for money laundering. But the reporting obligation does not require financial institutions to report funds that are the proceeds of criminal acts if there is no relation between the act and money laundering.

Analysis of effectiveness (R. 13)

829. At first sight, the number of subjective UTRs (SUTRs) received by the Dutch FIU from financial institutions appears relatively high and uneven over the years, as indicated in the table below.

Total number of subjective UTRs received by NL-FIU			
	2007	**2008**	**2009**
SUTRs	82 488	292 483	88 382

830. But these data deserve further analysis. A one-off effect related to a single bank explains the 2008 peak, and the level of reporting greatly varies from one type of financial institutions to one other, as evidenced by the two tables below:

Subjective UTRs received by type of institution (number, amount, and ratio) excl. money transfers (Amounts in Euro)									
	2007			**2008**			**2009**		
Institution	**Amount[1]**	**SUTRs**	**Ratio**	**Amounts**	**SUTRs**	**Ratio**	**Amounts**	**SUTRs**	**Ratio**
Banks	795 629 000	5 322	149 498	425 070 000	5 011	84 827	577 134 000	3 396	169 945
Credit card companies	115 000	1	115 000	54 000	2	27 000	26 000	2	13 000
Finance companies	418 000	9	46 444	49 000	6	8 167	18 000	4	4 500
Insurance agents	0	1	0	160 000	1	160 000	0	1	0
Investment companies	0	0	0	0	0	0	0	0	0
Life insurance companies	4 597 000	27	170 259	6 467 000	13	497 462	4 795 000	9	532 778
Money remitters	8 355 000	516	16 192	23 842 000	1 528	15 603	8 825 000	1 623	5 437
Stockbrokers	0	0	0	150 000	1	150 000	4 189 000	18	232 722
Total	809 114 000	5 876	137 698	455 792 000	6 562	69 459	594 987 000	5 053	117 749

[1] Amounts have been calculated based on executed transactions. This means the intended transactions have been excluded in the amount.

Subjective UTRs received by type of institution (number, amount, ratio), money transfers (Amounts in euro)									
	2007			2008			2009		
Institution	Amount	SUTRs	Ratio	Amounts	SUTRs	Ratio	Amounts	SUTRs	Ratio
Banks	25 574 000	42 874	596	78 103 000	200 745	389	1 483 000	293	5 063
Money remitters	51 222 000	33 738	1 518	101 579 000	85 176	1 193	79 331 000	83 036	955
Total	76 796 000	76 612	1 002	179 682 000	285 921	628	80 814 000	83 329	970

831. The pattern of reporting is quite different depending on the type of financial institution. Money remitters are the main providers of SUTRs. In 2009, they represented more than 95 percent of the total. Banks represented approximately 4 percent of the total, and other financial institutions less than 1 percent. It should be noted that, in 2009, approximately 80 percent of the UTRs have been reported by only 2 institutions, both money transfer companies operating from outside the Netherlands. In addition to the relatively lower and decreasing level of reporting by banks, it has to be noted that reporting from insurance agents has been almost nonexistent, reporting from life insurance companies is very low regarding the large size of this industry in the Netherlands, and reporting from bureau de change is relatively limited.

832. The average amount per transaction reported by a money remitter is around EUR1 000 in 2009 (objective UTR threshold is EUR2 000, see R.19). On the other hand, the amount of the transactions reported by the banks are much higher, with an average of approximately EUR170 000 per transaction reported in 2009. Overall, there has been a slight decrease (15 percent) in the average amounts of transaction reported by financial institutions over the period 2007-2009 (excluding money transfers).

833. On average, during the 2005–2009 period, 16 percent of the SUTRs were ultimately declared suspicious by the FIU. This is almost the same number than for objective UTRs and may consequently raise issues on the quality of the reporting of suspicious transactions by financial institutions (see analysis for R.26). Nevertheless, the trend is improving over the period, with more than 22 percent of the SUTRs ultimately declared suspicious by the FIU in 2009.

834. From interviews conducted with the authorities, it appears that the high number of reports sent by the money transfer sector has mostly been prompted by a letter sent by the DNB to money transaction offices in March 2007 which created some confusion regarding the reporting requirement. In order to clarify the reporting requirement, the DNB issued a guidance letter in September 2008 to indicate that money transfers that are not paid in cash should only be reported when there is a suspicion of ML or TF.

835. Statistical analysis also shows a significant decline (30 percent) in reporting from banks in 2009. The authorities indicated that the decrease in overall banking activity due to the financial crisis may be an underlying factor explaining the decrease. But international comparisons do not indicate such a dramatic trend in other countries (see analysis below).

836. Based on meetings with financial institutions, assessors are of the views that the reporting system lacks effectiveness. Regarding the money transfer sector (approx. 95 percent of the SUTRs), none of those interviewed by the assessors considered that the money transactions offices represented the main ML or TF risk faced by The Netherlands. The level of reporting, therefore, appears to be out of proportion to the likely ML/FT activity. Regarding other reporting entities, mainly banks, there may be a difficulty to adopt a risk-based system of disclosure. Financial institutions were used to a rule-based system which was preponderant until 2005 and is still in place regarding the objective indicators, and some of them still use the old indicators to determine their reporting of subjective UTRs. Some institutions met by the assessors do not seem to understand the concept of suspicion, as they tend to blacklist the customer related to the transaction reported to the FIU. Nevertheless, the recent decrease in the numbers of SUTRs reported by the

banks may indicate a better understanding of the risk-based reporting system. Finally, it is not clear how the weaknesses identified in the protection of civil liability which introduces a 'reasonable grounds' test for not being liable adversely impacts the reporting regime, in requiring a high degree of certainty of an offense. It is possible to consider that the risk of a civil action is less significant in relation to small money transfers, often related to foreigners and persons with limited access to the judicial system, than for other financial institutions.

837. Finally, the average completion time for money transfers report was 9 days in 2009. The average completion time is calculated by the FIU based on the 80% of reports received with the shortest delay from the date of the transaction. In 2009, the average completion time for banks was 34 days. This is to compare with the 14-day limit set out by the WWFT. The starting point of the average completion time is the date of the transaction, while the starting point of the 14 days is the day when the financial institution establishes the suspicious nature of the transaction. But this delay appears particularly long and may limit the possibilities of seizure or confiscation of assets.

Financing of terrorism

838. Reporting of subjective UTRs is assigned a code by the FIU which is the same for suspicions of money laundering or terrorism financing, making impossible to distinguish between the two. After the FIU introduced 'profile reports' in 2008, a code was assigned to subjective UTRs related to specific TF typologies. In addition, the FIU queries the new reported transaction to ensure that, if reporting bodies report transactions they think may have a relation to terrorism and indicate this in the free text part of the report, these transactions will be detected. The following table indicates statistics on TF-related subjective UTRs over the period 2007–2009.

TF-related subjective UTRs			
	2007	2008	2009
Based on sub-indicator	N/A	141[1]	32
Based on queries	16	7	5
Total	16	148	37

[1] The number of reports in 2008 is relatively high, because FIU-NL requested banks to run a query on the history of the accounts over a period of 3 years.

839. It should be noted that these numbers are limited to subjective UTRs and do not capture reports sent to the FIU based on name matches with relevant lists, as this triggers reporting following an objective indicator. In addition, due to the difficulties for financial institutions to detect financing of terrorism without the analytical tools available to the FIU, it is interesting to mention that while 37 TF-related SUTRs have been received by FIU-NL in relation to TF in 2009, information from 256 SUTRs has been sent to competent authorities and added to ongoing terrorism cases or terrorism intelligence during the same year.

840. In addition, information shared with the assessors indicates that every year, since 2007, cases have been prosecuted on terrorism charges in the Netherlands including a substantial share of information coming from the FIU. Two concrete examples in relation to a terrorist organization have been provided to illustrate concrete results with respect to countering TF. Firstly, a SUTR filed with the FIU has been of crucial importance in starting a successful investigation, which resulted in the arrest and prosecution of the entire top structure of the organization in the Netherlands. The financial aspects in this case are one of the main pillars of the investigation. The suspects are still in custody and the first court hearing will take place in2011. Another case involves a suspected financier of the same organization whose assets have been frozen following a report received by the FIU. The case is still in court.

International comparisons

841. A first look at the number of subjective UTRs would suggest that the Netherlands is an outlier in relation to other similar countries,[88] with a far higher relative number of reports. Analytical work by the Fund suggests that most countries assessed LC or higher for Recommendation 13 receive in the range of 15–50 STRs per USD billion of GDP.[89] The assessors acknowledge that some variations in reporting levels between countries can be explained by differences in regime design[90] and by methods used to count STRs (*e.g.*, whether reports relate to individual transactions, which is the case in the Netherlands, or to a bundle of transactions associated with the same suspicious activity). However, the number of reports being filed in the Netherlands, around 110 per billion of GDP, appears especially high by comparison with other FATF member with a comparable financial sector, as shown by the following table.

Cross-country comparison of STR reporting

Country	2007	2008	2009	STRs/Billion GDP (2009)
The Netherlands[1]	82 488	292 483[2]	88 382	112
Belgium	12 830	15 554	17 170	37
Canada	39 036[3]	50 354	67 740	51
Italy	12 544	14 602	21 066	10
Spain	2 783	2 380	2 326	2

[1] Subjective UTRs.
[2] In registration year 2008, one frequent reporting institution was ordered by its supervisor to report approximately 175 000 subjective transactions from 2006 and 2007 with retroactive effect.
[3] April 1–March 31.

842. While these results could lead to the conclusion of excessive reporting and raise questions on the relevance of suspicious information provided to the FIU-NL, the analysis needs to be refined to take into account the high proportion of subjective UTRs filled by the money transfer sector in the Netherlands. By international comparison, the money transfer sectors share in the total number of reports received by an FIU is far much higher in the Netherlands. Subjective UTRs from banks represent 4 percent of the total in the Netherlands, while STRs from bank represent more than 25 percent in comparable countries.

843. If we turn again to cross-country comparison with similar countries, but focusing on STRs reported by banks and credit institutions, the picture is different as the level of reporting appears more in line with the comparator while slightly below the average, as indicated in the table below.

88 The sample here includes Belgium, Canada, Italy and Spain which have broadly comparable banking sector assets and domestic financial sector assets.

89 Fund Staff has analyzed STR reporting for 35 countries assessed under the 2004 methodology, including all FATF countries. This work is not yet published. GDP is used to normalize the STR reporting as a proxy variable for the value of the proceeds of crime in need of laundering within a jurisdiction and for the value of transactions in the AML regulated sectors, neither data point being readily available. It is assumed that the criminal economy and the value of transactions conducted in the AML regulated sectors are related to the size of the economy, and that, generally, the level of STR reporting should relate to the amount of laundering activity that is taking place—which is some function of the proceeds of crime flowing through the economy.

90 Differences in the regime design that amount to deficiencies against the FATF 40+9 are not legitimate reasons to justify low reporting levels.

Cross-country comparison of STR reporting by banks and credit institutions				
Country	**2007**	**2008**	**2009**	**STRs/Billion GDP (2009)**
The Netherlands[1]	5 322	5 011	3 396	4.3
Belgium[2]	4 207	4 034	3 628	7.7
Canada	10 359[3]			7.8[4]
Italy[5]	9 770	11 040	13 360	6.3
Spain[6]	1 953	2 156	2 111	1.4

[1] The data for 2008 does not include 175 000 transactions reported by one single institution in relation to money transfers. This reporting was based on positive enforcement actions of the DNB and is related to several years (2006: 76 000; 2007: 99 000). FIU-NL received the majority of these reports towards the end of 2007 and they have been processed in 2008.
[2] See CTIF/CFI 2009 Annual Report, http://www.ctif-cfi.be/doc/en/ann_rep/2009_en.pdf.
[3] 2008 FATF MER.
[4] Data for 2007.
[5] See UIF 2009 Annual Report, numbers rounded, http://www.bancaditalia.it/homepage/notizie/uif/relazione-2009.pdf.
[6] See SEPBLAC 2008 Annual Report, http://www.sepblac.es/espanol/informes_y_publicaciones/memoria2008.pdf and http://www.sepblac.es/espanol/acerca_sepblac/estadisticas/2009/PDF/comunicaciones_operaciones_sospechosas_regimen_general.pdf.

844. While it is possible to make international comparisons on the aggregated number of STRs, there are no sufficient data available to conduct a similar exercise at the disaggregated level, and in particular to compare the levels of TF-related STRs. Out of the 5 countries in our sample, only Italy publishes the number of TF-related STRs in the FIU annual report.

Protection for Making STRs (c. 14.1):

845. Pursuant to Article 19.2 WWFT, financial institutions are protected from criminal liability for breach of Article 272 of the criminal code (duty of confidentiality) when they report UTRs or provide additional data or information to the FIU. Based on Article 19.3 WWFT this protection also applies for persons who work for an institution having provided data pursuant to Article 19.2 WWFT. Consequently, it covers directors, officers and employees of financial institutions.

846. Protection from civil liability is laid down in Article 20 WWFT. The institution that made a UTR pursuant to Article 16 WWFT will not be held liable for damage caused to a third party as a result of that disclosure, unless it is demonstrated that no such disclosure should reasonably have been made in view of all the facts and circumstances. While the protection of civil liability of persons who work for financial institutions is not mentioned in Article 20 WWFT, the authorities consider that it is not possible to seek the civil liability of natural persons in relation to a UTR reported to the FIU.

847. The requirement that protection from liability only occurs in the case of good faith is not adequately covered in the Dutch legal framework. Firstly, there is no requirement to report in good faith regarding criminal liability. Consequently, it would not be possible to hold a reporting institution criminally liable in relation to the transactions that are reported. It would only be possible to prosecute this institution on the basis of other information. Secondly, regarding civil liability, the indication that "disclosure should reasonably have been made in view of all facts and circumstances" limits the safe harbor provision more narrowly than contemplated by the standard, which requires the protection to be provided in all circumstances where the suspicion has been reported in good faith. Article 20 WWFT introduces a reasonable grounds test which is higher than a good faith test. Notwithstanding if he was acting in good faith, the reporter would have to demonstrate that the disclosure was made in view of all facts and circumstances. This is a higher test than to prove that he was not acting with a malicious motive. The authorities indicated that, in practice, they never encountered problems in relation to good faith and both the criminal and civil liability.

Prohibition Against Tipping Off (c. 14.2):

848. Pursuant to Article 23(1) WWFT, institutions, are prohibited to disclose the fact that a UTR or related information has been reported or provided to FIU-NL and that this disclosure or information may give rise to further investigation. Based on Article 23(2) WWFT, the obligation to maintain confidentiality also applies to information obtained by a financial institution from the FIU regarding the follow-up given to a specific UTR. Because institutions generally do not have a high degree of certainty when they file a subjective UTR, it is not common practice within the financial sector to suspend an account or to terminate a customer relationship once a UTR has been filed, which limits the risk of triggering inadvertent tipping-off.

849. Sanctions for unlawful disclosure are found in Article 26 and 27 WWFT. Based on Article 26, the Minister of Finance may impose an order for incremental penalty payment, and based on Article 27 the Minister of Finance may impose an administrative fine.

850. Pursuant to Article 23 (4) WWFT the general prohibition to disclose is waived to permit institutions that have a common interest in the transaction or the customer, provided that the other institution is an EU Member State or a third country deemed to have equivalent AML/CFT standards. This waiver is not in strict compliance with the FATF standard, which generally prohibits any disclosure to third parties other than the competent authorities. However, the FATF has considered three EU Member State's evaluation reports that contained a similar waiver, and has concluded that the waiver is reasonable and represents a positive contribution to the overall effectiveness of preventive measures.

851. But the law does not prohibit institutions' directors, officers or employees to disclose the fact that a UTR or related information has been reported or provided to the FIU. No provision restricts disclosure of the fact that a suspicious transaction has been identified and that a UTR is in the process of being prepared.

Additional Element—Confidentiality of Reporting Staff (c. 14.3):

852. Article 22 WWFT states that any person receiving and/or providing information related to a transaction is obliged to confidentiality on its content in any further or other way, than is required for the performance of that party's duties or than is required pursuant to the WWFT. Pursuant to Article 22 WWFT, the FIU keeps confidential the names and personal details of staff of financial institutions that make a UTR. This would theoretically not prevent a prosecutor to request this information from the FIU during an ongoing investigation, but no such case happened in 16 years of UTR reporting.

853. Consideration of Reporting of Currency Transactions Above a Threshold (c. 19.1):

854. Pursuant to Articles 15 and 16 WWFT, and Article 4 and annex UBWWFT, the Netherlands have implemented a system where financial institutions have to report to FIU-NL certain transactions in cash above a fixed threshold. FIU-NL serves as a national central agency with a computerized database.

855. The table below summarizes the different situations where financial institutions should report cash transactions to FIU-NL:

Type of institution	Cash threshold	Additional conditions
Credit institutions Financial institutions Investment firms Collective investment schemes Money transaction offices	EUR15 000 – All operations	Cash exchange into a different currency; or Cash exchange from small to large denominations.
	EUR2 000 – Money transfers	Funds are made available in the form of notes and coins; or Funds are made payable in the form of notes and coins
Credit card companies	EUR15 000	Cash deposits into a credit card account

856. The Dutch system does not require financial institutions to report all transactions in currency above a fixed threshold but is limited to certain transactions. The feasibility and utility of implementing a system where financial institutions report all transactions in currency above a fixed threshold has been considered when drafting the WWFT. But based on previous experience, and particularly a EUR15 000 threshold for car dealers which prompted too many UTRs, it was decided to establish thresholds targeted to certain specific risks and products, than to have a one size fits all approach that would have either led to too much reporting with a low threshold, or deprived FIU-NL information from risky sectors with a too high a threshold, while being costly for all financial institutions.

Additional Element—Computerized Database for Currency Transactions Above a Threshold and Access by Competent Authorities (c. 19.2):

857. The UTRs reported based on an objective cash threshold are maintained with all UTRs in the computerized database of FIU-NL. This database is only accessible by FIU personnel. Other officers, such as FIOD liaison officers are, under certain circumstances, allowed to access the database, but only after signing a declaration of confidentiality. The FIU-NL staff may access the data for examination and analysis. In addition to the UTR database, FIU-NL has another database that contains all transactions that have been classified suspicious after FIU's analysis, including transactions which were initially reported in UTRs based on an objective cash threshold. After authorization, competent authorities have digital access to the information in this latter database, through an Internet Portal called IVT.

858. FIU-NL is currently implementing a new computerized system (GOAML) that will contain both the unusual and suspicious transactions. This system, that offers many new possibilities on data-examination and analysis, will only be accessible to the FIU personnel. Other competent authorities will still be able to consult transactions that have been classified suspicious through the IVT.

Additional Element—Proper Use of Reports of Currency Transactions Above a Threshold (c. 19.3):

859. The FIU-databases are strictly secured and separated from all other systems and can only be accessed by authorized personnel bound to confidentiality and having been submitted to a strict screening process. Unless it has been classified as suspicious by the FIU and is no longer a UTR, the information can only be accessed following a request by the prosecutor.

Feedback and Guidelines for Financial Institutions with respect to STR and other reporting (c. 25.2):

860. *[Note: guidelines with respect to other aspects of compliance are analyzed in Article 3.10*] In The Netherlands, institutions are required by the WWFT to report unusual transactions and it is the responsibility of the FIU to judge if the reported transaction is suspicious. To inform institutions as to what kinds of transactions should be reported under Article 16 of the WWFT, the Annex to the WWFT implementing Decree (UBWWFT) lists a series of indicators that should prompt institutions to file unusual transaction reports. These include a subjective indicator (that the institution has reason to presume that a

transaction may be related to money laundering or terrorist financing) and various objective indicators (such as that a transaction in cash is of more than EUR15 000). Article 13 of WWFT requires the FIU to give a reporting institution information about the follow up to any report that has been submitted.

861. The Ministries of Finance and Justice have, in the past, organized an Indicators Working Group that analyses trends, typologies and causes of money laundering and terrorist financing, with a view to reviewing the indicators. In addition, it is the duty of the Committee on the Duty to Disclose Unusual Transactions (established under Article 21 of the WWFT) to consider the indicators. Both the Working Group and the Committee have included representatives of the private sector and the private sector representatives informed the mission that neither body had met for well over a year prior to the mission. However, the authorities confirmed that there had been a meeting of the Committee on the duty to disclose on May 26, 2010.

862. The Ministries of Finance and Ministry of Justice issued a joint memorandum on 20 May 2008 setting out the basis for providing feedback on STRs. The memorandum describes the approach to feedback on the basis of the response to individual reports and the publication of information on trends and analyses. It identifies five kinds of feedback:

- Individual: confirmation of receipt
- Individual: information that a report had been deemed suspicious by the FIU
- Individual: notification of result
- General: statistical analysis of the reports which were passed on
- General: casuistry, typologies, trends.

863. The routine feedback in respect of a report consists of a receipt for the report and the allocation of a registration number. The FIU is concerned that criminal investigations may be compromised if a customer were to be informed that a transaction were regarded as suspicious and the FIU will only inform a reporting institution that a transaction is regarded as suspicious if the supervisor confirms that the reporting institution has an independent department for money laundering that can be relied upon to protect the information. Where there is an investigation arising from or involving the report and this produces a result, this can only be notified to the reporting institution under Article 39f of the Data and Criminal Records Act, if the Board of Procurators General agrees.

864. The FIU publishes an annual report which gives statistical data on unusual and suspicious reports. This gives breakdowns of reports by reporting sector, by region, by reason for report and much other data. The report also gives details of particular cases and case law in an Annex to the report.

865. The FIU also provides other information and guidance to institutions. For example, an analysis of the profile of an account of a person involved in terrorist financing was prepared and this led to guidance to institutions on how to detect such patterns. The FIU reported that this had resulted in useful reports being received from institutions.

Effectiveness of Implementation (R.25)

866. The approach to feedback in the 2008 memorandum is thoughtful and well structured. The analysis undertaken by the FIU into terrorist financing patterns was impressive and there is no doubt that the FIU is committed to providing what information it can.

867. However, financial entities told the mission that the measures in the 2008 memorandum had not resulted in feedback of a sufficiently useful nature. The entities stated that normally, the extent of feedback on individual reports was confined to the receipt of an identification number and, where this occurred, to a notification that an unusual report was deemed to be suspicious. Most entities had received a notification from the FIU that a report had been deemed suspicious but some had only received this information from the supervisory authorities. It was also pointed out that, once an entity knew that a report had been deemed suspicious, they would undertake no further business with the client. However, the reporting entities remained ignorant as to whether the suspicion ever turned into a conviction or if the person or company concerned was eventually cleared. Their obligation to refuse to do business remained (although did not apply to their competitors who were unaware of the report). This prolonged state of limbo was regarded as unsatisfactory.

868. Private sector entities and associations stated that meetings with the FIU were rare in practice and that such meetings as did take place were concerned with more practical matters such as the way to deliver reports electronically. Entities to whom the mission spoke were either unaware of the other guidance available from the FIU or considered it to be too generalized to be helpful. It was pointed out to the mission that the FIU did not consult the private sector prior to issuing such guidance and such consultation might help the FIU prepare guidance in a more helpful manner. Some entities felt that the newsletters previously issued by the FIU were more effective as there was no alert system for drawing attention to new information on the FIU web site and so institutions got out of the habit of checking it for guidance.

869. As a result, entities stated that they did not consider that they had sufficient guidance on what the FIU would wish to see by way of reports.

870. It is inevitable that, to some degree, there may be some frustration from reporting institutions, since the process of monitoring to detect unusual transactions can be expensive and it would assist reporting institutions to know that their reports led to convictions. However, the inevitable delays in investigations and the use of a wide range of data in addition to reports when conducting investigations are bound to mean that there is rarely a direct connection between a report and a conviction. Moreover, in the Dutch system, it is possible for law enforcement agencies directly to access data from reports designated as suspicious by the FIU and in such cases, the FIU will not know who has seen the information and what use is made of it.

871. Nevertheless, it is regrettable that despite commendable efforts by the FIU and a determination by all parties to cooperate, the outcome is not as any of the parties would regard as satisfactory.

Statistics (R.32)

872. Annually, FIU-NL produces and distributes to a vast number of parties a substantial report on statistics and analyses. This report is also available on the FIU-NL website and is translated in English for international purposes. A sample of these statistics and additional information provided by FIU-NL has been used in the analysis of effectiveness for Recommendation 13 (see above).

3.7.2 Recommendations and Comments

873. In order to comply fully with Recommendations 13, 14, Special Recommendation IV, and Recommendation 25, the authorities should:

With respect to Recommendation 13 and Special Recommendation IV

- Ensure that suspicious transactions are reported promptly to the FIU.

- Enhance the effectiveness of the reporting system, including by raising awareness of financial institutions on the detection of suspicious transactions.

With respect to Recommendation 14

- Ensure that protection from criminal liability only applies if suspicions are reported in good faith.
- Ensure that demonstrating good faith is sufficient to be protected from civil liability, without having to prove that disclosure has reasonably been made in view of all facts and circumstances.
- Extend the tipping-off prohibition to apply to directors, officers and employees.
- Extend the tipping-off prohibition to cover cases where transactions are being reviewed internally to determine whether an STR should be filed.

With respect to Recommendation 25

874. The authorities are **recommended** to reconvene the Article 21 Committee or the Indicators Working Group to establish with the representatives of the reporting institutions how best to disseminate the analysis that is currently produced. They are further recommended to consider issuing alerts to institutions when new information is available on the FIU web site. Some off the difficulties in providing feedback relate directly to the decision to require institutions to make unusual rather than suspicious reports, the way in which those unusual reports are deemed suspicious and the method of dissemination of the reports to law enforcement. Such matters are discussed elsewhere in the context of the FIU.

3.7.3 Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV

	Rating	Summary of factors underlying rating
R.13	**LC**	• The 14 days period to report after a transaction has been established suspicious does not comply with the requirement of prompt reporting and raises an effectiveness issue in relation to the recovery of criminal assets. • Reporting by insurance agents, life insurance companies and bureaux de change is particularly low, which raises concerns regarding the effectiveness of the reporting regime.
R.14	**PC**	• Protection from criminal liability for STR reporting applies in the absence of good faith. • Protection from civil liability for STR reporting is subject to inappropriate conditions. • Tipping-off prohibition does not apply to directors, officers and employees. • Tipping-off prohibition does not apply to information in the process of being reported.
R.19	**C**	• This Recommendation is fully observed.
R.25	**PC**[1]	• Feedback not regarded as sufficient by the private sector.
SR.IV	**LC**	• Technical deficiency in the WWFT definition of TF limits the reporting obligation. Reporting of funds related to those who finance terrorism is not required. • The 14 days period to report after a transaction has been established suspicious does not comply with the requirement of prompt reporting.

[1] This is a composite rating, taking account of other comments relating to Recommendation 25, *e.g.*, in section 3.10.3.

Internal controls and other measures

3.8 Internal Controls, Compliance, Audit, and Foreign Branches (R.15 & 22)

3.8.1 Description and Analysis

Legal Framework:

875. The WWFT contains no explicit provisions on internal controls, compliance or audit and only limited provisions on training in Article 35. Given the limited provisions in the WWTF, it is necessary for the authorities to rely on the provisions in the Wft to meet the criteria relating to Recommendations 15 and 22. Articles 3:10 and 4:11 of the Wft. oblige specified regulated financial entities to have measures in place to prevent transgressions of any law by an enterprise and its employees. Such measures would include internal controls, training, compliance, and audit. Article 5 of the Wgt Regulation imposes a requirement on bureau de change to have internal controls necessary to ensure implementation of AML/CFT obligations.

876. Provisions on compliance functions are in Articles 21 of the BPR WFT and Article 31c of the BGFO Wft. Internal audit departments are required by Articles 17 of the BPR Wft and Article 31 of the BGFO Wft. Training for staff is required by Article 10 of BPR Wft and by Article 17 of BGFO Wft. These provisions are not explicitly linked to AML/CFT matters but the authorities state that such matters are implicitly extended to such matters by the obligation in Articles 3:10 and 4:11 to have measures in place that ensure compliance with any law. This is discussed in more detail below.

877. Article 2 of the WWFT has provisions relating to the overseas branches and subsidiaries of Dutch institutions.

Establish and Maintain Internal Controls to Prevent ML and TF (c. 15.1, 15.1.1 and 15.1.2):

878. The use of the Wft to impose requirements for ML and TF

879. There are no direct provisions in the WWFT requiring regulated financial entities to have internal controls to prevent ML and TF. There are, however, provisions in the Wft requiring internal controls. In the view of the authorities, these provisions require controls necessary to create AML/CFT defenses as defined in the WWFT. The assessors accept that the Wft provisions can be interpreted as requiring internal controls for AML/CFT defenses, but considers that the legal position is not robust. Moreover, the provisions do not apply to all regulated financial entities and more specific provisions are necessary.

880. Articles 3:10 and 4:11 of the Wft oblige certain entities to have policies that must be designed to safeguard controlled and sound business operations. These Articles do not refer directly to ML or TF. However, Article 3:10 (1) (b), Article 4:11 (1) (b) and 4:11 (2) require measures to prevent the entities that are subject to these Articles and their employees from committing offences or other transgressions of the law that could damage confidence in the financial enterprise or the financial markets. Articles 3:10(1(c) and Article 4:11 (1) (c) require institutions to have measures to prevent confidence from being damaged as a result of clients' activities. The authorities consider that these Articles effectively import into the Wft, the obligations created by the WWFT. This view is reinforced by the fact that certain provisions of the implementing regulation refer explicitly to client identification obligations (Articles 14 of the BPR Wft and Articles 21 and 26 of the BGFO Wft). The authorities state that these Articles are intended to encompass all the AML/CFT obligations created by the WWFT. The view of the authorities is that provisions in the Wft, relating to internal controls (relevant to Recommendation 15) and the supervisory powers and sanctions (relevant to Recommendations 17, 23 and 29) and supervisory cooperation powers (Recommendation 40) can be used to monitor and enforce WWTF obligations.

881. The legal position is rendered more complex by the fact that the relevant Articles of the Wft and the relevant Articles of the detailed implementing regulations (BPR and BGFO) each apply to a list of specified categories of regulated financial entity and that the application differs in different Articles. Specifically, Article 3:10 of the Wft applies the requirement to have controls to clearing institutions, entities for risk acceptance (reinsurance vehicle), credit institutions, payment institutions (including money transfer offices) and insurers. Article 4.11 applies the requirement to have controls to a management company, investment company, investment firm depository and financial services provider (insurance brokers). These provisions do not, therefore, apply to the Wft categories of financial institutions or collective investment schemes.

882. The authorities have explained that the reference to a financial institution in the Wft is not intended to imply that there is a license category known as "financial institution." The definition has a much narrower meaning than that normally associated with the term "financial institution" and refers only to entities that are not banks but which undertake certain activities. In fact, there are no entities that meet this definition at present in The Netherlands and the authorities have stated that any entity carrying out the activities included within the definition would, in practice require a license under another license category in the Wft. It is accepted that the authorities would not grant a license to an entity meeting that definition. The fact that some of the provisions do not apply to "financial institutions" is not therefore regarded as significant.

883. The Wft (Article 3:17 and 4:14) also provides for detailed rules to be established in regulations that cover the control of integrity. "Integrity" is defined to cover transgressions of the law and relations with clients that might undermine confidence and the authorities state this encompasses measures to combat ML and TF. On the interpretation of the law described above, this would therefore mean that the detailed requirements in the implementing regulation could also be used to justify the use of WFT provisions and supervisory powers to implement WWFT obligations. The Wft provisions on integrity do not however apply to the Wft category of collective investment schemes.

884. The argument that the provisions described above allow the use of the Wft provisions and supervisory powers to monitor and enforce WWTF obligations and (in the case of internal controls, compliance, audit and training, to fill in the gaps in the WWFT) is open to challenge for the following reasons:

- The AFM informed the mission that, on at least one occasion, they considered that a breach of AML/CFT obligations was sufficient to justify removing a license from a regulated entity. There is no provision for removing a license for such an offence in the WWFT and the only provision for removing licenses that the AFM could use would be Article 1:104 of the Wft–which provides for license revocation as a penalty for breaches of the Wft. In that case, the AFM did not feel able to use the power in Article 1:104 of the Wft to withdraw a license from a regulated financial entity for failing to implement adequate CDD measures, since they did not think the connection between the Wft integrity provisions and the WWFT were sufficiently robust to survive an appeal (they nevertheless persuaded the entity voluntarily to give up the license, as is frequently their practice and, post mission, pointed out that the removal of a license would always be a last resort).

- The Wgt also has provisions, similar to those in the Wft, that require a bureau de change to have measures in place to protect integrity—which means to prevent transgressions of any law. However, in the case of the Wgt there is an explicit obligation to have measures in place to implement the provisions of the anti money laundering law. It could be argued that, given that precedent, the absence of comparable provisions in the Wft implies an intention **not** to use the

Wft provisions to enforce WWFT obligations (although the authorities state that these differences are a reflection of different legislative histories).

- The WWFT has some provisions that create obligations to enhance implementation (such as requirements to inform employees of the law's provisions) but does not include measures on internal controls or other measures required by the Recommendations and it could be argued that the omission of such other requirements from the WWFT was deliberate and should not be overridden by importing provisions imposed for quite different purposes in the Wft.

- One major regulated financial entity interviewed by the mission stated that they would regard the use of Wft powers to implement AML/CFT defenses not explicitly included in the Wft or not explicitly stated to be relevant to AML/CFT as being open to challenge although this is not regarded as necessarily definitive on its own and other institutions made no comment on this point).

885. The provisions of the Wft implementing regulations that impose the more detailed requirement for internal controls to mitigate integrity risk do not apply uniformly to all regulated financial entities. Each Article defines its own scope and different articles differ in the definition of their scope. While the Articles usually apply to credit institutions, clearing institutions and insurers, they frequently exclude the Wft categories of financial services providers. Occasionally, other entities, such as entities for risk acceptance, investment firms, management companies, investment companies, collective investment schemes and depositories are excluded from the scope of requirements on internal controls and related matters. All regulated financial entities have obligations to implement WWFT and yet none of the Wft measures necessary to meet the requirements of the Recommendations apply to all of the Wft categories and most apply to varying combinations of such categories. The description below of the analysis of compliance with the Recommendations describes, in each case, where the provisions exclude certain categories of regulated financial entity.

886. Moreover, there are particular difficulties with respect to the Wft category of collective investment schemes:

887. Some of the provisions in the implementing regulation BGFO Wft apply directly to collective investment schemes. Other provisions refer to management companies, investment companies and depositories (sometimes to all of these and sometimes to one or more of them).

888. As can be seen from the analysis above, there is uncertainty over whether the provisions on internal controls in the Wft amount to a requirement that such controls should mitigate ML and TF risk. Moreover, the provisions of the Wft imposing internal control and related obligations apply only to some but not all categories of regulated financial entity, even though all of them are subject to the WWFT. For the purposes of this assessment, the assessors accept the interpretation of the authorities that the provisions on internal controls (and other provisions on such matters as compliance units, internal audit, record keeping and information exchange) that are in the Wft can be used to implement AML/CFT defenses. However, as noted above, even with this interpretation, the obligation to have internal controls is not comprehensive.

Specific provisions in the Wft and Wgt on internal controls (c15.1):

889. Articles 3 to 11 of the WWFT impose customer due diligence obligations on institutions subject to the Act and the authorities state that it is implicit that any institution subject to the Act should have sufficient internal controls to ensure that it fulfils these obligations. Articles 15 and 16 of the WWFT impose an obligation to report unusual transactions. Indicators of what should be regarded as reportable

unusual transactions are set out in the Annex to the implementing decree (UBWWFT). The WWFT does not establish any requirement to have systems and controls in place to detect such transactions so as to be able to report them, although the authorities state that such procedures and controls would be necessary in order to be able to meet the obligation to recognize unusual transactions and that, in practice, their experience is that this is what happens. Article 35 of the WWFT imposes a direct obligation to ensure that staff are familiar with the provisions of the Act but does not make it a requirement to inform staff of the nature of any internal controls and systems. The assessors do not accept that the criteria in Recommendation 15 can be met by creating an obligation to recognize and report suspicions and then relying on an assumption that this will result in the appropriate controls being put in place. It is therefore necessary for the authorities to rely on the Wft to meet the criteria in Recommendation 15 for explicit requirements that control training, compliance, audit, etc. are made.

890. Article 10 of the BPR Wft has been issued to implement the requirement for rules in Article 3:17 of the Wft referred to above and applies to clearing institutions, credit institutions, payment institutions, insurers and branches. It states that the regulated financial entities in these categories should make an analysis of integrity risks, translate policies into procedures and measures and inform all business units of these measures. Article 17 of the BGFO Wft (which implements Article 4:14 of the Wft) makes similar provisions for collective investment schemes, management companies and custodians. Article 23 of the BGFO Wft (also implementing Article 4:14 of the Wft) requires an investment firm to have procedures and measures for the honest conduct of business, but there is no link back to concept of integrity risk (which is deemed by the authorities to encompass AML/CFT obligations) and the Article does not require the investment firm to inform the business units of these measures. Thus, there are no training provisions for investment firms and financial services providers and no requirement to make an assessment of integrity risk.

891. Article 5 of the Wgt Regulation requires a bureau de change to have procedures and measures relating to internal controls that will ensure compliance with at least the provisions of the two Acts that were the predecessors of the WWFT. The July 2008 decree that implements the WWFT makes amendments to a number of statutes to delete the references to the predecessor statutes and replace them with references to WWFT. However, it makes no such amendment with respect to the reference in Article 5 of the Wgt Regulation (although such an amendment will be made at the earliest opportunity.

Independent compliance function (c15.1.1 and 15.1.2):

892. Article 21 of the BPR Wft and Article 31c of the BGFO Wft require clearing institutions, credit institution, payment institutions, insurers, branches, and investment firms to have an independent compliance function. The compliance function is required to verify compliance with statutory rules. The statutory rule to which the Article refers includes statutory rules issued under the WWFT. The authorities state that they interpret this to mean that the compliance unit must verify compliance with any rules or procedures designed to ensure that a regulated entity meets its AML/CFT obligations under the WWFT as well as under the Wft itself. The requirement to have compliance functions does not apply to management companies, investment companies, depositories, or financial services providers.

893. In respect of banks that provide investment services or activities in the Netherlands (but not other banks) and in respect of investment firms, Article 21 of the BPR Wft and Article 31c of the BGFO Wft make additional requirements for the compliance unit. The unit must:

- Advise those providing services on compliance with statutory and internal rules.
- Supervise the soundness and effectiveness of internal rules.

- Assess the effectiveness of procedures and measures.
- Report at least once a year to those responsible for day to day policy of the entity.
- Have the necessary authority, means, expertise and access to information to carry out its duties independently and effectively.
- In the case of an investment firm (but not a bank providing investment services) the compliance unit must monitor compliance with statutory and internal rules.

894. There is no requirement on any entity to have a Compliance Officer, although clearly a compliance function as required by the provisions described above would be staffed by officers and would have a person who was responsible for it. However, there is no requirement that such a person should be at management level.

895. There is no provision that the compliance function should have timely access to any data. Even though the authorities state that this is implicit, there is no reference to data on customer identification and other CDD information, transaction records and other relevant information.

896. There are no requirements in the Wgt on bureaux de change to have compliance officers. Some do so voluntarily.

Independent Audit of Internal Controls to Prevent ML and TF (c. 15.2):

897. Article 17 (4) of the BPR Wft require clearing institutions, credit institutions, insurers, branches, and payment institutions to have an internal audit function. This should audit, in an independent manner, the procedures and measures and the structure of the organization at least annually. While there is no direct reference to ML and TF, the provisions apply to all procedures and measures. There is a similar requirement in BGFO 31(6) that requires an investment firm to have an annual assessment (not audit) by an internal control (not audit) unit. The authorities state that the distinction between audit and control function in the English version is a translation error and has no significance. There is no requirement for internal audit for a financial services provider management company, collective investment scheme, custodian or investment company. Article 10 (5) BPR WFT requires institutions to have independent oversight of its implementation of its procedures and measures and that it should have procedures to ensure that identified shortcomings and weaknesses are reported to the compliance function. Above all this Article states in Article 10 (6) that these identified shortcomings and weaknesses lead to an adjustment of mentioned policies, procedures and measures. The assessors are satisfied that the internal audit requirements apply to the AML/CFT obligations.

898. Article 17a of the BPR Wft, amplifies the role of the internal audit department in respect of a bank (but not the other entities referred to in Article 17) and Article 31a amplifies the role of the internal control unit for an investment firm. Under these provisions, the internal audit department should:

- Establish and implement an audit plan to examine and assess the soundness and effectiveness of the systems, internal control procedures and rules of the bank.
- Make recommendations.
- Verify whether these recommendations are followed up.
- Report at least annually to the persons who determine the day-to-day policy of the bank.

899. There is no requirement that the internal audit department should be adequately resourced but the supervisory authorities consider this matter during on-site examinations and require institutions to make adequate resources available.

900. The Explanatory Note for Article 7 of the Wgt Regulation, which defines the term "integrity sensitive position," refers to an internal auditor but the Regulation does not require a bureau de change to have an internal auditor.

Ongoing Employee Training on AML/CFT Matters (c. 15.3):

901. There is no direct obligation to provide training on AML/CFT matters. Article 35 of the WWFT requires institutions to inform employees of the provisions of the Act and to train employees to recognize unusual transactions Articles 10 of the BPR Wft, and Articles 17 of the BGFO Wft require clearing institutions, credit institutions, insurers, payment institutions, management companies, collective investment schemes, depositories[91] (but not entities for risk assessment, investment companies, investment firms, or financial services providers) to inform all business units of the policies, and measures designed to mitigate against integrity risk (which, as discussed under c 15.1 above, is deemed to include measures to mitigate against ML and TF risk, even though there is no reference to this in the requirements to inform business units of internal controls). There are no explicit requirements that employees should be trained in new developments, including information on current ML and TF techniques but this would be implicit in the requirement to train staff to recognize unusual transactions. The authorities suggest that the requirement to provide training in UTR recognition implies a training requirement in new developments, trends and typologies. However, there is no explicit requirement. The assessors experience in interviews demonstrated that training in typologies, trends or new developments was not always given and that the absence of such training did not result in sanctions.

902. There is no additional requirement relevant to training staff of bureau de change in the Wgt or implementing Regulation which are covered by the WWFT obligation. .

903. The Wft and WWFT provisions do not include any further information on the nature of the measures an institution might take to ensure that employees were informed of the provisions of the WWFT and how they should be informed of the policies and measures established to mitigate against integrity risk.

904. The DNB and AFM state that the extent of training required would be tested during on-site inspections by asking staff about their knowledge of the procedures. Regulated entities confirmed to the mission that the DNB and AFM obtain copies of training policies and materials, interview staff and make suggestions during AML/CFT inspections. All the entities interviewed confirmed that, in practice, some training on CDD and reporting was given.

Employee Screening Procedures (c. 15.4):

905. The Wft requires senior officers and owners of certain regulated entities to be subject to a full fit and proper test and there are requirements for some employees to be subject to a propriety test. However, there is no comprehensive requirement for screening to ensure high standards that applies to staff in all relevant institutions.

906. Articles 3:8 and 3:9 of the Wft require that senior officers of clearing institutions, credit institutions, entities for risk acceptance, payment institutions and insurers have expertise and are otherwise fit and proper. Articles 4:9 and 4:10 set out similar provisions for senior officers of management companies, investment companies, investment firms, depositories and financial services providers.

91 The authorities state that the actual reference to custodians is a mistranslation.

907. Article 2 (1) of the Wgt states that the integrity of the senior management of a bureau de change is a criterion for considering registration. Registration may be cancelled if the assessment of the integrity of one or more of those responsible for the day-to-day policy of a bureau de change is such that it might impair the integrity of the financial system.

908. Article 13 of the BPR Wft creates an obligation to ensure the propriety of staff in integrity sensitive positions and this applies to the same institutions as are subject to Articles 3.8 and 3.9 of the Wft, except for entities for risk acceptance. Article 20 of the BGFO Wft makes a similar provision on the propriety of staff in sensitive positions and applies to a management company, collective investment scheme or depository. Article 25 of the BGFO makes a similar requirement for investment firms. Article 28 of the BGFO requires a financial services provider to ensure that all of its employees pass a properness test. There is no such requirement for an investment company.

909. Article 7 of the Wgt Regulation requires the management of a bureau de change to form an opinion of the integrity of new and existing recruits. However, no requirements are made, as to what action to take in the event that such an opinion is a negative one. The authorities consider that it is implicit that a negative opinion would result in a contract being terminated (or not entered into).

910. There are no other more general provisions requiring companies to put in place screening procedures to ensure high standards when hiring employees.

911. All private sector regulated financial entities interviewed by the mission confirmed that they had employee screening procedures in place. Most, but not all, had screening for all employees. Some had more rigorous approaches for more sensitive positions.

Additional Element—Independence of Compliance Officer (c. 15.5):

912. As noted above, although there are requirements for compliance units that act in an independent effective manner, (in Article 21 of the BPR Wft and Article 31c of the BGFO Wft) there are no specific requirements for a Compliance Officer, and hence, no requirements as to the independence of the head of the compliance function. However, the compliance function as a whole is required to act independently by BPR Article 21(3) and BGFO Article 31c(3). The requirement to have compliance functions does not apply to management companies, investment companies, depositories, or financial services providers. There are no provisions for a Compliance Officer in the Wgt.

Application of AML/CFT Measures to Foreign Branches and Subsidiaries (c. 22.1, 22.1.1 and 22.1.2):

913. Article 2 of the WWFT instructs entities subject to the Act to ensure that branch offices and subsidiaries in a non Member State should follow the same customer due diligence requirements and record retention requirements that are laid down in the WWFT. There is no requirement to pay particular attention to this principle where the branches and subsidiaries are in countries that do not apply or which insufficiently apply the FATF Recommendations. There is no requirement to apply the higher of the Dutch or host country standards in foreign countries. There are 20 Dutch banks which have, in total, 125 branches outside the Netherlands. Furthermore, there are eight insurance companies which have 25 branches outside the Netherlands.

914. There is no requirement to ensure that branches and subsidiaries in Member States follow the same customer due diligence and record retention obligations as are required by Dutch Law.

Requirement to Inform Home Country Supervisor if Foreign Branches and Subsidiaries are Unable to Implement AML/CFT Measures (c. 22.2):

915. Article 2 (2) of the WWFT requires the entity subject to the Act to inform the Dutch supervisory authority where it is unable to apply customer due diligence measure equivalent to Dutch standards in its branches or subsidiaries in non-Member States and to take measures to prevent money laundering and terrorist financing. There is no comparable provision for branches and subsidiaries in Member States and the requirement to apply Dutch standards applies only to CDD and not to all AML/CFT measures.

Additional Element—Consistency of CDD Measures at Group Level (c. 22.3):

916. There is no explicit provision requiring consistent CDD measures at group level. The Article 2 requirement on foreign branches and subsidiaries mean that the same measures would apply through a group whose holding company was based in The Netherlands, provided that the holding company was regulated entity in the Netherlands. However, Article 2 does not apply to branches and subsidiaries in Member States.

Analysis of effectiveness

917. The WWFT contains no provisions with respect to procedures, policies controls, compliance monitoring, internal audit, employee training (apart from the requirement to inform employees about the provisions of the Act) or employment screening.

918. Provisions on all these matters can be found in the Wft and its implementing regulations. In order to regard the Wft provisions on these matters as applicable, it is necessary, as noted above, to accept the view that the definition of integrity in Articles 3:10 and 4:11 of the Wft encompass measures to mitigate ML and TF risk. The assessors' views on this interpretation are set out above.

919. In the view of the assessors, it would be far preferable to amend the Wft to make it explicit that the obligation to have policies, procedures, and controls applies directly to the requirements placed on institutions that are created by the WWFT. This is the approach adopted in the Wgt (the law that used to apply to money transfer offices and still applies to bureaux de change). Nevertheless, for the purposes of this assessment, it is accepted that this interpretation would mean that, for the institutions described in the various relevant Articles of the Wft, BPR Wft and BGFO Wft, the Wft requirements can be regarded as applying and that they could be enforced.

920. As described in detail above, a number of the provisions in the implementing regulations only apply to selected license categories. In particular:

- There is no requirement for an investment firm, an investment company or a financial services provider (an insurance broker) to make a risk assessment of integrity risk.

- There is no requirement for an investment company, an entity for risk assessment, a financial services provider or an investment firm to inform employees of policies and procedures (the training requirement).

- There is no requirement for an entity for risk assessment, management companies, investment companies, depositories and financial services providers to have a compliance function.

- There is no requirement for an entity for risk assessment, a financial services provider, management companies, collective investment schemes, investment firm, or investment

companies to have an internal audit function (although an investment firm has to have an internal control function with similar duties).

- Of those that do have to have an internal audit function, clearing institutions, insurers, payment institutions and investment firms do not have to have an audit plan.

- Entities for risk acceptance and investment companies do not have to screen employees in sensitive positions.

921. Even on the basis of the assessors' acceptance that the provisions of the Wft apply, there remain a number of weaknesses in the regime:

- There are gaps in the application of the requirements as described above.

- The Wgt Regulation requires controls to implement the obligations in the predecessor Acts to the WWTF.

- There is no requirement for a compliance officer as such in either the Wft or the Wgt and hence no requirements relating to seniority or access to management.

- The detailed requirements in the Wft for compliance functions, relating to their access to resources and documents, their reporting requirements and other matters do not apply to insurers, clearing institutions or banks with no investment functions and there are no comparable requirements in the Wgt.

- There are no explicit requirements in the WWFT for employee training (except with respect to the provisions of the law and the ability to recognize unusual transactions and the broad and general provisions regarding the provision of information to employees and to business units are not accompanied by any guidance as to the nature of the training that should be given or the degree of knowledge that should be retained by the employees.

- There are no training requirements of any kind for staff of bureaux de change beyond those in the WWFT.

- The provisions on screening employees for high ethical standards do not apply to all employees.

- There are no provisions requiring the institutions subject to the WWFT to apply Dutch standards to branches and subsidiaries in Member States of the EU (or EEA).

- There is no requirement that institutions subject to the WWFT should pay particular attention to the principle that foreign branches and subsidiaries apply Dutch standards in countries which do not or which insufficiently apply FATF Recommendations.

- The WWFT does not require an institution subject to the Act to apply higher host country standards if they exist.

- The WWFT requirement to apply Dutch standards to foreign branches and subsidiaries applies to CDD but not to all appropriate AML/CFT measures.

922. Notwithstanding these weaknesses, the assessors established that all the regulated entities they interviewed had internal controls to implement AML/CFT. With the exception of the financial services

providers and subject to the points that follow, the interviews with regulated entities established that regulated financial entities had compliance units, with access to senior management levels and a practice of frequent reporting. They generally engaged in some employee training and screening—in most cases applying such screening to all employees with more rigorous procedures applying to more sensitive posts. They were all aware of the requirement to apply Dutch standards in foreign branches and subsidiaries (although the assessors were not in a position to judge the extent to which this requirement was effectively implemented). DNB and AFM discussed all these matters with regulated financial entities, examining procedures manuals, training materials and screening procedures.

923. However, the practice of regulated entities interviewed by the mission on these matters varied in a way not always clearly related to the size and nature of the business. It was not easy to assess, in interview, the adequacy of internal controls. Moreover, for employee training, some major institutions had minimal provisions. Although all institutions engaged in employee screening, their practices differed somewhat and none could give a clear indication of what they regarded, in their institutions, as an integrity-sensitive position (which is a term defined in the Wft).

924. With respect to the requirement in the WWFT that employees should be informed of the provisions of the WWFT, the assessors could not help noticing that most of those interviewed, who tended to include the compliance and legal personnel, were unclear themselves as to many of the specific provisions of the WWTF that applied to their institution and it seems unlikely that the level of knowledge would be substantially higher amongst the generality of employees without specific compliance responsibilities. It could well be argued that a provision to ensure that employees are informed about the provisions of the law would seem to be less useful than a requirement that employees should be given training on a regular basis about AML/CFT matters in general and the AML/CFT policies and procedures adopted by the regulated entity. This appeared to be the practice adopted by the regulated financial entities and is required by the Wft. It does not, however, meet the requirement in the WWFT, which is solely about information on the provisions of the WWFT itself.

3.8.2 Recommendations and Comments

925. The authorities are **recommended** to make the following amendments to the WWFT, Wft, and Wgt with the overall objective of ensuring that all of the relevant obligations apply to all of the relevant institutions:

- Amend the Wft to clarify that the policies, procedures and controls required by the Wft must apply to the implementation of the obligations in the WWFT.

- Amend the WWFT to include a direct requirement to train staff , on a regular basis, on policies, procedures and controls and in particular on requirements on CDD and reporting of unusual transactions, and on new developments, including information on current ML and TF techniques, methods and trends.

- Amend the final reference to the predecessor AML/CFT statutes in the Wgt Regulation, so that the requirement for internal controls applies to the WWTF.

- Amend the Wft and Wgt to create a requirement for all regulated entities to have a compliance officer with adequate seniority, access to senior management, full access to documents, adequate resources and independence and with a requirement to make regular reports to management.

- Amend the Wft or implementing regulations to require screening of all employees to ensure high standards.

- Amend the Wft or implementing obligations to apply the ongoing obligations on internal controls, compliance units, internal audit, training, and employee screening to all regulated financial entities covered by the WWFT.

- Consider the publication of guidance on what might be expected with regard to training, employee screening and other matters relating to compliance units and internal controls without diluting the primary responsibility of regulated financial entities to determine the precise level of training to be provided.

- Amend Article 2 (1) of the WWFT (or provide in implementing regulations) to ensure that regulated entities with foreign branches and subsidiaries should apply all AML/CFT measures (not just CDD) that are equivalent to Dutch standards or applying local standards where these are higher.

- Amend Article 2 of the WWFT to apply its provisions to EU and EEA Member States.

- Amend the WWFT to create a requirement that regulated entities should pay particular attention to the principle that foreign branches and subsidiaries apply Dutch standards in countries which do not or which insufficiently apply FATF Recommendations.

3.8.3 Compliance with Recommendations 15 & 22

	Rating	Summary of factors underlying rating
R.15	**PC**	• The internal control requirements are mostly to be found in the Wft rather than the WWFT. The coverage of the Wft is not the same as that of the WWFT and some of the requirements in the Wft (including the requirements for internal controls, internal audit and compliance functions) do not apply to certain categories of regulated financial entity as described above. • There is no requirement relating to the seniority or access to managers of the head of the compliance function. • The detailed requirements in the Wft for compliance functions, relating to their access to resources and documents, their reporting requirements and other matters do not apply to banks with no investment functions and there are no comparable requirements in the Wgt. • The requirements for employee training on AML/CFT in the WWFT are limited to the obligation that employees be instructed in the provisions of the WWFT and trained to recognize unusual transactions. The broad and general provisions in the Wft regarding the provision of information to employees and to business units are not accompanied by any guidance that makes it clear that training should cover internal policies, procedures and controls, new developments and current ML and TF techniques, methods and trends, as well as all aspects of AML/CFT laws and obligations, including, in particular requirements on CDD and reporting.
R.22	**PC**	• There are no provisions requiring the institutions subject to the WWFT to apply Dutch standards to branches and subsidiaries in Member States of the EU (or EEA). • The requirement to apply Dutch standards applies only to CDD and not to all appropriate AML/CFT measures. • There is no requirement that institutions subject to the Act should pay particular attention to the principle that foreign branches and subsidiaries apply Dutch standards in countries which do not or which insufficiently apply FATF Recommendations. • The WWFT does not require an institution subject to the Act to apply higher host country standards if they exist.

3.9 Shell Banks (R.18)

3.9.1 Description and Analysis

Legal Framework:

926. The relevant provisions are in Articles 2:11 to 2:23 and 3:5 of the Wft and Articles 5(3) of the WWFT, together with implementing regulations.

Prohibition of Establishment of Shell Banks (c. 18.1):

927. Neither the WWFT, nor the Wft directly prohibit shell banks but the effect of the criteria for licensing is to prevent a shell bank from obtaining authorization (unless, of course, it ceased to be a shell bank). Since a shell bank without licence would be operating illegally, the provisions have the effect of making it illegal to establish and operate a shell bank.

928. Article 2 of the Wft does not allow any party with a registered office in the Netherlands to conduct the business of a bank without a license granted by the DNB. Article 3:5 prohibits any person from taking deposits from the public beyond a restricted circle without authorization from the DNB.

929. Where the applicant for a license is registered in the Netherlands, Article 3:15 of the Wft states that there must be at least two natural persons, who determine the day to day policy of the credit institution and who must be physically present in the Netherlands. Moreover, Article 3:16 states that the credit institution must not be affiliated to persons in a formal or actual control structure that is so lacking in transparency that it constitutes or may constitute an impediment to the adequate exercise of supervision of that financial enterprise. For banks that are licensed in other Member States, although there is no separate requirement for a license in the Netherlands (in line with single market requirements) the prohibition on shell banks in the Third Money Laundering Directive would apply.

930. Where the applicant for a license is registered in another Member State, where it does not require a license, Article 2:16 of the Wft states that a credit institution that does not have a license in that Member State must obtain a license from the DNB before it conducts a business from a branch office. In that case, the DNB can only give a license if Article 3:15 is satisfied, namely, that there should be at least two persons, physically present in The Netherlands who are responsible for day to day policy.

931. Where a person has a registered office in another Member State, does not require a license from the supervisory authority in that Member State and there is no branch office in the Netherlands, Article 2:16 states that the DNB may permit the provision of services in the Netherlands, provided that the DNB is notified of the operation of the credit institution and that the credit institution complies with the solvency provisions in Article 3:57 of the Wft. Such a person would be subject to the application of the Third Money Laundering Directive which prohibits shell banks

932. Where the applicant for a license is registered in a non Member State, Article 2:21 of the Wft states that the applicant will only get a license to operate from a branch office if Article 3:21 applies. Article 3:21 requires that the day to day policy of the credit institution should be determined by at least two natural persons physically present in The Netherlands.

933. Moreover, under Article 27 of the BPR Wft, a bank (like other financial undertakings covered by the Article) may not outsource its activities if such outsourcing were so to compromise transparency as to impede effective supervision.

Prohibition of Correspondent Banking with Shell Banks (c. 18.2):

934. Article 5 (3) of the WWFT forbids a Dutch bank from establishing or continuing a correspondent bank relationship with a shell bank. The term "shell bank" is defined in accordance with the glossary to the FATF Recommendations.

Requirement to Satisfy Respondent Financial Institutions Prohibition of Use of Accounts by Shell Banks (c. 18.3):

935. Article 5 (3) of the WWFT forbids any correspondent banking relationship with a bank that is known to allow a shell bank to use its accounts. Article 8 (3) (a) requires a bank to gather sufficient information about a correspondent bank outside the EU to obtain a complete picture of the nature of the business operations. This should ensure that a bank establishes if the correspondent bank allowed its accounts to be used by shell banks. There is no such requirement in relation to EU banks. The Third Money Laundering Directive requires Member States to prohibit banks from providing facilities to shell banks. Strictly speaking, the Directive does not absolve the authorities in the Netherlands from requiring its institutions to conduct sufficient due diligence about an EU bank to ensure that it abides by the EU requirement.

936. Articles 26–29 of the WWFT includes penalties for breaches of its provisions relating to shell banks.

Analysis of effectiveness

937. The Wft clearly prevents any shell bank that is incorporated within The Netherlands from obtaining a license. The DNB has a special unit to prevent unlicensed banking activity. However, its resources are primarily devoted to detecting unlicensed trust and company services providers or money transfer offices and it has not, in practice, discovered any shell banks operating in The Netherlands.

3.9.2 Recommendations and Comments

938. The absence of any requirement to determine whether EU correspondent banks may have accounts with shell banks leaves a potential gap in the framework, although, in practice, this is unlikely to create a major risk. Nevertheless, the authorities are recommended to amend Article 8 (3) of the WWFT so that it applies to all correspondent banks.

3.9.3 Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	**C**	• This Recommendation is fully observed.

Regulation, supervision, guidance, monitoring and sanctions

3.10 The Supervisory and Oversight System—Competent Authorities and SROs. Role, Functions, Duties, and Powers (Including Sanctions) (R. 23, 29, 17, 25, & 30)

3.10.1 Description and Analysis

Legal Framework:

939. The powers of the supervisory authorities to monitor and supervise financial entities' obligations with the WWFT are set out in Article 24 of the WWFT.

940. In addition, as noted in the context of Recommendation 15 (internal controls), the Wft imposes obligations on most financial entities to have measures in place to prevent transgression of any law. (Articles 3:10 and 4:15). If it is accepted that these Articles mean that the Wft requirements for internal controls, compliance, audit, and training apply to AML/CFT measures, it also follows that the supervisory powers and sanctions in the Wft can be used to supervise and monitor compliance with AML/CFT obligations. This is important because, although there are supervisory powers in the WWTF, the ability to impose sanctions (including license revocation) are stronger in the Wft. The Wgt requires has explicit provisions that bureaux de change to have internal controls to implement AML/CFT obligations. As noted in the context of Recommendation 15, the assessors accept that Wft supervisory powers and sanctions can be used in respect of AML/CFT obligations but consider that the position is open to challenge for the reasons given in the observations of Recommendation 15, where precisely the same legal nexus applies.

Competent authorities—powers and resources: *The competent authorities and SROs, and their roles, functions and duties in regulating the application of AML/CFT measures in the financial system, their organizational structures and resources (R.23, R.30 - in particular criteria 23.1, 23.2, 30.1-30.3).*

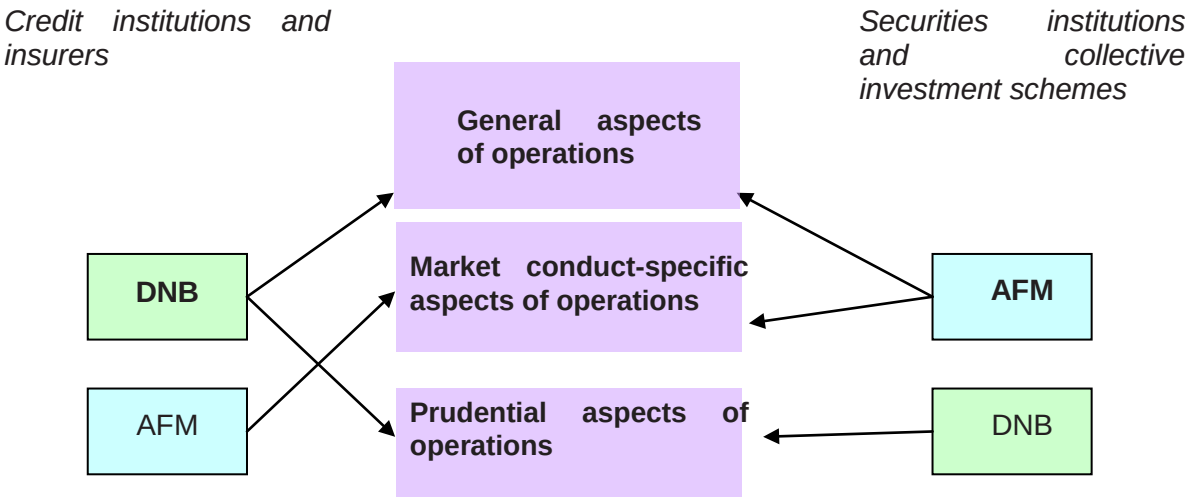
The roles, functions and duties of the supervisory authorities (c 23.1)

941. The Netherlands financial system is dominated by a few very large financial—internationally oriented—conglomerates offering a wide range of financial products and services, with centralized risk management functions. The Netherlands financial services regulatory system is structured according to the "Twin Peaks" model. According to this model, one supervisory agency, the DNB, focuses on the prudential objective of promoting the soundness of financial institutions, whereas the conduct of business objective of enhancing orderly and fair market practices is performed by the AFM. Integrity supervision (which also contains AML/CFT supervision) is performed by both.

942. The key institutional features of the Twin Peaks model are:

- The consolidation of all macro- and micro-prudential supervision into a single body within DNB.
- The consolidation of all conduct-of-business supervision within the AFM.
- The establishment of a 'covenant' between the two supervisors to ensure good coordination and cooperation.

The Twin Peaks model is demonstrated in the following diagram:



943. This approach results in most financial firms being supervised by both DNB and AFM. The covenant referred to above was set up to avoid overlap and reduce regulatory burdens. It was agreed in 2002, and updated in 2004 and 2007. This covenant sets out a basic framework for cooperation among the two supervisors, including:

- Designation of a lead ("authorizing") agency with overall responsibility for supervision (including licensing) of each financial institution and coordination of supervisory activities. DNB is the lead agency for institutions mainly in the banking, insurance, and pensions sectors, while AFM leads for securities firms.
- Agreement that the lead supervisor would defer to the judgment of the other supervisors in their areas of responsibility.
- Agreement on which aspects of a firm's management come under prudential supervision, and which come under conduct-of-business supervision.
- Rules for consultation and sharing of information between the supervisors.
- Provision for annual review of the Covenant and adjustments as needed.

944. As noted above, in the assessment on internal controls (Recommendation 15), the definition of "integrity supervision" in the WFT and in the underlying regulations (BPR Wft and BGFO Wft) is deemed to encompass obligations designed to prevent ML and TF. Integrity supervision is carried out by both DNB and AFM as part of their ongoing supervisory efforts through regular contacts with the supervised institutions. Each authority takes responsibility for monitoring compliance with AML/CFT provisions of different institutions as outlined in the table below.

Designation of Competent Authority (c. 23.2):

945. Article 24 (1) of the WWFT gives the Minister of Finance and the Minister of Justice the power to designate the supervisory authorities for financial activities defined in the WWFT. This delegation is undertaken in the implementing decree BATWWFT and is detailed in the table below. The supervision of all financial institutions is delegated to either the DNB or the AFM.

FATF description of type of business	Definition in Dutch Law	Supervisor	Reference
Acceptance of deposits and other repayable funds from the public	Credit institution (defined in Wft as a bank or electronic money institution)	DNB	BATWWFT Article 1(a); EC 2006/48
Lending	Credit institution	DNB	See above
Financial leasing	Credit Institution Financial institution	DNB	BATWWFT Article 1 (a) gives supervisory responsibility to DNB for services defined in WWFT Article 1(1)(a)(2), which refers to Article 1:1 Wft, which refers to paragraphs 2-12 of Annex 1 of EC/2006/48, Paragraph 3 of which is financial leasing
The transfer of money or value.	Credit Institution Financial institution Payment institution	DNB	See above: paragraph 4 of Annex 1 of EC/2006/48 is money transfer
Issuing and managing means of payment (*e.g.*, credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).	Credit Institution Financial institution	DNB	See above: paragraph 5 of Annex 1 of EC 2006/48 is issuing and managing means of payment
Financial guarantees and commitments.	Credit Institution Financial institution	DNB	See above: paragraph 6 of EC 2006/48 is guarantees and commitments
Trading in: (a) money market instruments (cheques, bills, CDs, derivatives, etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading.	Credit institution Financial institution	DNB	See above: paragraph 7 of Annex 1 of EC 2006/48 covers all these items except commodity futures.
Participation in securities issues and the provision of financial services related to such issues.	Investment firm	AFM	BATWWFT Article 1(b) gives AFM supervisory responsibility for services in WWFT Article 1(1)(a)(6) investment firms, which are referred to in Wft Article. Although not stated explicitly, investment firms are assumed to be those who give investment services, which includes underwriting advice and other services in relation to securities
Individual and collective portfolio management.	Investment firm Collective investment scheme Management Company Investment company	DNB	BATWWFT Article 1 gives AFM responsibility for services in Article 1(1)(a)(6) WWFT, investment firm. Reference is made to Article 1:1 Wft, which defines investment firm as a firm that provides investment services or investment activity. Investment activity is not defined but investment services include management of individual capital (this is assumed to be portfolio management since investment services and activities are defined in MiFiD EC/2004/39 to include portfolio management) BATWWFT Article 1 gives AFM responsibility for institutions concerned with Article 1(1)(a)(7) WWFT, collective investment scheme. WWFT Article 1 refers to Wft Article 1:1 which defines

FATF description of type of business	Definition in Dutch Law	Supervisor	Reference
			collective investment scheme as an investment company or unit trust. This must be collective portfolio management
Safekeeping and administration of cash or liquid securities on behalf of other persons.	Credit institution Financial institution	AFM	BATWWFT Article 1 (a) gives supervisory responsibility to DNB for services defined in WWFT Article 1(1)(a)(2), which refers to Article 1:1 Wft, which refers to paragraphs 2-12 of Annex 1 of EC/2006/48, Paragraph 12 of which is safe keeping of securities This would appear to be the responsibility of DNB However, "ancillary service" as defined in Article 1:1 of Wft includes "custody and management of financial instruments, including cash and securities custody." An investment firm is not defined to include the provision of ancillary services. Nevertheless, the authorities have stated that the AFM is the lead supervisor for this activity.
Otherwise investing, administering or managing funds or money on behalf of other persons.	Investment firm Investment company Management company Collective investment scheme	AFM	BATWWFT Article 1 gives AFM responsibility for services in Article 1(1)(a)(6) WWFT, investment firm. Reference is made to Article 1:1 Wft, which defines investment firm as a firm that provides investment services or investment activity. Investment activity is not defined but investment services include management of individual capital (this is assumed to be portfolio management since investment services and activities are defined in MiFiD EC/2004/39 to include portfolio management)
Underwriting and placement of life insurance and other investment related insurance.	Life insurer	DNB	BATWWFT Article 1(a) gives DNB responsibility for services defined in WWFT Article 1(1)(a)(5), life insurer which is defined in Article 1:1 of Wft and services defined in WWFT Article i(1)(a)(8) life insurance broker
Money and currency changing.	Payment institution Exchange office	DNB	BATWWFT Article 1 refers to Article 1(1)(a) 4 of Wft, money transfer office

Organization and resources—Supervisory Authorities (R.30 - in particular criteria 30.1-30.3):

946. The DNB and AFM are both independent from the Ministry of Finance in their daily operations. On a generic level, the Ministry determines the policy directions for AML/CFT (in cooperation with the Ministry of Justice). The assessors considered that the authorities were not subject to undue influence or interference from government, financial services industry or any other person.

947. The structure the DNB adopts for supervision is as follows:

- The Expert Centre for Integrity (ECI; 13 staff) deals specifically with supporting and advising the supervisory teams by acting as a centre of expertise concerning integrity issues and by taking part in examinations on integrity, interpreted to include AML/CFT compliance.

- Prudential supervisory teams (approximately 200 staff divided over 6 banking teams, 1 financial conglomerate team and 2 insurance teams) deal with AML/CFT supervision in their overall supervisory tasks. There are 58 Dutch banks (including conglomerates) and 45 foreign owned banks, with a total of EUR2.6 billion. 4 banks account for 80 percent of the assets. There are 60 life insurers and 213 non life insurers. Insurance companies account for EUR 0.37 billion. Each team has an appointed expert on compliance and integrity issues regarding their supervised institutions. AML/CFT issues are discussed in bimonthly meetings (consisting of all compliance and integrity experts of these teams and staff from the Expert Centre).

- A supervisory team deals specifically with integrity supervision of casinos, bureaux de change, payment services providers (money transfer offices) and trust and company service providers (12 staff in total, of which 5 full time equivalents deal with money transfer offices and bureau de change. There are 28 money transfer offices and bureaus de change.

- An Expert Centre for testing fitness and properness and maintaining a Register (ECTI; 7 staff).deals specifically with the fit and proper testing of members of the (supervisory) board of financial institutions.

- An Expert Centre for Enforcement (14 staff) deals with illegal financial institutions (institutions acting without a permit/registration from DNB); about 5 staff (full time equivalent) deal with AML/CFT issues.

- The Supervisory Policy Department, Accountancy, Organization and Integrity division (about 3 of the 15 staff deal with over all policy issues regarding integrity (including AML/CFT).

948. The AFM implements its objectives in the following task areas:

Task area 1: Financial services and products

949. The AFM has two expert teams for market entry, one for the financial service providers and one for the investment fund and investment institutions. They are equipped to deal with fit and proper testing. These teams are staffed with 20 employees.

950. Three expert teams deal with ongoing supervision. These three financial company supervisions groups are staffed with 120 supervisors and can be divided in two parts.

- One supervision group deals with analyzing signals and supervising financial service providers and investment firms and investment institutions which have no need for increased supervision. These account for most of the 14 000 entities within the responsibility of the AFM.

- The other two teams deal with ongoing supervision of financial institutions and service providers that on the one hand are placed under increased supervision, because of signals or patterns in their business operations that points at improper activities or at least appear to be improper, or, on the other hand, are included among the nine largest financial institutions, for which there is contact on a regular basis. Up to 50 entities are covered by each of these teams.

951. All the ongoing supervision teams can deal with AML/CFT supervision in their overall supervisory tasks. When a visit or another form of contact lead to signals that for instance that the business operation is not properly controlled, the supervisors can investigate this and thereby also control the compliance with the AML/CFT obligations.

Task area 2: Capital market and infrastructure

952. The AFM supervises the institutions that participate in regulated securities markets, focusing on transparency, compliance with listing requirements and continuing obligations and threats to market integrity. The AFM also supervises the conduct of, and the information supply from, all parties operating in the financial markets in the Netherlands; that is, the savings, loans, investment, and insurance markets. The term "financial infrastructure" in the title of this task area refers to the whole process that comprises securities trading, clearing, and settlement.

Task area 3: Integrity

953. The AFM monitors the compliance with the integrity provisions in the Wft, which includes unauthorized activity and ML/TF. There is one expert team dealing with these issues which is staffed with 25 employers. The integrity unit operates on the basis of signals from various sources, which prompt further investigation. These signals come from supervision (50 percent), consumer complaints (31 percent) financial institutions (12 percent) and 5 percent from law enforcement.

954. The supervisory authorities receive their funding regarding their AML/CFT supervisory tasks from the Government. They consider that their funding and resources are adequate. They are able to obtain the skilled staff they need and conduct a program of on-site and off-site inspection that fulfils their responsibilities.

955. Both DNB and AFM consider that their staff have appropriate skills and receive sufficient training. The details of the training provision are set out below.

956. DNB supervising officers who are members of the inspection teams specialized in integrity issues (including AML/CFT) have a program of training that includes ACAMS, AML/CFT conferences and workshops. In addition, all new examining officers have to follow an introductory course which includes AML/CFT supervision. Staff working on integrity supervision have university level education in law, economics, and/or accountancy. Staff members more generally have followed on or more of the following training courses:

- FATF evaluators training (8 staff received training in the 4 years prior to the mission).
- Participation in FATF, CFATF or MONEYVAL mutual evaluation(s) and/or typology exercises (5 mutual evaluations between 2005–2010).
- ACAMS AML/CFT training sessions (5 staff received training in the 2 years prior to the mission).
- Office of the Comptroller of the Currency (OCC) AML/CFT training in Washington DC (1-2 staff per year).
- Central Banking events; world forum for central bankers and financial supervisors training courses on AML/CFT current issues (2 per year).

- Regular conferences and workshops on AML/CFT, organized by private organizations (12 in 2010 and 10 in 2009).
- On the job training within the Bank by employees and external speakers (all officers).
- University Post Graduate Compliance and Integrity management (3 in 2009 and 2 in 2008).
- Netherlands Compliance Institute training (1-2 per year).

957. The AFM spends EUR1 million annually on training. Staff working in supervisory teams or supervisory supporting teams all have university level education in law, economics, public administration, physics, history, econometrics, political science, etc. All staff working in supervisory (supporting) divisions is obliged to receive training on integrity matters as part of their ongoing training program. Staff members also attend workshops and conferences such as ACAMS. The AFM encourages the exchange of staff with other organizations. On a regular basis there are work placements with the FEC and the FIOD-ECD. The AFM were not able to provide data on the extent to which staff received specialized training on AML/CFT matters.

958. Overall, the structure of the authorities and the resources devoted to supervision appear to be adequate. The assessors found no evidence to challenge this judgment and, on the basis of interviews with market participants about the extent of their interaction with the supervisory authorities, would share the assessment of the authorities. The general level of skills is appropriate for the supervision of AML/CFT compliance and it is appropriate that all staff should receive some training on AML/CFT matters. However, the description of the training program consists of a list of training opportunities, almost all of which are taken up by no more than one or two of the 200–250 relevant staff each year. There is no indication of more regular (for example annual) training on AML/CFT as being a matter of routine for relevant staff after the introductory course for examining officers. In the absence of further data on the extent of AML/CFT training, the assessors were not able to judge that the training was adequate.

959. The authorities seek to maintain standards of integrity of supervisory staff, initially by conducting screening of staff. Every candidate for a new position in the DNB is checked against the public prosecution database and for certain functions, references from former employees are obtained and a declaration of financial circumstances is required. The AFM also screens new employees against the public prosecutor database and checks references of former employees (as well as checking the candidates integrity self assessment with the last employer). Both authorities also state that integrity is a core value and that this quality is a key part of the regular training and assessment process. The Wft imposes a duty of confidentiality on any person performing duties under the Act and this applies to supervisory staff (Article 1:89). These provisions are sufficient to meet the criteria.

Power for Supervisors to Monitor AML/CFT Requirement (c. 29.1 Authority to conduct AML/CFT Inspections by Supervisors (c. 29.2); Power for Supervisors to Compel Production of Records (c. 29.3 and 29.3.1):

960. Chapter 4 of the WWFT provides for the supervision and enforcement of AML/CFT obligations. As noted above, it gives the Ministers of Finance and Justice the power to nominate the supervision authorities. Article 24 of the WWFT also states that the authorities may adopt a risk based approach to supervision and enforcement and it applies the provisions of Chapter 5.2 of the Awb to the AFM and DNB for the purposes of exercising their supervision and enforcement powers. Chapter 5.2 of the Awb provides, inter alia, the following powers:

- An inspector, who can be nominated by the supervisory authority and must carry appropriate identification and documentation is responsible for monitoring compliance with statutory rules and may exercise powers to the extent reasonably necessary for the performance of his or her duties.

- The inspector may enter any place with the exception of a dwelling without the occupant's consent, taking with him the necessary equipment, if necessary with the assistance of the police.

- An inspector is empowered to demand information, to see a person's identity card to inspect business information and documents, to make copies of the information and documents or, if it is impossible to make copies on-site, he may take the information and documents away for a short time for this purpose, giving a written receipt for them.

961. Moreover, under Article 5:20 of the Awb:

- Any person shall give an inspector all such assistance as he may reasonably demand in the exercise of his powers within a reasonable time limit set by him.

- Persons who are bound to secrecy by virtue of their office or profession or by law, may refuse to cooperate if this follows from their duty of secrecy. The DNB and AFM confirm that this does not inhibit their ability to obtain information from regulated financial entities.

962. These powers can be used by the DNB and AFM to compel the production of documents without a court order. They are sufficient to obtain all relevant documents, records and other information relating to accounts, other business relationships, transactions and the internal policies of the institution.

963. In addition to the monitoring and supervision powers provided by the WWTF, the authorities consider that they are able to use the supervisory powers given in the Wft. This point is discussed in more detail above in the section on the legal framework and the assessors accept that, although the legal position could be open to challenge, it is reasonable to interpret the provisions as allowing the supervisory bodies the ability to use the powers in the Wft to monitor the implementation of AML/CFT measures.

964. The DNB and AFM exercise these powers to conduct programs of on-site and off-site inspections in practice. As noted above, the inspection teams have dedicated staff with expertise in different areas (including AML/CFT) and these are supported by specialist teams with expertise in integrity issues. The use of these powers is discussed in more detail below in the assessment of ongoing supervision.

965. Notwithstanding the assessors' views on the use of Wft powers to monitor and enforce AML/CFT obligations (which are discussed in the context of Recommendation 15), the mission concluded that the supervisory authorities assert their powers to obtain information, to conduct inspections, and to review policies and procedures.

Sanctions: Powers of Enforcement & Sanction (c. 29.4); Availability of Effective, Proportionate & Dissuasive Sanctions (c. 17.1); Designation of Authority to Impose Sanctions (c. 17.2); Ability to Sanction Directors and Senior Management of Financial Institutions (c. 17.3): Range of Sanctions—Scope and Proportionality (c. 17.4)

Powers of Enforcement & Sanction (c. 29.4) Availability of Effective, Proportionate & Dissuasive Sanctions (c. 17.1); Range of Sanctions—Scope and Proportionality (c. 17.4):

966. There are both criminal and administrative sanctions available to the authorities for breaches by institutions and their senior management of the AML/CFT obligations. The sanctions apply to both natural and legal persons.

967. A breach of the WWFT is punishable by law as a criminal offence with a maximum of 2 years imprisonment (for natural persons) and a fine (for both natural and legal persons), or both (Article 9, paragraph 3, of the Dutch Penal Code–WvSr).

968. Article 27 of the WWFt provides for administrative penalties which can be imposed by the DNB and AFM for specific breaches of the WWFT, including all of the AML/CFT obligations. Penalties may apply to both natural and legal persons.

969. In addition, the DNB and AFM have powers to impose administrative sanctions on natural and legal persons under the Wft. These sanctions can be applied in respect of breaches of the law or regulation. Whilst the administrative penalties can be exercised in respect of breaches of specified regulations (which, in practice encompass all the regulations relevant to ML and TF), the sanctions involving the withdrawal of or placing a condition on a license can be applied in respect of any breach of any rule. The ability of the authorities to place a Wft sanction on a regulated financial entity for failing to abide by WWFT obligation rests on the interpretation of the provisions on integrity in the Wft that are discussed in more detail in the "legal framework" section above. The assessors accept that the provisions of the Wft can be used to impose requirements for controls to implement WWFT measures and that therefore weaknesses in such controls could result in sanctions. However, the mission does not regard this method of applying the Wft provisions as robust. As noted above, the AFM has informed the mission that it felt itself unable in a particular instance to impose a regulatory sanction (the withdrawal of a license) for a failure to conduct CDD, because there is no direct provision justifying the use of the penalty in Article 1:104 of the Wft for breaches of laws other than the Wft itself. In practice, penalties, such as fines or license withdrawals are rarely imposed by the supervisory authorities for AML/CFT matters and so the question of the use of sanctions has not been tested.

970. The administrative enforcement powers in the Wft consist primarily of the following:

- Issuing a direction/instruction (Article 1:75 Wft), failure to abide by which can result in the appointment of an administrator under Article 1:76.
- Imposing an incremental penalty payment (Article 1:79 of the Wft, Article 27 of the WWFT and Articles 5.32–5.35 of the Awb).
- Imposing an administrative fine, which can be announced publicly (Article 1:80 of the Wft and Articles 5.32–5.35 of the Awb).
- Issuing an announcement that an offense or issuing a public warning (Article 1:95 of the Wft).
- Amending, revoking—wholly or partially—or restricting a license or a registration (Article 1:104 of the Wft).
- Appointing an administrator (Article 1:76 Wft).

971. Administrative fines can be imposed up to a maximum of EUR4 million or EUR8 million in the event of previous offenses. There is also scope for requiring financial institutions to pay an amount up to twice the financial gains from a violation. For most institutions, these fines would be dissuasive and would, if imposed, have the potential to be proportionate and effective. However, for the major financial businesses, these maximum limits could limit the effectiveness of such penalties.

972. When imposing an administrative fine the supervisors can sanction either the financial institution or the individual responsible for the transgression in very much the same way as in the criminal law system (Article 5.0.1. Awb). It is also possible to impose a penalty on an individual lower in the hierarchy where the violation can be directly attributed to the decisions or acts carried out by this person.

973. The supervisors also point out that regulatory measures can be (and in the vast majority of cases, are) enforced without resort to sanctions. Reports of inspection visits carry recommendations relating to AML/CFT and these are accepted and implemented by the institutions. In most cases, this method is effective in correcting weaknesses in the arrangements in institutions.

974. DNB has noted that in respect of measures to mitigate integrity risk by banks and insurers in the 5 years to 2010, there were the following enforcement actions:

- 3 written warnings.
- 31 oral or written orders to comply with DNB instructions.
- 10 orders to provide regular reports on measures taken.
- 2 cease and desist orders.
- 2 administrative fines (with 2 currently under consideration).

975. For money transfer offices, the record on sanctions given the DNB is shown in the table below.

Type of sanction	2005	2006	2007	2008	2009
Cease and desist order			1	1	
Administrative fine		1		2	1
Direction/Instruction	1	5	8	3	3
Cancellation registration	4		1		
Reporting public prosecution	2	1			
Total	**7**	**7**	**10**	**6**	**4**

976. Although AFM have taken enforcement action against many institutions, their approach is to conduct investigations into multiple offences and focus on taking enforcement action in respect of the offences where the evidence is strongest and the penalties harshest. Although tough penalties are available for breaches of internal controls and other AML/CFT related matters, the AFM have, in practice, rarely taken enforcement action on AML/CFT matters. Following the assessors' on-site visit, the AFM provided additional information on 5 cases where it had taken enforcement action. In 2 cases, the AFM gave written warnings for failure to conduct adequate client identification and in a third, a financial services provider convicted of a money laundering offence after a police investigation was removed from office on integrity grounds. In the two other cases, the AFM discovered a number of violations of the Wft, as well as weaknesses in client identification and took enforcement action in respect of the violations as a whole.

977. As noted above, the AFM expressed the view that it would be unsafe to use the sanctions powers in the Wft (such as the power to withdraw a license) for breaches of the WWFT and this is reinforced by the further material provided to the assessors. It is not therefore possible to conclude that the enforcement measures are, in practice, used effectively in the enforcement of WWTF obligations.

978. The range of sanctions appears to be sufficient and could be effective, proportionate and dissuasive (with the caveat noted above in respect of major institutions). The data supplied by the authorities and described above demonstrates that punitive sanctions are rarely used for AML/CFT breaches other than with money transfer offices and it is not therefore possible to make a judgment on the effectiveness of their use.

Ability to Sanction Directors and Senior Management of Financial Institutions (c. 17.3):

979. Criminal charges can be filed against both the legal person and the persons that commissioned the criminal act and the persons who were the leaders of the act (Article 51 of the WvSr). This would include Directors and senior management. Legal persons can only be given a fine as a criminal sanction.

980. The supervisory authorities may also give an instruction to any regulated financial enterprise under Article 1:75 of the Wft where there is a breach of the Wft and this could include an instruction to dismiss a director or senior manager with responsibility for the breach. This would apply to breaches of the WWFT on the basis that a regulated financial enterprise is required to have systems and controls in place to prevent breaches of any act, so a breach of the WWFT.

Designation of Authority to Impose Sanctions (c. 17.2):

981. For criminal sanctions, the responsible authority is the public prosecutor. The public prosecutor decides whether or not a case can be brought and whether a settlement can be reached. Final decisions are made by the courts.

982. Article 27 of the WWFT gives the power to the Minister of Finance to impose administrative sanctions. However, this has been delegated by administrative decree to the DNB and AFM. The Wft gives the power to impose sanctions directly to the DNB and AFM, for example in Article 1:104 of the Wft on license conditions and withdrawals and 1:79 and 1:80 on administrative penalties.

Market entry: *Fit and Proper Criteria and Prevention of Criminals from Controlling Institutions (c. 23.3 & 23.3.1); Licensing or Registration of Value Transfer/Exchange Services (c. 23.5); Licensing of other Financial Institutions (c. 23.7):*

Fit and Proper Criteria and Prevention of Criminals from Controlling Institutions (c. 23.3 & 23.3.1):

983. The Wft provides that no person may undertake financial services business without a license from one of the supervisory institutions. For example, Article 3.5 prohibits any person from accepting deposits without a license from the DNB. Article 2.96 prevents a person from conducting investment activities without a license from the AFM. Article 2.11 prevents any person from establishing a bank or electronic money institutions with a registered office in the Netherlands without authorization. There are provisions relating to other financial services providers with special provisions for institutions based in another Member State of the EU.

984. In each case, (except where there is a "passport"[92] provision for an institution already approved by another Member State) the licensing criteria for credit institutions, clearing institutions, entities for risk assessment, payment institutions and insurers include fitness and properness tests as prescribed in Articles 3.8 and 3.9 of the Wft. These tests apply to those responsible for the day to day policy of the institution which includes the directors and supervisory boards. The tests require the necessary expertise and integrity. Article 3.99 Wft also applies a fitness and properness test to those who may acquire qualifying holdings that could determine or codetermine the policy of the enterprise concerned. Similar criteria are set out for investment companies, management companies, investment firms, depositories and investment services providers in Articles 4.9 and 4.10. of the Wft. Article 3.95 prevents any person from obtaining a qualifying holding (defined as ten percent of the capital or voting rights in Article 1.1) in a bank, management company, investment firm, entity for risk acceptance or an insurer without a declaration of no objection from the DNB or AFM as appropriate to the kind of institution.

985. The fitness and properness provisions do not apply to collective investment funds (except where the latter is in the form of an investment company).

986. In addition to the requirements for integrity in the Wft, Articles 5 to 9 of the BPR Wft lay down specific criteria for fitness and properness of the senior management of a clearing institution, entity for risk acceptance, credit institution, payment institution or insurer. Articles 12 to 16 of the BGFO Wft make similar provisions for the senior management of a management company, investment company, investment firm, depository or financial service provider. These provisions include the criminal antecedents of a person and, in particular, various specified crimes of dishonesty. There are no specific requirements relating to expertise in the BPR of BGFO, but the requirement for appropriate expertise is established in the Wft (as noted above) and this is assessed, in respect of directors and senior management on a case by case basis by the authorities.

987. In respect of bureau de change, the Wgt gives the DNB the power to refuse registration if it has sufficient doubts about the integrity or management expertise of directors, those who determine day to day policy, those who appoint the directors and day to day policy controllers and those who have a qualifying holding. The criteria for refusal of registration include an assessment that the integrity of the financial system may be at risk or the management is not capable of ensuring the proper conduct of the business. These tests amount to requirements for expertise and integrity. There is no requirement for prior approval for any of these posts specified, but the bureau is obliged to notify the DNB of any changes. Following this notification, Article 2 gives the DNB the power to veto an appointment if it does so within six weeks after receiving the notification.

988. These provisions give the supervisory authorities most of the powers necessary to prevent criminals from exercising day to day policy control over most regulated financial entities and all those covered by the Core Principles.

989. The AFM gave the assessors an overview of the assessment of fitness and properness of regulated entities. The following sources would be checked in respect of individuals:

- The public prosecutor–to establish if there were any convictions or investigations.
- Tax authorities.
- Insolvency and bankruptcy records.

92 The passport refers to the ability of a financial services business in the EU to operate in any Member State without a license other than that issued by the regulator in its home country.

- The Dutch Securities Institute (which provides certification for certain qualifications).
- Professional organizations such as the accountants' institute.
- Employer references.
- Professional qualifications.
- The DNB and AFM itself.

990. For the applicant firms themselves, the AFM would check the equity (the DNB would be responsible for checking adherence to prudential standards).

991. Following the granting of a license, the entity would be subject to a "nursery visit" after three months in operation.

992. The procedure outlined by the AFM follows the provisions of Article 12-16 of the BGFO Wft. The DNB follows a similar process according to the comparable Articles of the BPR Wft checking the same sources as the AFM with respect to individuals.

993. Neither the Wft, nor the regulations make any explicit reference to the need to establish the source of wealth and funds of the license applicants themselves or the qualifying holders, although the BPRWft (Article 138) requires an examination of the financial position and legal group structure of a qualifying holder to be examined. However the authorities have demonstrated that they examine the capital structure and the ownership of the capital of institutions when an institution applies for a licence and when there is a change in qualifying owner. The assessors are satisfied that this approach, together with the other fitness and properness tests described above, meets the standard required by criterion 23.3.

Licensing or Registration of Value Transfer/Exchange Services (c. 23.5):

994. Article 2:3a of the Wft prohibits any person from operating as a payment institution without being registered. The fitness and properness criteria in the Articles 3.8 and 3.9 of the Wft are applied to money transfer offices at the time of authorization. This would result in the application of Articles 5 to 9 of the BPR Wft. However, there is no comparable restriction on those with qualifying holdings.

995. Under the Payment Services Directive, those providing payment services are able to provide payment services in any Member State on the basis of a registration in another Member State. Most money transfers activity in The Netherlands is undertaken by agents of Western Union (legally based in Ireland) and Moneygram (legally based in the United Kingdom). For such agents, there is no separate licensing requirement in The Netherlands, as the agents are simply notified to the authorities with no powers to apply fit and proper tests. This is a new development and the DNB will be monitoring its effect. It is part of the EU financial services single market. It continues to meet the requirement that there should be licensing or registration of value transfer businesses.

996. For exchange services, the provisions of the Wgt apply. Article 3 of the Wgt prohibits any activity as a bureau de change unless the operator is registered. Article 2 of the Wgt lays down conditions for registration which include the integrity of the senior managers and qualifying holders (owners of five percent or more), financial requirements and other matters.

Licensing of other Financial Institutions (c. 23.7):

997. Financial activities that are not covered by the Core Principles are, for the most part, conducted by businesses that are defined as "financial institutions" in the Wft. There are no entities operating within this category in The Netherlands at the moment. There is no direct requirement that such entities be licensed but the DNB explained that a financial institution would, in practice be undertaking at least one activity that would be licensed under the Wft.

Ongoing supervision: *Regulation and Supervision of Financial Institutions (c. 23.1); Application of Prudential Regulations to AML/CFT (c. 23.4); Monitoring and Supervision of Value Transfer/Exchange Services (c. 23.6); AML/CFT Supervision of other Financial Institutions (c. 23.7); Guidelines for Financial Institutions (c. 25.1):*

Regulation and Supervision of Financial Institutions (c. 23.1):

998. Article 24 of the WWFT gives powers to monitor compliance with the AML/CFT obligations of financial services providers and those powers have been allocated to AFM and DNB as described above. Articles 26 *et seq* provide sanction powers in the form of administrative fines.

999. For all financial services providers, the Wft provides for further regulation and supervision on prudential and conduct of business matters. The Wft gives the DNB and AFM the powers to:

- License or refuse to license (Articles 2:4 to 2:130 of the Wft).
- Impose conditions on licenses or withdraw licenses (Article 1:104 of the Wft).
- Collect information from and mount inspections on financial institutions (Article 1:74 of the Wft).
- Apply global consolidated supervision (Article 1:55).
- Require institutions to amend their practices (by issuing an instruction under Article 1:75).
- Impose administrative sanctions on financial institutions (Article 1:79 and 1:80 of the Wft).

1000. The supervisory authorities apply a risk based approach. The AFM and DNB adopt different systems but are confident that they would result in the same assessment of AML/CFT risks. By way of example, the DNB risk-based approach examines the risks posed by each institution from the point of view of the customers, products and business. This is assessed and updated as part of the regular contacts with the institution, including the inspections and the quarterly meetings. The supervisor will assess the gross risk, take account of mitigating factors and then arrive at an estimate of residual risk. This assessment then prompts the allocation of resources and then priorities for the supervisory process. The authorities state that following this approach puts attention for integrity risks (including ML and TF) high on the agenda of DNB's ongoing supervisory activities.

1001. There is no comprehensive data on the number of inspections undertaken by the DNB and AFM on AML/CFT related matters, although the DNB state that, over a period of four years, the 58 licensed banks had been subject to 86 AML/CFT related inspections (up till October 2010). Some examinations can be spread out over a considerable period. These have been undertaken with increasing frequency as the following table demonstrates:

DNB AML/CFT-audits (banks) over the last 5 years (till October 2010)	
2006	7
2007	6
2008	12
2009	35
2010	25

1002. The DNB were not able to give comparable data on insurance businesses but stated that in 2009 an audit among 10 life insurance companies (selection based on a risk assessment) has taken place and 3 insurers had been subject to action taken in the context of thematic examinations of integrity risks regarding real estate.

1003. The AFM, after the assessors' on-site visit provided additional information on its investigation and enforcement action. It was pointed out that in 2010, 41 investigations of "low end" financial services providers took place, each one of which included a file review to assess the adequacy of CDD, including the identification of ultimate beneficial owners.

The DNB and AFM state that AML/CFT matters are usually included within inspections with a broader theme. The DNB have further stated that AML/CFT compliance form part of regular inspections. In the case of AML/CFT related incidents or thematic inspections, special AML/CFT inspections of targeted institutions are undertaken. In addition to the inspections, the supervisors have quarterly meetings with the major institutions and even more regularly in the contacts between the appointed expert in compliance and integrity issues of the supervisory team and the supervised institution. The supervisors have stated that AML/CFT is usually on the agenda.

1004. The DNB indicated that, a typical thematic inspection process relating to a regulated financial entity would involve the appointment of a project leader of a team of inspectors charged with examining a particular theme. The theme might be, for example, the compliance with the sanctions legislation or correspondent banking requirements. The entities to be visited would be chosen according to set criteria, for example, the size of the business the known risks and previous experience of compliance weaknesses. Pre inspection information would be requested and reviewed. A visit might take anything from 1–2 to 9–10 days during which there would be discussion with the management, benchmarking of policies against industry practice, sampling of individual customer or transaction files as appropriate, and an examination of the institution's risk assessment and mitigation procedures. This latter examination would cover the entity's policies, procedures, controls, information systems and evaluation process and governance arrangements.

1005. In 2009, the DNB had conducted such a themed visit on the CDD practices of insurers. The selection of entities to visit was based on a self assessment and market share. The DNB stated that the insurers covered by this programme account for 85 percent of the business for which independent life insurers (i.e. those not associated with one of the major four international banking groups) were responsible. The DNB noted that their ability to adhere to a priority based inspection program had been disrupted on several occasions by the need to respond to more immediate concerns such as a financial fraud involving real estate. Nevertheless they considered that they had sufficient resources to carry out effective monitoring of AML/CFT compliance.

1006. The AFM risk based approach results in a focus on high impact firms (which are those responsible for most of the business in the Netherlands). Such institutions are subject to regular inspection visits. Although it would be rare for such visits to focus exclusively on AML/CFT, compliance with AML/CFT requirements is included as part of a broader inspection and action has been taken on AML/CFT compliance failures. The AFM has decided to conduct specific compliance visits on AML/CFT matters in future, starting in 2011 The remaining institutions are subject to lighter monitoring which

involves maintaining alert for signals of possible weaknesses (such as customer complaints). Where appropriate, firms may be subject to more intensive monitoring. This method arises from an overview of the risks of the entity and is not directly related to AML/CFT matters. It is rare that there are any signals relating to AML/CFT matters.

1007. The institutions interviewed by the mission confirmed that there was a regular program of inspections and quarterly meetings. Each of the institutions interviewed by the assessors was fully aware of the names of the individual supervisors with responsibility for them and reported that they have found the supervisors to be helpful and accessible.

1008. In the case of money transfer offices and bureaux de change, the institutions interviewed by the assessors considered that the DNB specialist team was innovative and effective. The team took a proactive approach and suggested ways in which AML/CFT controls could be enhanced and monitored to ensure they were taken up. The money transfer offices and bureau de change were clear that there was substantial added value in the supervisory approach.

1009. Each of the major banks interviewed by the assessors reported that inspections in general were relatively frequent for the major institutions and often included some AML/CFT element but that inspections focusing solely on AML/CFT matters were rare. They told the mission, that their AML/CFT systems were primarily developed using their own experience or research elsewhere and that significant recommendations by the DNB on the adequacy of the defences were rare. However, the institutions confirmed that, when inspections were undertaken, the inspectors reviewed policies, procedures, books and records and conducted sample testing.

1010. One smaller bank, recently established had clearly found the advice of the DNB invaluable in setting up AML/CFT systems in their particular context. They had sought DNB advice, found it convincing and relevant and had followed it.

1011. On the other hand, one major insurance institution, reported that a recent inspection on AML/CFT consisted solely of a one day visit by two inspectors. The inspectors identified that the institution had not been adequately monitoring its customers' transactions and made recommendations for improvement which were accepted. The supervisors had examined policies, procedures manuals and the web based learning module that is available for all staff who do not require the more extensive training designed for those with compliance responsibilities. The institution had noted that the supervisors made no comment on the training in their report, even though the training module had not been updated to take account of the WWTF and that it was not the practice of the institution to provide this training annually to staff, nor to test staff on their knowledge of it. No sanction had been applied.

1012. In addition to their direct powers, the authorities are able to make use of internal and external audit reports. Internal audit reports are made available to the supervisory authorities and are discussed. One person interviewed by the assessors estimated that over 10 percent of internal audit of a bank might be related to AML/CFT. External auditors are concerned with the financial position of the regulated entity but would be required to examine governance and control arrangements of interest to the supervisors. Discussions with the external auditors also routinely take place.

Application of Prudential Regulations to AML/CFT (c. 23.4):

1013. Many of the prudential requirements that are imposed on financial institutions are, in themselves, relevant to defenses against money laundering and terrorist financing. These would include requirements for policies that result in sound business operations (Article 3:10), the control structure (Article 3:16), the assessment of integrity risk (Article 10 BPR Wft). In the latter context, Article 3:17 of the Wft requires a

financial institution to have measures that prevent the enterprise or its employees from breaking the law or preventing clients from operating in a way that might undermine confidence in the enterprise or the financial markets. In addition, the detailed implementing regulations impose requirements for customer identification and transaction monitoring on certain regulated entities that are clearly relevant for AML/CFT (Article 14 BPR Wft and Articles 21 and 26 of the BGFO Wft).

1014. The use of the broad range of Wft supervisory powers to monitor and supervise compliance with AML/CFT obligations is discussed in the legal framework section. The assessors accept that the supervisory authorities are able, in practice, to apply prudential regulation to AML/CFT.

1015. The authorities have stated that, in addition to the use of supervisory powers to assess AML/CFT compliance in domestic institutions, it is the practice of the DNB to regularly visit foreign branches and subsidiaries of Dutch financial institutions and to include an assessment of AML/CFT compliance in those inspections.

Monitoring and Supervision of Value Transfer/Exchange Services (c. 23.6):

1016. Payment services providers (money transfer offices) must be licensed by the DNB (Article 2.3a of the Wft). Until November 2009, money transfer offices were subject to the provisions of a dedicated statute (Wgt). However, the supervision of money transfer offices is now subject to the Wft. Bureaux de change are still subject to the Wgt. Chapter 3 of the Wgt provides monitoring and supervisory powers.

1017. The DNB has been conducting monitoring activities in relation to money transfers and exchange offices. Inspections take place very frequently, for a number of offices, inspections occur every three months. The inspectors have given detailed advice on risk management issues and the obligations of the money transfer offices and bureau de change. The program of inspections is regarded as effective by the money transfers and exchange offices themselves; there is clear value added in the advice given to the offices by the DNB inspectors and the frequency of inspections is sufficient. The evidence available to the assessors supports this view. The offices were clearly aware of their obligations and were prepared to share detailed statistics on their operations and risk management. The data on the inspections is as follows:

Number of inspections money transfers and exchange offices					
Year	**2005**	**2006**	**2007**	**2008**	**2009**
Number of on-site inspections	45	55	58	70	61

AML/CFT Supervision of other Financial Institutions (c. 23.7):

1018. In practice, all financial services activities are undertaken by entities that are subject to the Core Principles with the exception of money transfer offices and bureaux de change, which are required to be licensed or registered (bureau de change) and have been discussed in the previous section.

1019. Financial activities that are undertaken by entities not covered by the Core Principles would, for the most part, be conducted by businesses that are defined as “financial institutions” in the Wft. This is not a separate license category in the Wft and the DNB explain that any entity carrying out the activities included within the definition would, in practice require a license under another license category in the Wft. There are no licenses for “financial institutions” as defined in the Wft. The supervisory powers granted in the WWFT apply to all these institutions and therefore the AFM and DNB are able to exercise supervisory oversight.

Guidelines for Financial Institutions (c. 25.1):

1020. Although there are some detailed provisions in the WWFT and Wft and accompanying regulations (for example on customer identification), the provisions in the WWFT and the Wft are, for the most part, written at a very high level of generality. This is considered necessary to enable the statute to provide stable requirements that are applicable to a widely-diverse financial sector, which is subject to constant change.

1021. In addition to the WWFT and regulations, the supervisors have drawn the attention of regulated financial entities to the guidance issued on AML/CFT by international standard setting bodies, including, for example, the papers on customer due diligence and guide to account opening (issued in February 2003) that were issued by the Basel Committee for Banking Supervision in October 2001 and February 2003, respectively. The authorities have published frequently asked questions on their web sites. In cooperation with the Netherlands Bankers Association, the DNB has issued guidance on customer due diligence from the start of the international efforts in this respect. This guidance, which was based very closely on the Basel Committee 2001 paper already mentioned, was originally issued in 2003 and updated in 2006. Both the DNB and the Bankers' Association informed the mission that it is still considered valid. However, it refers to the statutes that preceded the WWFT and includes advice that is no longer correct (for example, Section 2.3 states that there is no need to identify beneficial owners except for high risk services). The guidance is heavily skewed towards the process of identifying customers. Monitoring activity is discussed but receives far less attention.

1022. The assessors consider that the guidance issued is not sufficient to provide a clear indication from the authorities as to their expectations of the measures the regulated financial entities should put in place to ensure adequate AML/CFT measures. Moreover, the DNB should not allow formal guidance to remain in place with outdated references and advice that is inconsistent with current requirements. The authorities have indicated that revised guidance will be issued before February 2011.

1023. On the other hand, the published guidance is supported by further guidance given on a case by case basis, both orally and in writing by the supervisory authorities as part of the process of supervision. This point was confirmed in meetings with regulated entities and is discussed below in the context of effectiveness.

Analysis of effectiveness of the Supervisory and Oversight System

1024. The supervision and oversight of all the activities listed in the definition of "financial institutions" is properly allocated to the DNB and AFM. In each case, there are licensing requirements that prevent unauthorized activity. The provisions give the authorities the powers to ensure that those in control are fit and proper and that criminals are excluded from ownership of the financial businesses.

1025. All relevant financial entities are subject to the WWFT. This law gives the DNB and AFM powers to obtain information from and generally monitor the activity of the institutions. There are adequate powers to enforce the provisions of the WWFT, although, as noted in the legal framework section above, the application of more detailed provisions in the Wft on such matters as internal controls, training and employee screening do not apply to all regulated financial entities and their application to mainstream institutions such as banks and insurers could be challenged. There are adequate sanctioning powers in the WWFT itself and further powers in the Wft although the use of the latter is subject to the same caveats; namely, that it rests on an interpretation of the Wft that could be challenged and the sanctioning powers in the Wft could not be used in respect of those entities not subject to its detailed provisions. In practice, the data on punitive sanctions is insufficient to enable the assessors to make a judgment on whether they are

used adequately to impose effective, proportionate and dissuasive sanctions in order to achieve an adequate level of compliance.

1026. Each of the private sector regulated entities interviewed by the mission confirmed that their lead regulator (whether AFM or DNB) discussed AML/CFT obligations with them and, in particular:

- Held regular meetings (usually quarterly) with management that often included AML/CFT matters.
- Conducted inspections that usually involved some analysis of compliance with AML/CFT obligations.
- In the case of DNB had conducted some inspections devoted to the theme of compliance with customer due diligence obligations.
- Made recommendations and suggestions for enhancing compliance with AML/CFT obligations.

1027. The information given to the assessors, and described above, and the interviews with the private sector, confirmed that the supervisors conduct a program of supervision and inspection that includes AML/CFT.

1028. The WWFT imposes AML/CFT obligations that are written, for the most part, at a relatively high level of generality. Although there is very considerable detail in the implementing regulation on the documents than can be used to verify identity, the main obligations to conduct customer due diligence, to monitor transactions, to apply enhanced or simplified due diligence in certain circumstances, to screen new staff and to train employees are written in broad terms. This is consistent with the risk based approach, which enables the regulated entity to determine the most appropriate measures to meet the objectives of the WWFT. However, this approach means that considerable supervisory guidance is required to supplement the broad provisions.

1029. There is published guidance, as noted above in the assessment of criterion 25.1. However, as noted there, the guidance is also at a high level of generality. Some of it is out of date and incorrect and will be replaced by new guidance before February 2011.

1030. In addition to the published guidance, the DNB has provided its staff with a manual that provides much more detailed information on the kinds of procedures that inspectors might expect to see in different financial entities and to provide the basis for the oral guidance that the examiners should give to regulated entities. This 90 page manual includes detailed guidance on management frameworks, risk analysis and CDD procedures that should be expected in regulated entities. The manual is a very useful guide to identifying an appropriate AML/CFT strategy and focuses, quite rightly, on governance and the development of an appropriate risk management strategy for AML/CFT defenses, in the context of a risk based approach. Any regulated financial entity that followed the advice would have strong and robust systems. This is used as the basis for specific recommendations to banks. However, it is not published and therefore not directly available to the regulated entities.

1031. The AFM manual was not available to the assessors in English but it is clear that it is not as extensive as that of the DNB.

1032. In other jurisdictions adopting principles based and risk based approaches, there tends to be more guidance concerning the kinds of measures the supervisory authorities would expect to see implemented by different institutions in different kinds of business. In practice, as observed elsewhere, the regulated entities

in the Netherlands adopt practices that go beyond the provisions of the WWFT and follow procedures not unlike those followed by similar entities in other countries. The mission sought to establish on what basis the institutions developed their own procedures.

1033. None of the entities referred to the public guidance issued by the Bankers' Association and DNB as being a source of information when developing their systems, in some cases, pointing out that it was out of date and written before the current WWFT was in force.

1034. In the absence of comprehensive data on AML/CFT inspections, the assessors have little information on which to base an assessment of effectiveness beyond the interviews with a selected number of institutions (albeit including the largest and most significant). Some major global banks clearly adopt standards based on international best practice as defined in other jurisdictions. One bank had sent a senior compliance manager to the United States to establish what best practice existed there. Another bank told the mission that the commercial bank's AML/CFT policy had been prepared in the United Kingdom. A third major bank pointed out that it had its own experience based on working in most major countries in the world and adopted practices derived from that experience. In each case, the banks told the mission that they considered that their approach was accepted by the DNB (as lead regulator for banks) without the need for significant recommendations for change in inspection reports or other discussions.

1035. For smaller institutions, that did not have access to such international experience, it was clear that more reliance was placed on the discussions held with supervisory staff. In some cases, it is clear that such discussions have been central to the development of the policy. For example, money transfer offices expressed very considerable satisfaction with the assistance given by the DNB in respect of their identification and monitoring procedures and the systems they needed to have in place to meet their obligations. They regarded the DNB supervisors as knowledgeable and helpful. Similarly, another small institution recently established as a bank had clearly relied heavily on DNB guidance in establishing its systems and expressed itself as satisfied by the support given.

1036. The assessors could not help noticing, however, that the compliance position was not always as positive as in the cases described above. One important insurance institution had received its first inspection visit on CDD matters in 2009 and had been found to have inadequate monitoring systems in place which had failed to detect even those transactions that were consistent with the classic ML typologies for that institution. For this insurance institution, supervision could clearly not be regarded as effective, and, the other data supplied by the authorities suggested that the experience of the insurance institution in being subject to its first inspection visit on AML/CFT matters in 2009 was not atypical. The absence of sanctions in this case, suggests that the weaknesses found in this case were also not atypical. Other entities, during interviews with the mission had shown themselves uncertain as to the provisions of the law. Some entities, including some whose lead supervisor was the AFM suggested that AML/CFT matters were rarely discussed.

1037. The supervisory approach adopted by the DNB and AFM varied according to the different categories of financial entity and according to their risk-based approach, as might be expected. The DNB team responsible for the money transfer offices is very much a "hands on" regulator, giving very specific guidance, mounting inspection visits every three months and providing detailed guidance as to electronic and manual systems that might be used. For major banks, the supervisors engage in more general discussions about AML/CFT matters while satisfying themselves, through occasional inspections that the detailed implementation of CDD and other obligations was satisfactory. A similar approach is adopted towards insurers. The last full round of themed CDD inspections by the DNB was in 2006, followed by yearly follow up examinations regarding the institutions found to have weaker CDD-controls in place. Elements of CDD (such as identification, reporting, ongoing CDD, high risk areas) are subject of ongoing supervisory actions by DNB. The DNB informed the mission that there had been other CDD related

inspections since that time and that a further round of thematic inspections was expected in 2010 and 2011 regarding, for example, CDD and the mitigation of TF risks in trade financing.

1038. The AFM is faced with the task of supervising a large number of institutions. It informed the mission that there are about 10 000 financial services providers and it is clearly impossible to conduct active monitoring of them all. The AFM adopt a risk based approach, focusing on the larger providers and relying on a series of signals to alert them of possible difficulties in the smaller regulated entities. In practice the financial service providers, who are primarily insurance brokers, do not handle client money and the risk of money laundering or terrorist financing through these businesses is low. For this reason, the AFM regards each of these businesses as being of low risk and not requiring active monitoring unless there is an alert (such as customer complaints or a reference from an insurance company). In general, and subject to what follows, this is a reasonable and pragmatic approach. However, the financial services providers are the first step in the CDD chain and, although the insurance companies carry the responsibility for proper CDD of customers, the role of the financial services providers is important and there needs to be some more regular and routine monitoring of effectiveness of their CDD procedures.

1039. The AFMs active monitoring is focused on the larger businesses, which are also those where the AML/CFT risks are higher than with the smaller firms. The AFM informed the assessors that their view of the risks associated with money laundering in these larger firms was influenced by the fact that the entities could not accept cash as payment for services. All payments went through banks that were responsible for customer identification and monitoring. Where there was action taken in respect of breaches of AML/CFT requirements, the AFM would investigate them along with other offences and impose penalties in respect of the offences which were easier to prove and carried heaviest penalties. These were not often AML/CFT breaches. The AFM also informed the assessors during their interview that they did not regard a focus on procedures adopted by regulated entities as being necessary. They preferred, instead, to pay attention to breaches of the law that created identifiable harm. The AFM subsequently modified their position and stated that its staff checked the effectiveness of procedures.

1040. The mission was concerned that this approach may result in too low a priority being given to AML/CFT matters and this view was reinforced by the interviews with private sector entities whose lead regulator was the AFM. In particular:

- The absence of cash as a payment for financial services does not mean that the risk of money laundering can be regarded as low in a sophisticated financial sector such as The Netherlands, where financial businesses can be used to layer and integrate laundered money into the financial system.

- Smaller brokers (financial services providers) play a key role in identifying and verifying the identity of customers of banks and insurers and it is important that their CDD practices are properly monitored.

- Banks may be monitoring the customers who also undertake investment business but the investment firms will know more about the clients' investment objectives and will be in a better position to monitor whether or not the investment activities match the expected profile of activity.

- All regulation, to some extent, and particularly the creation of defenses against AML/CFT, rely on procedures as preventive measures and the initial suggestion made by the AFM to the mission that a focus on procedures was not appropriate was surprising (although the AFM has subsequently modified its statement, as described above, having seen the preliminary conclusions of the assessors).

1041. The mission is concerned that these factors may result in supervision of AML/CFT being less effective than it could be. The assumptions that the absence of cash meant that that ML/TF risk was low, the statement (albeit subsequently modified) that regulated entities would not understand the importance of preventative procedural measures and the communication of those approaches to the regulated sector undermine the effectiveness of implementation of the AML/CFT defenses. The absence of routine monitoring of CDD practices of financial services providers, the limited data on inspections, sanctions or even training on AML/CFT matters meant that there was little evidence to counter the assessors' concerns.

1042. The assessors concluded that:

- The legal and regulatory provisions were broadly adequate for the task of implementing AML/CFT controls (although as noted above, the legal position with respect to the use of Wft powers to enforce controls on AML/CFT matters may be open to challenge).

- A risk-based, principles-based approach is a sound basis on which to approach the implementation of AML/CFT defenses.

- The limited data on inspections and punitive sanctions being imposed gave little basis on which to assess the effectiveness of the supervisory approach but the interviews conducted by the assessors suggested that:

    - In some cases, the value added by the supervisor in assisting companies develop AML/CFT systems clearly added considerable value.

    - In the absence of detailed guidance given by the supervisor as to what is expected of the financial entity, some entities were choosing to implement the provisions in the WWFT in a minimalist manner while others were looking to their international experience to establish best practice.

    - One major insurance institution had failed to implement even the most minimal monitoring arrangements prior to an inspection in the year preceding the mission, although this has since been addressed by the DNB through the issuance of an instruction.

- There is a need for a more active approach to AML/CFT implementation in the AFM regulated sector that recognizes the risks, in particular of the use of investment intermediaries for layering and integrating the proceeds of crime into the financial system stresses the importance of good CDD practices, even amongst small brokers who do not handle client money and instills in the regulated sector a full understanding of the importance of well thought through procedural and governance arrangements designed to mitigate the AML/CFT risk.

- The variation in practice between different institutions could not always be explained by the differences in the character of the institution itself and may result from differences in the approach of supervisors, some of which were identified by the assessors.

In respect of the formal powers of supervision, the DNB and AFM have the powers they require. The assessors took very seriously the weaknesses identified in respect of insurance and the businesses for which AFM were responsible. Nevertheless, looking at the financial system as a whole, the assessors took the view that, notwithstanding these weaknesses, the DNB has a supervisory program that enables it to satisfy itself of the adequacy of the AML/CFT systems, procedures and controls in the major institutions that dominate financial services business in The Netherlands. Moreover, for the smaller banks (and other smaller financial businesses for which it is responsible) the DNB had been helpful in assisting the

development of AML/CFT defences. For independent insurance companies, although the assessors noted weaknesses as described, the DNB had begun to implement a more intensive program that covered business accounting for most of that conducted by independent insurers. On balance, essential criterion 23.1 is therefore largely met and, as noted in the detailed account above, all other criteria for Recommendation 23 are fully met.

3.10.2 Recommendations and Comments

1043. While the supervision process is mature and appropriately integrated in the general supervision of all financial institutions, the mission would make the following recommendations:

- The authorities should collect more comprehensive and detailed data by sector and by year, on the use of their inspection and enforcement powers with respect to AML/CFT matters and on the nature of the weaknesses being identified, so as update their understanding of ML and TF risks and to satisfy themselves that appropriate and effective action is taken in this area.

- The AFM should review their approach to AML/CFT and increase their focus on monitoring the procedures put in place by regulated entities to detect and deter money laundering and terrorist financing and should implement increased monitoring of CDD practices by the large number of smaller businesses that are brokers.

- The DNB should formally withdraw the guidance issued with the Bankers Association in 2006 and issue revised guidance based on.

- The useful material currently in the DNB staff manual and underlining the importance of ongoing customer monitoring as well as the formal identification and verification obligations together with advice on staff vetting and training (the authorities have indicated an intention to complete both tasks by February 2011.

- The staff training program should be reviewed to ensure that each member of staff receives adequate training on AML/CFT (preferably on an annual basis) and comprehensive data should be maintained on this.

- The authorities should use the powers they state are available to ascertain the source of funds and wealth as one of their measures to make sure that financial institutions are not controlled or owned by criminals or their associates and the implementing decree for the relevant provisions in the Wft should be amended to make explicit that this information should be supplied.

3.10.3 Compliance with Recommendations 17, 23, 25 & 29

	Rating	Summary of factors underlying rating
R.17	**LC**	• Punitive sanctions are available which, for the most part are capable of being used in an effective, proportionate and dissuasive manner but there is limited use of such sanctions in practice. • In respect of their impact on the largest institutions, administrative fines remain modest and may, in some instance, be insufficiently effective or dissuasive.
R.23	**LC**	• There are doubts about the effectiveness of supervision for independent insurance businesses (although the DNB has been addressing this since 2008); and • The approach of the AFM gave particular concern that they were not ensuring that institutions in the relatively minor part of the financial services business within their jurisdiction were effectively implementing their AML/CFT obligations.
R.25	**PC**	• Guidance issued to financial institutions is at too high a level of generality to ensure

	Rating	Summary of factors underlying rating
		that implementation of AML/CFT defenses is adequate and there is a need for more detailed guidance on the nature of AML/CFT risks in The Netherlands, the importance of establishing a profile and monitoring and the training and screening of staff. • Guidance is, in some respects, out of date, incomplete, and inaccurate. • Feedback to reporting institutions from the FIU is not regarded as sufficient by those institutions.
R.29	**LC**	• The observations on the administrative sanctions noted in the rating for R.17 are equally relevant here.

3.11 Money or Value Transfer Services (SR.VI)

3.11.1 Description and Analysis (summary)

Legal Framework:

1044. AML/CFT obligations are imposed under WWFT. Supervisory responsibility is allocated to the DNB under BATWWFT. There is a licensing requirement for money transfer offices under Article 2:3a of the Wft as amended. Bureaux de change are subject to registration under Article 3 of the Wgt.

Designation of Registration or Licensing Authority (c. VI.1):

1045. Article 2 (1) of the Wgt gives the registration power for bureaux de change to the Minister but this has been delegated to the DNB under the delegation decree. Article 2:3b of the Wft gives the licensing power in respect of money transfer offices to the DNB. Banks providing these services are registered under the Wft but are exempt from separate registration as providers of these services under Article 2:3a (2).

Application of FATF Recommendations (applying R.4-11, 13-15 and 21-23, and SRI VI)(c. VI.2):

1046. These Recommendations are imposed by the WWFT. Article 1 (1) (a) (4) of WWFT applies the AML/CFT provisions to money transfer offices and in this context, this includes money transfer offices and bureaux de change. These provisions are applied to money transfer offices by this Article of the WWTF in the same way as they are applied to all other regulated financial entities. SR VII is imposed on money transfer offices directly by EU Regulation 2006/1781, since such businesses would be payment services providers as defined in Article 2 of the EU Regulation.

Monitoring of Value-Transfer Service Operators (c. VI.3):

1047. The monitoring of compliance by money transfer offices and bureaux de change with their obligations under the WWFT is allocated to the DNB under Article 1 (1) of the implementing decree BATWWFT. The supervisory powers of Chapter 5.2 of the Awb are applied to the monitoring of WWFT obligations by Article 24 (4) of the WWFT.

List of Agents (c. VI.4):

1048. Article 2:3c of Wft requires the money transfer office to notify the DNB of its agents. It is clear that this is done effectively and that the DNB is aware of the agents of the money transfer offices. The DNB demonstrated their knowledge of the agents within their supervision.

Sanctions (applying c. 17.1-17.4 in R.17) (c. VI.5):

1049. The sanctions available under Articles 26 *et seq* of the WWFT apply to money transfer offices. These sanctions can be applied in respect of breaches of the AML/CFT obligations in that Act. There are

also sanctions available in the Wgt for bureaux de change. The applicability of sanctions available in the Wft is discussed in the section on the legal framework for supervision.

Adequacy of Resources—MVT Registration, Licensing and Supervisory Authority (R.30):

1050. The DNB devotes sufficient resources to the registration and supervision of money transfer offices and bureau de change. The entities report that they are subject to frequent inspection visits and that the advice they receive is helpful and informative. Details are given in the section on supervision.

Additional Element—Applying Best Practices Paper for SR VI (c. VI.6):

1051. The authorities state that the provisions of the best practices paper have been applied. It is clear that the requirement for registration is in place and that the AML/CFT obligations for money transfer offices and bureaux de change apply. The regulated entities interviewed by the mission considered that there was little evidence of widespread illegal money transfer activity. The authorities stated that the use of money transfer offices was largely confined to specific groups and that their monitoring of illegal activity was based on a risk assessment derived from this analysis. The assessors concluded that the existing businesses would be aware of and would have an incentive to identify illegal offices acting in competition with them and their assessment that there was little such activity confirmed the authorities' view. It would therefore appear that the resources devoted to the deterrence of such activity are adequate.

Analysis of effectiveness

1052. The regulation and supervision of money transfer offices is now encompassed within the Wft, while that for bureaux de change remains with the Wgt. It is understood by the mission that the bureaux de change may, in due course, be brought within the Wft as well.

1053. The use of the Wft to enforce controls on AML/CFT matters is as vulnerable to challenge in the case of money transfer offices as it is with any other entity regulated under the Wft. There is less risk in respect of bureaux de change, supervised under the Wgt, since the Act refers explicitly to the need to have controls to implement the obligations of the WWFT. The recommendations made above will deal with this problem in respect of money transfer offices.

1054. The assessors found a considerable degree of satisfaction on the part of the money transfers offices and bureaux de change about the nature of the support they received from the DNB as supervisor. The DNB officers were knowledgeable and innovative, providing specific and practical suggestions about systems and controls to the regulated entities. The assessors were initially concerned that, perhaps the approach was so intensive that the supervisors were in danger of taking over some aspects of the management of the money transfer offices and bureaux de change but, on reflection, following interviews with the regulated entities, concluded that the level of supervision was appropriate, particularly for high risk offices unused to detailed AML/CFT regulation. It was clear that the supervisory officers had no difficulty in asserting their requirements.

1055. The assessors are aware that money transfer offices and bureaux de change provide the large majority of unusual transactions reports to the FIU, including reports under the subjective indicator. The representatives of these offices who were interviewed stated that their reporting practices followed guidance from the supervisory authority. They showed the assessors their records that demonstrated that, in recent years, very few of the reports resulted in a determination by the FIU that a transaction was suspicious. One office informed the assessors that the percentage was below two percent and all confirmed it was below five percent. The authorities insisted that the overall figure for money transfers was between 15–20 percent. The supervisors may wish to consider therefore, whether this level of reporting in fact reflects the presumption of ML or TF that is required by the WWFT for a report to be filed. If relatively

few of the reports result in a determination that the transaction was suspicious, then, either the level of reporting is inappropriate, or the way in which suspicion is determined by the FIU is missing important information. Both these possibilities may be an accurate statement of the position. If the level of reporting is not appropriate the DNB should consider adjusting their guidance.

1056. Overall, the assessors concluded that the supervision of money transfer offices and bureaux de change was effective.

3.11.2 Recommendations and Comments

1057. The FIU data shows that reports from money transfer offices form the large majority of all reports submitted to the FIU and the offices' own records show that few of these reports have been deemed suspicious in recent years. Although the data provided by the FIU suggested a higher proportion were deemed suspicious, the fact remains that none of those interviewed by the assessors considered that the money transfer offices represented the main ML or TF risk faced by The Netherlands. The level of reporting, therefore, appears to be out of proportion to the likely ML/FT activity. The DNB is recommended to review its advice to the money transfer offices on reporting on the basis of the subjective indicator, in consultation with the FIU, so as to maximize the value of the reporting system and seek a level of reporting that accurately reflects the presumption of money laundering. As noted above, the authorities are also recommended to apply the provisions of Article 3:99 to payment services providers, so that the owners may be subject to fit and properness tests.

3.11.3 Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
SR.VI	**LC**	• The application of the FATF Recommendations to money transfer offices and bureau de change suffers from the same deficiencies as identified in relation to the rest of the financial sector (see sections 3.1 to 3.10 of this report).

4. PREVENTIVE MEASURES—DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

Legal Framework:

1058. The preventive measures for DNFBPs are set out in the WWFT, with the exception of customer due diligence and record-keeping requirements for TCSPs which are set out in the Wtt (Trust offices act). With minor variations, as discussed in the relevant sections, the preventive measures are the same for DNFBPs and financial institutions. The strength and weaknesses of the general CDD and record-keeping regime are analyzed in section 3 above and the comments there apply equally to DNFBPs unless indicated otherwise.

1059. The scope of the businesses and professions subject to AML/CFT preventive measures generally follows the FATF definition. Other non-financial business and professions covered by the WWFT are mentioned in relation to Recommendation 20. The discrepancies between the scope of the DNFBPs in the Netherlands and in the FATF standard are analyzed.

1060. **Casinos:** Pursuant to Article 1 (1) (a) (16) WWFT, a "natural person or company operating a casino within the meaning of Article 27g (2) of the Game of chance act" is included into the scope of the institutions subject to the law. Only one casino license has been granted on the basis of the definition provided in Article 27g (2), namely, to the company "Holland Casino". At present, the Games of Chance Act does not provide for the granting of permits to organize games of chance via the internet, and therefore it is forbidden.[93] No threshold applies in relation to the AML/CFT preventive measures for casinos. A number of gaming halls are operating in the Netherlands but they fall outside the definition of a casino in the gaming act even though a number of them are named "Casinos". Their services are limited to slot machines and arcade games. While the FATF standard does not define the term "casino" it is possible to rely on the dictionary definition of a casino being "a public building or room where gambling games are played." Consequently, gaming halls operating in the Netherlands would fall into the scope of the term "casino" as used by the FATF standard. This said, based on the strict regulations[94] that apply to slot machines in gaming halls, summarized in the table below, the assessors conclude that the risks of gaming halls being used for ML/FT are low in the Netherlands.

1061. Cruise ship casinos operating to or from Dutch ports are subject to the game of chance act when in Dutch waters. At present, only the state owned 'Holland Casino' is allowed to operate a casino on the basis of the definition provided in Article 27g(2) of the game of chance act. Holland Casino does not operate cruise ship casinos. In the harbour of Rotterdam, a special police force (*Zeevaartpolitie*, or Seaport

93 In August 2010, an Advisory Commission on Internet Gaming presented its findings regarding this subject. The main conclusion was that a possible legalization should be limited to poker, and take the shape of a licensing regime with a limited number of licenses to be granted for a fixed term and periodically assigned through an open and transparent procedure.

94 The minister of Economic Affairs is responsible for the supervision on licence holders for the exploitation of slot machines, as per art. 30w-1 WoK.

police) is responsible for safety and the general compliance with Dutch laws. The available enforcement methods include on-board checks.

Regulation of slot machines in gaming halls and in Holland casino		
	Slot machines in gaming halls	**Slot machines in Holland casino**
Maximum 'bet' per game	EUR 0.20	EUR 50-
Maximum profit per game (excl. jackpot)	200 times the bet, = EUR40-	not specified (in practice: several thousand times the bet)
Maximum jackpot	EUR 2 500-	unlimited (millions)
Maximum loss per game	200 times the bet, = EUR40-	EUR 150-
Maximum average losses per hour (after 100 hours play)	EUR 40-	not specified (in practice: unlimited)
'Casino Value Instruments'	Cash only	Different options (credits, vouchers, cards, etc)
Legal provisions	Art. 30 WoK and Art. 13-15 Decree on slot machines	Art. 30 WoK and Art. 11 Decree on slot machines

1062. **Real estate agents:** Article 1 (1) (a) (14) WWFT provides that any "intermediary as referred to in Section 62 of the commercial code (*Wetboek van Koophandel*), insofar as this intermediary provides brokerages services in the establishment and conclusion of agreements on immovable property and rights attached to immovable property" is within the scope of the law. It has to be noted that in the Netherlands, real estate agents only represent one party in a transaction but may never represent both the buyer and the seller in order to avoid conflict of interest.

1063. **Dealers in precious metals and dealers in precious stones:** Article 1 (1) (a) (15) WWFT provides that the law applies to any "seller of goods acting in the course of a business or profession, insofar as payment for these goods is made in cash for an amount of EUR 15 000 or more, regardless of whether the transaction takes place in one operation or in several related operations".

1064. **Accountants:** The scope of application of the AML/CFT requirements for this profession is defined in Article 1 (1) (a) (11) WWFT which relates to "external chartered accountant, external accounting consultant or tax advisor, insofar as they act in the course of their professional activities, or a natural person, legal person or company, insofar as they perform comparable activities in another independent professional or business capacity". In addition, accountants are governed by their own professional law, the Act supervising organizations of accountants (*Wet toezicht accountantsorganisaties*), which does not specifically address AML/CFT issues but is relevant with regard to integrity and monitoring of the profession. There are two types of accountants in the Netherlands. Public chartered accountants/business consultants are governed by the *Wet op de Accountants-Administratieconsulenten*, and are members of the professional association NOvAA. Public chartered accountants are governed by the *Wet op de Registeraccountants*, and are members of the professional association NIVRA. The merger of the two professional associations is currently envisaged. The coverage of accountants under the WWFT is broader than the FATF standard. Under the WWFT, all professional activities are covered while the FATF standard only covers a limited number of activities.

1065. **Lawyers and notaries:** The scope of application of the AML/CFT requirements for these professions is covered in two Articles. First, Article 1 (1) (a) (12) WWFT includes into the scope of the law any "natural person, legal person or company, providing advice or assistance as a lawyer, civil-law notary or junior civil-law notary or in the course of a similar legal profession or business in an independent professional or business capacity with regard to:

- The purchase or sale of immovable property.

- The management of money, securities, coins, banknotes, precious metals, precious stones or other assets.

- The incorporation or management of companies, legal persons or similar bodies as referred to in Article 2 (1) (b) of the State Taxes Act (*Algemene wet inzake rijksbelastingen*).

- The purchase or sale or acquisition of business entities.

- Activities in the field of taxation that are comparable with the activities of the professional groups described under (11)."

1066. In addition, pursuant to Article 1 (1) (a) (13) WWFT, lawyers and notaries are subject to the AML/CFT requirements when they engage in any kind of transaction or property transaction in the name and at the expense of a customer.

1067. It has to be noted that, based on Article 1 (1) (a) (11) WWFT, when lawyers or notaries provide tax advice, they must also observe the regulations of the WWFT. In addition, pursuant to Article 1 (2) WWFT, the AML/CFT requirements do not apply to lawyers and notaries, insofar as they perform activities for a customer in relation to the determination of its legal position, representation and defense before the courts, the provision of advice before, during and after legal proceedings, or the provision of advice about instituting or avoiding legal proceedings.

1068. According to the explanatory memorandum to the WWFT, the "determination of a customer's legal position" aims at providing the lawyers and notaries with the opportunity to determine which services are required. Lawyers need information in order to determine whether or not the service they are requested to perform is being requested in connection with legal proceedings. Notaries need to carry out an initial check to ascertain whether the service requested is the most appropriate one for the customer in this particular case. In order to adequately determine which service is involved, an exploratory meeting with the customer will be required in any case, which is always strictly confidential. This ensures that every customer can freely submit all information that is relevant to assess whether legal assistance is being requested in connection with legal proceedings, and whether services are required that are covered by the scope of the WWFT. The initial meeting should be sufficient for gaining insight into the customer's motives. To the extent that it becomes clear afterwards that the required activities are activities covered by the WWFT and are not related to legal proceedings, these activities will classify as a service governed by the rules of this law. In that case, the lawyer or notary will have to suspend the actual provision of services until he can identify his customer in accordance with chapter 2 of the WWFT.

1069. Additionally, lawyers and notaries are governed by their own professional laws, the Lawyers Act (*Advocaten wet*) and the Notaries Act (*Wet op het notarisambt*), both of which do not specifically address AML/CFT issues but are relevant with regard to integrity and monitoring of the profession. Both lawyers and notaries have self-regulated organizations, respectively the Netherlands Bar Association and the Royal Notarial Association. The Bar association has adopted a by-law on administration and financial integrity, including AML/CFT mandatory rules.

1070. **Trust and company service providers:** Pursuant to Article 1 (1) (a) (10), "trust offices as referred to in Article 1 (a) of the supervision of trust offices act (*Wet toezicht trustkantoren*–Wtt)" are covered by the WWFT. A trust office is defined in Article 1 (a) Wtt as a legal entity, partnership or natural person providing, either by itself or together with other legal entities, partnerships or natural persons, one or more of the following services:

- Being a director of a legal entity of partnership.

- Making an address or correspondence address as referred to in Sections 9(1)(b) and 10(a) of the trade registry decree (*Handelsregisterbesluit* 1996) available to a legal entity or partnership, if at least one of the ancillary activities listed below is provided for the benefit of that legal entity or partnership or for the benefit of another legal entity, partnership or natural person belonging to the same group:
  - Providing advice or assistance in the area of private law.
  - Providing tax advice or preparing tax returns and related work.
  - Performing work in connection with preparing, reviewing or auditing financial statements or keeping accounting records.
  - Recruiting a manager for the legal entity of partnership.
  - Other ancillary activities designated by an order in council.
- Selling legal entities.
- Being a trustee within the meaning of the Convention on the law applicable to trusts and on their recognition.
- Other services designated by an order in council.

1071. These services can be performed in a professional capacity or on a commercial basis on the instructions of another legal entity, partnership or natural person, not being part of the group to which the trust office belongs. Note that the legal framework does not fully encompass one of the activities listed by the FATF for TCSPs, namely the providing of a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangements. This activity is only envisaged by the Wtt as ancillary to another activity, not as a standalone service. While the list above only covers the activity of being a director of a legal entity or partnership, manager are also covered based on Article 3 (1) b Wtt. There is no reference to the activity of forming a trust, but trusts cannot be formed under Dutch law. Similarly, there are no references to the activities of acting as a nominee shareholder for another person, or arranging for another person to act as a trustee of an express trust. But these activities are not allowed to be performed by businesses in the Netherlands.

1072. The Implementing Regulation on Sound Operational Management of Trust Offices (Rib Wtt) details the CDD measures required to be applied by trust offices. In addition, pursuant to the "Exemption Regulation Pursuant to the Act on the Supervision of Trust Offices" from April 22, 2004, and based on Article 2 (3) Wtt, the Minister of Finance has decided to exempt trust offices from the licensing requirement in the three cases listed below if it has been considered that there is already a different type of integrity supervision applying to them or that the integrity risks are negligible:

- Trust offices only providing services to object companies which are registered as a collective investment scheme.
- Natural persons who only provide the service of being a manager of a foundation (*stichting*) which solely hold shares for depositary receipt holders.
- Natural persons who only provide the service of being a manager or partner to object companies, to which a licensed trust office provides service in connection with preparing, reviewing or

auditing financial statements or keeping accounting records. At least, the keeping of accounting records has to be provided by the licensed trust office to the object company.

1073. The table below summarizes the DNFBPs activities not covered by the Dutch AML/CFT legal framework.

Scope of DNFBPs–Activities not covered by the Dutch legal framework		
Type of business	**Legal definition**	**Activities not covered**
Casinos	Article 1 (a) (16) WWFT Article 27(g) (2) Gaming act	Gaming halls – but measures in place to mitigate the risks.
Real estate agents	Article 1 (a) (14) WWFT	Only one party to the transaction is covered, not both the buyer and the seller.
Dealers in precious metals and stones	Article 1 (a) (15) WWFT	Fully covered
Lawyers	Article 1 (a) (12) WWFT Article 1 (a) (13) WWFT	Fully covered
Notaries	Article 1 (a) (12) WWFT Article 1 (a) (13) WWFT	Fully covered
Accountants	Article 1 (a) (11) WWFT	Fully covered
Trust and Company Service Providers	Article 1 (a) (10) WWFT Article 1(a) Wtt	Providing a registered office; business address for a company, a partnership or any other legal person or arrangements, when this service is provided on a standalone basis.

1074. For easy reference, the table below summarizes the most relevant legislation and supervisory or mechanism for each of the DNFPBs. In addition, as for the financial institutions, some provisions of the UBWWFT and URWWFT also apply to DNFBPs.

DNFBPs–Relevant legislation and supervisory/monitoring mechanisms				
Type of business	**Governing law for AML/CFT**	**Regulatory Law**	**SRO**	**AML/CFT Supervisor**
Casinos	WWFT	Game of chance act	No	DNB
Real estate agents	WWFT	No	No	BHM
Dealers in precious metals and stones	WWFT	No	No	BHM
Lawyers	WWFT	Lawyers act	Bar association	BFT
Notaries	WWFT	Notaries act	KNB	BFT
Accountants	WWFT	Act supervising organizations of accountants	NIVRA NOvAA	BFT
Trust and Company Service Providers	WWFT Wtt Rib Wtt	Act on the supervision of trust office, and implementing regulations	No	DNB

4.1 Customer Due Diligence and Record keeping (R.12)

4.1.1 Description and Analysis

CDD Measures for DNFBPs in Set Circumstances (Applying c. 5.1-5.18 in R. 5 to DNFBP) (c. 12.1):

1075. **Casinos:** All the CDD measures described in section 3 apply to the casino licensed according to the Game of Chance Act. In addition, according to Specific Regulation (*Beschikking Casinospelen*, Stcrt. 1997, 248) casinos have to identify all their customers when entering the casino. Holland Casinos holds deposit accounts for clients. It is possible to transfer funds to and from these accounts from and to an account of owner. The WWFT requirements apply to these accounts.

1076. **Real estate agents and precious metals and stones dealers:** All measures described in section 3 apply to these professions. As real estate agents only represent one of the parties, they are not in a position to perform CDD obligations for both the buyer and the seller. They act before the transaction is finalized by a notary.

1077. **Lawyers and notaries:** In general, all the CDD measures described in section 3 apply to lawyers and notaries, with the two exceptions already analyzed.

1078. First, the CDD requirements do not apply to the services listed in Article 1 (a) (12) and Article 1 (a) (13) when they are related to legal proceedings and in relation to the first meeting with the client in order to ascertain its legal position. It has to be mentioned that Recommendation 12 does not exempt lawyers and notaries from CDD requirements, even in case of relation to legal proceedings or in relation to the first meeting. The mandatory by-law on administration and financial integrity issued by the Bar Association adds additional requirements. For example, Article 7.1 of the by-law requires lawyers "when accepting an assignment to satisfy themselves of the identity of the client and, if necessary, the identity of the intermediary who extended the assignment, unless the nature or circumstances of the case make this impossible". While this provide additional coverage and extends some CDD requirements to assignments in relation to legal proceedings or in relation to the first meeting, the by-law does not have the status of primary legislation, and most of the CDD requirements have to be set out in primary legislation.

1079. Secondly, pursuant to Article 4 (5) WWFT, notaries "may verify the identity of the customer and, where applicable, of the beneficial owner at the moment when identification is required under Article 39 of the Notaries Act," which in turn requires verification of the identity only prior to notarial authentication of a deed. In the event no notarial deed is part of the service provided, the standard WWFT provisions apply.

1080. **Accountants:** All the CDD measures described in section 3 apply to accountants.

1081. **TCSPs:** The CDD requirements for trust offices differ from the ones described in section 3 with respect to financial institutions as Article 3 (5) WWFT exempts TCSPs from the CDD measures. This decision has been made because certain identification requirements are included in Article 10 of the Wtt, and details are set out in the Regulation on Sound Operational Management of Trust Offices (Rib Wtt) as analyzed below. The Rib Wtt is a regulation issued by the Dutch National Bank (DNB) and is thus considered secondary legislation for the purpose of this assessment.

TCSPs – When CDD is required (c.5.2:)

1082. The Wtt and the Rib Wtt do not include comprehensive provisions indicating when CDD measures are required. Article 18 Rib Wtt requires trust offices to keep a client acceptance file for every object company. Due to the specificities of TCSP activities, some of the requirements in c.5.2 do not apply, such as (*i*) carrying out occasional transactions above USD/EUR 15 000; (*ii*) carrying out occasional transactions that are wire transfers; or (*iii*) when there is a suspicion of ML or TF regardless of any exemption or thresholds. While there is no explicit requirement in the Wtt or the Rib Wtt to undertake CDD measures when the TCSP has doubts about the veracity or adequacy of previously obtained customer identification data, pursuant to Sections 1 and 2 of Article 12 Rib Wtt a trust office shall not provide any service if it cannot claim to know the identity of the customer

TCSPs—Required CDD measures

1083. There are no requirements in the Wtt and Rib Wtt to identify and verify the identity of the customer, other than the beneficial owner, nor to verify that any person purporting to act on behalf of the customer is so authorized and to identify and verify the identity of that person.

1084. According to Article 12 Wtt, trust offices should know the identity of the ultimate beneficial owner of an object company and gather evidence to ascertain this determination. If an object company has no ultimate beneficial owner, the trust office shall keep available the evidence based on which the identity of the ultimate beneficial owner has been established. Article 1 (c) defines "beneficial owner" as "the natural person who has a qualifying holding in an object company or who is a beneficiary of at least ten percent of the capital of a foundation (*stichting*) or a trust as referred to in the Convention on the law applicable to trusts and on their recognition." Article 1 (h) defines the qualifying holding as a direct or indirect interest of at least ten percent of the issued share capital or a comparable interest, or the ability either directly or indirectly to exercise at least ten percent of the voting rights, or exercising comparable control. Pursuant to Article 14 Rib Wtt, trust offices are required to know the relevant parts of the structure of the group that the object company belongs to. Article 16 Rib Wtt also requires a trust office acting as trustee of a trust to know the identity of the settlor of the trust and the ultimate beneficiary of the trust. If there is no ultimate beneficiary, the trust office shall keep available the evidence from which it was established.

1085. Pursuant to Article 13 Rib Wtt, trust offices shall know the source of assets of an object company and have available evidence of the source of assets when providing a service to the object company. A trust office can be a legal entity, a partnership or a natural person. In addition, the trust office shall keep available evidence of the source and destination of resources of the object company and assess whether these involve integrity risks. Pursuant to Article 14 Rib Wtt, trust offices shall know the objective for which the structure has been set up.

1086. Article 15 Rib Wtt requires the trust office to know the identity of the buyer. It shall also know the identity of the holder of a qualifying holding in the buyer if it is involved in selling legal entities. The trust office should also know the source of assets of the buyer and keep records and documents on how the source was determined, and assess whether the sale of legal entities involves integrity risks. The trust office is prohibited from concluding any contract for the sale of legal entities until the requirements of Article 15 Rib Wtt are complied with. Pursuant to Article 16 (3), if the trust office acts as a trustee of a foreign trust, it shall know the source of assets of the settlor of the trust.

1087. The Rib Wtt contains a general provision in its Article 3 requiring the management of a trust office to take care of the integrity of the trust office and its object companies, on a daily basis. Pursuant to the Explanatory memorandum to the Rib Wtt, under Section 14, "the trust offices must regularly check whether there have been any changes in the structure." In addition, Articles of the Wtt relevant for the CDD indicate that "trust office shall know." In the supervisory practice of the DNB these provisions are interpreted as requiring that the information collected under the CDD process is kept up to date.

TCSPs—Risk

1088. There are no requirements in the Wtt and the Rib Wtt to perform enhanced due diligence for higher risks categories of customer, business relationship or transaction. As indicated above, trust offices are however required to assess the integrity risks in relation to the source and destination of resources of an object company (Article 13 Rib Wtt), and in relation to sale of legal entities (Article 15 Rib Wtt).

1089. The Wtt and the Rib Wtt do not provide for situations where trust offices can apply reduced or simplified due diligence measures.

TCSPs – Timing of verification and failure to satisfactorily complete CDD

1090. Pursuant to Article 10 (g) Wtt, no service may be performed by a trust office if the CDD requirements are not fully complied with.

TCSPs – Existing customers

1091. Pursuant to Article 19 Rib Wtt, trust offices have had a maximum period of six months to comply with the Rib Wtt's CDD requirements for business relations started before the enactment of the Rib Wtt on February 23, 2004.

CDD Measures for DNFBPs in Set Circumstances (Applying Criteria under R. 6 and 8-11 to DNFBP) (c.12.2):

Recommendations 6, 8, and 11

1092. The description and analysis of measures in place for financial institutions (section 3) also apply to all DNFBPs.

1093. Regarding PEPs, while Articles 1 (1) (18) (e) and 8 (4) WWFT applies to trust offices, the same provisions are also found in Articles 1 (i) Wtt and 15 (a) Rib Wtt.

Recommendation 9

1094. For all DNFBPs except trust offices, the description and analysis of measures in place for financial institutions apply. Regarding trust offices, while in practice intermediaries may be used to perform elements of the CDD process (see discussion below on feeders), there are no rules governing such reliance on third parties.

Recommendation 10

1095. For all DNFBPs except trust offices, the description and analysis of measures in place for financial institutions pursuant to the WWFT also apply.

Trust offices

1096. Pursuant to Article 18 (3) Rib Wtt, a client acceptance file must be retained for at least five years after the end of the provision of services. The records that have to be kept are: (*i*) the written contracts between the trust office and the object company and other contracts that the trust office has concluded on the services provided by the trust office covered by the acceptance file, (*ii*) a list of the services provided by the trust service by the client acceptance file, (*iii*) information collected on the beneficial owner, (*iv*) information on the source of assets of the object company, (*v*) information on the relevant parts of the structure of the group that the object company belongs to and the objectives for which the structure as been set up, (*vi*) information required in relation to the sale of legal entities, and (*vii*) information on the source of assets of the settlor of a trust.

1097. In addition, trust offices are required to keep record of information collected on the beneficial owner (Article 12 Rib Wtt), information on the source and destination of resources of the object company (Article 13 Rib Wtt), information on the relevant parts of the structure of the group that the object company belongs to and the objectives for which the structure as been set up (Article 14 Rib Wtt), and information required in relation to the sale of legal entities (Article 15 Rib Wtt). There are however no indications in the Rib Wtt regarding the duration of the record keeping obligation other than in relation to the client acceptance file.

1098. Consequently, the record-keeping requirements for trust offices in the Rib Wtt do not include information on the customer, if different from the beneficial owner, do not include elements related to business correspondence, and there is no indication of duration except for the records kept in relation to the

client acceptance file. But, the general record keeping requirements set out in the Article 52 AWR and Article 10 (1) of Title 1 of Book 2 BW and described in section 3 under c.10.1, apply to trust offices. They enable to set out a general record keeping duration of seven years. However, the requirement for retention of records for seven years does not say from when that period should start. The natural reading of the provision would be that the records should be kept for seven years from when they were created, while to meet the requirements of criterion 10.2, the records should be kept for five years from the date that the relationship with the customer ceases.

Analysis of effectiveness (R.12)

General Findings

1099. Some general findings emerge from the teams' discussions with representatives of non-financial businesses and professions and their associations. Associations and private sector representatives were generally comfortable explaining how they implement the risk-based and principle-based approaches which underpin the Dutch AML/CFT regime. Knowledge of the legal framework, as well as the assessed level of implementation of preventive measures, varied between institutions.

1100. Partly related to the absence of clear guidance, some weaknesses in the implementation of preventive measures have been noticed for all DNFBPs. For example, the obligation to verify the identity of the ultimate beneficial owner for legal persons was generally interpreted to be only applicable in high-risk situations, for which the institutions had implemented different risk assessments and therefore verified the identity under different circumstances. DNFBPs were also confused about the difference between the obligation to "verify the legal status of the legal person" and "verify the identity of the beneficial owner of the legal person". In most cases an excerpt from the Commercial Register, or even a self-declaration by the customer, seemed to satisfy the DNFBP's requirements, regardless of how many shareholders may be present and whether a name may be available on the shareholder list. There was also a universal focus on ownership rather than control, such as when no one person held at least 25 percent, that any one shareholder would meet the requirement, or that there would be no further research on the identity of the beneficial owner. Finally, most of the representatives of the private sector met by the authorities expressed difficulty to implement requirements related to politically exposed persons, only a small number of important DNFBPs have access to external PEPs databases, or have sufficient resources to perform in-house research.

Casinos

1101. Based on the meeting with the casino supervisor and the supervisee, preventive measures appear implemented and specific risks mitigated. The casino managers of the 14 branches of the state monopoly casino are responsible for the implementation of the effective measures in their branch. In addition, there is a dedicated AML function at the headquarter level in charge of ensuring the group's compliance. When certificates of winnings or checks are issued, specific controls are performed on the origin of the funds and behavior of the client. In 2008, 110 checks have been issued for EUR3.8 million, and in 2009 120 checks have been issued for EUR7.4 million. It is possible to hold an account at the casino. Preventive measures for financial institutions apply for this service. This possibility is mostly used by frequent poker players. Based on internal rules, deposits and withdrawals to/from these accounts have to be made from/to the same account holders. It is possible for a company to hold an account. This is specifically the case of companies sponsoring poker players. There are approximately 100 accounts open with a current total deposit of EUR3 million.

1102. Discussion with the private sector indicated suspicions of the existence of internet casinos operating illegally from the Netherlands, and that this situation has been brought to the attention of the

supervisor and prosecutors. The net operating profit from the State monopoly fell in 2008 with 83.3 percent to EUR14.3 million (2007: EUR85.6 million). This is attributed to the impact of the crisis, the implementation of anti-smoking law, and online gambling.

Real estate agents

1103. The implementation of the CDD measures by real estate agents is supported by their professional associations. It is not mandatory for a real estate agent to join an association, but only 1 000 out of the 7 000 agents are not member of one of the three associations. The main association, NVM, has raised awareness of its 4 200 members through a comprehensive section of its website on AML/CFT, Articles in professional journal and organization of presentations. The common view from real estate agents met by the assessors was that the risks for their profession are limited because at the end the notaries will always have to perform CDD measures. But there was also recognition that the real estate agents may have access to information that a notary may not necessary have and that could lead to suspicions in relation to the beneficial owner or the speed and conditions of the transaction.

Dealers in precious metals and dealers in precious stones

1104. While the knowledge of the AML/CFT requirements appears more limited than for other professions in part due to the fragmentation of the profession in different types of businesses, meetings with the supervisor, professional associations, and representatives of the sector that the number of transactions in cash above the EUR15 000 are very limited in the Netherlands. Potential risks were mentioned in relation to the development of e-commerce in precious metals and stones, and the major role a Dutch financial institution has in the financing of diamond trade worldwide. But the former is not covered by the standards and the latter is covered by the preventive measures for financial institutions.

Lawyers

1105. According to meetings with the Dutch bar association and lawyers, most of the lawyers in the Netherlands do not perform services listed by the FATF. Based on a questionnaire sent to lawyers in 2006, it is estimated that only one third perform services listed by the FATF. The effective implementation of CDD requirements by lawyers is supported by the work of the Dutch bar association. The association has issued guidelines on the implementation of the WWFT, and a by-law on administration and financial integrity issued by the Bar Association which, as indicated in relation to R.5 above adds requirements additional to the WWFT. The internal controls performed by the bar association, detailed in the description for R.24, support the effective implementation of the CDD requirements by lawyers. Based on inspections performed, the Bar association estimated that 89 percent of the lawyers were implementing all the requirements.

Notaries

1106. According to the meeting with the Royal notarial association, most of the acts performed by notaries in the Netherlands are in the perimeter considered by the FATF. Out of the 1.4 million deeds drafted by notaries, approximately 75 percent are related to real estate transactions. The effective implementation of CDD requirements by notaries is supported by the work of the Royal notarial association. Guidelines have been issued to assist notaries in implementing the WWFT and, based on a peer review mechanism, each office is assessed every three years. The notary met by the assessors was implementing a risk based approach to its customers. Approximately 5-10 percent of the customers are categorized high risk, based on the nature of the services requested or their country of origin. This categorization leads to the request of additional information, more extensive looking at annual reports regarding legal persons, and enhanced ongoing monitoring of the relationship.

Accountants

1107. The implementation of CDD requirements by accountants is supported by the work of the two professional associations, NOVAA and NIVRA, which have issued guidelines to assist their members in implementing the WWFT. While accountants are subject to the AML/CFT framework for all their operations, they prepare for or carry out three of the activities listed by the FATF standards: the management of bank, savings or securities accounts; the organization of contribution for the creation, operation or management of companies; and the creation, operation or management of legal persons or arrangements and buying or selling of entities. NOVAA and NIVRA have a peer review mechanism which includes a one-day onsite visit of each accountant every six years. The time dedicated to the implementation of the AML/CFT was estimated to approximately 30 minutes. Compliance with the standard appears easier for large accounting firms than smaller offices. Some large firms have central client acceptance teams performing checks, using risk assessment tools and able to identify politically exposed persons.

TCSPs

1108. Regarding TCSPs: Even if the current legal framework regarding the CDD requirements presents some weakness, it has to be noted that up to the introduction of the Wwft as per 1st of August 2008, there was an explicit obligation for trust offices under the WID to identify and verify the identity other than the beneficial owner, or the person purporting to act on behalf of the customer is so authorized. The DNB informed the assessors that, based on its supervisory practice, trust offices identify the representative of the beneficial owner and verify that he/she is authorized to do so (by filing of a written authorization prepared by the beneficial owner). This practice was confirmed in meetings with representatives of the TCSPs.

1109. In general, the clients (beneficial owner) are referred to trust offices by Dutch tax advisors, notaries, or by overseas liaised trust offices.

1110. While the general findings above apply to TCSPs, the implementation of CDD measures is supported by the awareness raising work done by professional associations, and benefits from having been subject to AML/CFT preventive measures for a longer time than other DNFBPs.

4.1.2 Recommendations and Comments

1111. Customer due diligence measures in place are generally elaborated and effectively implemented. In this regard, the situation in the Netherlands is particularly advanced in comparison with assessments of similar jurisdictions. Nevertheless, compliance with Recommendation 12 is difficult to achieve as it is assessed against 6 other recommendations (R.5, 6 and 8–11), making a total of 35 essential criteria, not counting sub-criteria, to be applied to 7 types of businesses and professions.

1112. In order to comply fully with Recommendation 12, the authorities should:

Extend the scope of the CDD requirements to:

- Both the buyer and the seller of a transaction performed by a real estate agent.
- The services designated by the WWFT for lawyers and notaries, when related to the first meeting with the client. This requirement should be set out in primary or secondary legislation.
- TCSPs when providing a registered office; business address for a company, a partnership or any other legal person or arrangements, when this service is provided on a standalone basis.

With respect to Recommendation 5

All DNFBPs

- Provide further guidance on all CDD measures.

All DNFBPs (except TCSPs)

The recommendations made in section 3 for financial institutions also apply to DNFBPs (except TCSPs).

TCSPs

Adopt measures consistent with the standards regarding the identification of the customer other than the beneficial owner and enhanced due diligence.

With respect to Recommendation 6, 8, 9 and 11

- The recommendations made in section 3 for financial institutions also apply to DNFBPs.

With respect to Recommendation 10

All DNFBPs (except TCSPs)

- Remove the ambiguity created by the different and conflicting record-retention provisions in the AW, BWR and the WWFT, and make explicit that the record-retention requirements necessarily apply to all transactions and to business correspondence, account files, customer identification on all legal persons and arrangements and beneficial owners.

- Ensure that records of transactions are maintained in a way that permits reconstruction of transactions for the purpose of prosecution.

- Give the authorities the power to extend the retention period if necessary in particular cases.

TCSPs

- Ensure that record keeping requirements on information on the customer (if different from the beneficial owner) and business correspondence, are kept for five years from the date the relationship with the customer ceases.

4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
R.12	**PC**	All DNFBPs (except TCSPs) • The shortcomings identified under Recommendation 5 and 10 in section 3 also apply. All DNFBPs • The shortcomings identified under Recommendation 6, 8, 9 and 11 in section 3 also apply. Effectiveness issues. Real estate agents • CDD required only on one party to the transaction is covered, not both the buyer and the seller. Lawyers and Notaries • Exemption of CDD requirements in relation to the first meeting with the client.

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
		TCSPs • No requirements for providing a registered office; business address for a company, a partnership or any other legal person or arrangements, when this service is provided on a standalone basis. • No requirements in relation to the identification the customer other than the beneficial owner, and enhanced due diligence. • No indication to when the retention period should start for records of customer information (if different from the beneficial owner) and business correspondence.

Indicative table of compliance with Recommendation 12 by type of DNFBPs

1113. In order to enable better fine-tuning of the risk-based system, and to take into consideration the specificities of each business and profession, the following compliance breaks down the ratings by different types of DNFBPs.

DNFBP	Indicative rating	Rationale
Casinos	PC	Compliance with some of the essential criteria. Indications of effective implementation.
Real estate agents	PC	Compliance with some of the essential criteria. Implementation varies across the profession. Shortcomings regarding the scope of the activity subject to CDD measures.
Dealers in precious metals and dealers in precious stones	PC	Compliance with some of the essential criteria. Implementation varies across the profession.
Lawyers	PC	Compliance with some of the essential criteria. Indications of effective implementation
Notaries	PC	Compliance with some of the essential criteria. Indications of effective implementation
Accountants	PC	Compliance with some of the essential criteria. Implementation varies across the profession.
TCSPs	LC	Large majority of the essential criteria are fully met. Indications of effective implementation Minor shortcomings regarding the scope of TCSPs.

4.2 Suspicious Transaction Reporting (R.16)

4.2.1 Description and Analysis

Legal Framework:

1114. The reporting requirements are set out in Articles 15 and 16 WWFT. Implementing elements are contained in Article 4 and the annex of the UBWWFT. Sanctions are provided in Articles 26 and 27 of the WWFT.

Requirement to Make STRs on ML and TF to FIU (c.16. 1):

1115. Most of the requirements described under Recommendation 13 and Special Recommendation IV for financial institutions also apply to DNFBPs. With exception of lawyers and notaries, the reporting obligation regarding subjective UTRs, which are similar to STRs as defined by the FATF, are the same for FIs and DNFBPs. The specificities of the reporting obligation are indicated below, including the existence of specific objective indicators for reporting UTRs, which do not fall in the scope of STRs as envisaged in Recommendation 13 and 16, but may prompt an analysis leading to a subjective UTR.

Casinos

1116. In addition to the general reporting requirements described in section 3, Casinos have to report UTRs based on three objective indicators, as indicated in the annex to the UBWWFT. These objective indicators are:

- Acceptance on deposit of coins, banknotes or other assets worth EUR15 000 or more.
- Funds transfers of EUR15 000 or more.
- Sale to a customer of chips with an equivalent value of EUR15 000 or more in exchange for checks or foreign currency.

Dealers in precious metals and dealers in precious stones

1117. Pursuant to the annex to the UBWWFT, an objective indicator for reporting UTRs applies to dealers in high value goods, and consequently to dealers in precious metals and dealers in precious stones. These professions should report any transaction in which precious stones or precious metals are sold in full or partial exchange for cash, whereby the applicable threshold is EUR15 000 or more.

Real estate agents, accountants, trust offices

1118. According to the annex to the UBWWFT, real estate agents, accountants and trust offices have to report transactions based on an objective indicator when EUR15 000 or more is paid to or through the agency of the professional in cash, by means of bearer checks or by means of similar payment instruments.

Lawyers and notaries

1119. The objective indicator referred above in relation to real estate agents, accountants and trust offices also applies to lawyers and notaries. In addition, based on Article 1 (2) WWFT, the requirement to report subjective UTRs does not apply to lawyers and notaries when they perform activities for a client in relation to legal proceedings or in relation to the first meeting with the client (for an analysis of these concepts in the Dutch context, see the legal framework for section 4). The exemption of the reporting requirement in relation to the legal privilege is consistent with the framework provided by the FATF in the relevant note to the methodology. While the involvement of lawyers in legal proceedings fully justifies the exemption, its rationale is less evident in the case of notaries which are not directly involved in legal proceedings in the Netherlands.

Role of the Self-Regulatory organization in relation to STRs (c.16.2):

1120. Lawyers, notaries and accountants are monitored by self-regulatory organizations (SROs) but are not allowed to send their UTRs to a SRO. According to Article 16 WWFT all financial institutions and DNFBPs have to send UTRs to the FIU.

Application of R.14, 15 and 21 to DNFBPs (c.16.3):

Recommendation 14

1121. Most of the requirements described under Recommendation 14 for financial institutions also apply to DNFBPs, with the differences indicated below:

Lawyers, notaries, and accountants

1122. Pursuant to Article 23 (3) WWFT, the general prohibition to disclose that a UTR has been reported or other information been provided to the FIU does not apply to lawyers, notaries and accountants when this aims at causing the customer to refrain from an illegal act. The exemption of Article 23 (3) WWFT does not refer to the possibility to disclose to the customer that a UTR has been reported. Instead, the notification may only state that the customer's activity is illegal and that the customer is advised not to carry out this activity.

Notaries, real estate agents, dealers in precious metals and stones, TCSPs

1123. Unlike financial institutions and other DNBFPs, part of the waiver to the general prohibition to disclose in Article 23 (4) does not apply to notaries, real estate agents, dealers in precious metals and stones and TCSPs. These non-financial businesses and professions are not allowed to disclose that they have reported a UTR or provided information to the FIU to an institution outside the European Union, even if this institution belongs to the same category of business or profession.

Recommendation 15

1124. The key legislative provisions on controls are in the Wft, which only applies to financial institutions. Consequently most of the analysis and description of Recommendation 15 for financial institutions does not apply to DNFBPs. Article 35 WWFT imposes a direct obligation to ensure that employees are familiar with the provisions of the Law. But this obligation does not make it a requirement to inform staff of the nature of any internal controls and systems. Regarding lawyers, Article 11 (a) of the by-law on administration and financial integrity obliges lawyers to have internal procedures in place to implement the AML/CFT rules.

1125. Article 35 WWFT also requires that employees are trained to enable them to recognize unusual transactions. According to the explanatory memorandum to the WWFT on Article 35, the training should serve to teach the employees concerned how to act if they come across an unusual transaction in the course of their duties. But there is no mention of ongoing training and training on CDD measures. In addition, there are no general provisions, based on the risk of ML/FT and the size of the business, requiring DNFBPs to establish and maintain internal procedures, policies and control to prevent ML and FT, and to communicate these to their employees. There is also no requirement to maintain an independent audit function to test compliance with these procedures, policies and controls. Finally there is no requirement to have screening procedures in place to ensure high standards when hiring employees. The legal framework on internal controls set out in the Wtt is more developed for TCSPs.

TCSPs

1126. In addition to the few requirements set out in the WWFT and applicable to all DNFBPs, there are a number of requirements pertaining to internal control in the Rib Wtt. Pursuant to Article 7 Rib Wtt, the trust offices shall have an up-to-date procedures manual containing:

- Procedures on compliance with the rules laid down in the Wtt, as well as in the WMOT and the WID (which were the legal basis for the AML/CFT framework until August 2008), and the Sanctions act.
- Documentation of duties, responsibilities and authorities of the management and employees such that there is segregation of duties between positions with an operational and a checking nature.
- Procedures on handling of and requirements for employees in integrity-sensitive positions.

- Procedures on handling incidents.
- Internal control procedures for establishing that the trust office is performing its activities in accordance with the provisions of the Rib Wtt, and the provisions of the procedures manual.

1127. Article 8 Rib Wtt contains provisions requiring trust offices to put in place screening procedures to ensure high standards when hiring employees. It includes the verification of the identity, the verification of the accuracy and completeness of the information and references provided an assessment with evidence of the integrity of the person, and an assessment of this integrity in relation to holding an integrity-sensitive position at a given level. The trust office should keep records of these verifications and assessments. The trust office has to apply objective and transparent criteria for classifying a position as one that entails a material risk to sound operational management by the trust office. Pursuant to Article 9 Rib Wtt, a trust office is also required to assess the integrity of persons who undertake to perform activities in an integrity-sensitive position for the trust office other than under an employment contract.

1128. While the legal framework in place regarding internal controls in TCSPs is much more developed than for other DNFBPs, there is still the absence of a clear requirement of an independent audit function to test compliance with the procedures, policies and controls.

Recommendation 21

1129. The description and analysis under Recommendation 21 for financial institutions (section 3) also apply to DNFBPs.

Analysis of effectiveness (R.16) and statistics (R.32)

1130. Overall the number of SUTRs from the DNFBPs is in constant progression and the average amounts involved in each reported transactions are quite high, especially in comparison with SUTRs reported by the financial sector. In 2009, the average suspicious transactions amounted to more than EUR400 000 for DNFBPs, to compare with EUR8 000 for financial institutions (with approx. EUR150 000 for SUTRs by banks). It is interesting to note that, in 2009, SUTRs by DNFBPs amounted to 28 percent of the total number of SUTRs received by FIU-NL from reporting entities designated by the FATF.

Subjective UTRs received by type of DNFBP (number, amount, ratio)									
	2007			2008			2009		
Type of DNFBP	Amount	SUTRs	Ratio	Amounts	SUTRs	Ratio	Amounts	SUTRs	Ratio
Casinos	4 096 000	414	9 894	6 772 000	538	12 587	6 812 000	510	13 357
Real estate agents	665 000	2	332 500	0	0	0	1 450 000	3	483 333
Dealers in precious metals and stones	231 000	7	33 000	69 000	2	34 500	106 000	4	26 500
Lawyers	544 000	5	108 800	4 198 000	16	262 375	750 000	15	50 000
Notaries	376 895 000	339	1 111 785	408 922 000	594	688 421	153 119 000	338	453 015
Accountants	95 177 000	84	1 133 059	35 106 000	112	313 446	433 580 000	578	750 138
TCSPs	15 006 000	3	5 002 000	2 970 000	4	742 500	1 097 000	5	219 400
Total	**492 614 000**	**854**	**576 831**	**458 037 000**	**1 266**	**360 943**	**596 914 000**	**1 453**	**411 665**

Note: Amounts in Euro

1131. The performance of the DNFBP sector in relation to the number of suspicious transactions reports from financial institutions is quite good in the Netherlands in comparison with similar economies, as indicated in the table below.

Cross-country comparison of STR reporting (DNFBPs)				
Country	**2007**	**2008**	**2009**	**STRs/Billion GDP (2009)**
The Netherlands[1]	854	1 266	1 453	1.8
Belgium	184	160	179	0.4
Canada	366			0.3
Italy	215	173	136	0.1
Spain[2]	296	308	256	0.2

[1] Subjective UTRs.
[2] STRs from the transportation of funds' sector and art dealers are not included here.

1132. While the level of reporting is high compared to other jurisdictions, it is mostly concentrated on three DNFBPs: casinos, notaries and accountants making more than 98 percent of the total. Based on meetings with the private sector, the spike in the number of reports by accountants in 2009 may be related to the ongoing tax amnesty. While the level of reporting of notaries is relatively high, until 2009 it was considerably lower for real estate agents involved in similar transactions.[95] The sharp increase in the number of STRs in 2010 appears logical both in the context of the risks and of the awareness raising campaigns from the professional associations and the supervisor. Based on the information received on the limited use of cash in the purchase or sale of precious metals and stones it is expectable that these businesses would report less than others. But the reporting has been particularly low raising questions on the awareness of the profession. Finally, the number of reports by TCSPs is very low having in mind that special financial institutions (SFI)-related flows were estimated to EUR4 500 billion in 2007, or more than five times the GDP. In addition, a 2006 study commissioned by the Dutch Ministry of Finance pointed out that "some of the experts expressed that they would not be surprised if 1 percent of SFI transactions are used for money laundering".[96] An explanation for this low level or reporting may be related to the weaknesses previously identified regarding the identification of the beneficial owner and the access of information on PEPs.

1133. Despite the absence of provisions in the WWF requiring internal controls, in practice accountants, lawyers and notaries have introduced measures to this extent based on international professional standards or regulations by the relevant SROs. While these measures could not be considered as enforceable means, they contribute to encourage the establishment of internal controls.

1134. Concerning internal controls for TCSPs, Article 7.1b of the Rib requires trust offices to have up to date procedures manual, that contains documentation of duties, responsibilities and authorities of the management and employees such that there is segregation of duties between positions with an operational and control nature. Therefore, a very small trust office (one person office) needs to hire a person for the compliance function (*i.e.* external compliance officer) in order to comply with this requirement. In practice, these small trust offices hire a company specialized in compliance function for trust offices to perform such activities. This company performs this function for about 40 small trust offices in the Netherlands. The big trust offices that perform global activities usually have an independent compliance function and internal audit function.

4.2.2 Recommendations and Comments

1135. In order to comply fully with Recommendation 16, the authorities should:

95 43 SUTRs have been received from real estate agents from January to October 2010.
96 B. Unger *et al*, "The amounts and the effects of money laundering," February 16, 2006, p. 11.

With respect to Recommendation 13

- Extend the scope of the reporting requirement to:
  - Both the buyer and the seller of a transaction performed by a real estate agent.
  - TCSPs for providing a registered office; business address for a company, a partnership or any other legal person or arrangements, when this service is provided on a standalone basis.
- Ensure that suspicious transactions are reported promptly to the FIU.
- Enhance the effectiveness of the reporting system.
- Keep statistics on suspicious transactions reports related to the financing of terrorism.

With respect to Recommendation 14

- Ensure that protection from criminal liability only applies if suspicions are reported in good faith.
- Ensure that demonstrating good faith is sufficient to be protected from civil liability, without having to prove that disclosure has reasonably been made in view of all facts and circumstances.
- Extend the tipping-off provision to cover cases where transactions are being reviewed internally to determine whether an STR should be filed.

With respect to Recommendation 15

All DNFBPs (except TCSPs)

- Require DNFBPs to develop internal policies, procedures and controls (except lawyers).
- Require DNFPBs to establish an appropriate ongoing employee training.
- Introduce the requirement of an independent audit function to test compliance with the procedures, policies and controls.

TCSPs

- Introduce the requirement of an independent audit function to test compliance with the procedures, policies and controls.

With respect to Recommendation 21

- Re-introduce practice of issuing detailed circulars to reporting entities after each FATF Plenary.
- Introduce an enforceable obligation for DNFBPs to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations.
- Introduce enforceable provisions for the application of countermeasures in the case in which a country continues not to apply or insufficiently applies the FATF Recommendations.

4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors underlying overall rating
R.16	**PC**	All DNFBPs • The shortcomings identified under Recommendation 13, 14 and 21 in section 3 also apply to DNFBPs. All DNFBPs (except TCSPs) • No requirement of internal policies, procedures and controls (except lawyers). • No requirement to establish an appropriate ongoing employee training. • No obligation of an independent audit function to test compliance with the procedures, policies, and controls. Real estate agents • Reporting requirement only in relation to one party to the transaction, not both the buyer and the seller. Lawyers • Inadequate awareness of potential ML vulnerabilities contributing to underreporting. TCSPs • No reporting requirements for providing a registered office; business address for a company, a partnership or any other legal person or arrangements, when this service is provided on a standalone basis. • Inadequate awareness of potential ML vulnerabilities contributing to underreporting.

Indicative table of compliance with Recommendation 16 by type of DNFBPs

1136. In order to enable better fine-tuning of the risk-based system, and to take into consideration the specificities of each businesses and professions, the following compliance breaks down the ratings by different types of DNFBPs.

DNFBP	Indicative rating	Rationale
Casinos	PC	Compliance with some of the essential criteria. Indications of effective implementation
Real estate agents	PC	Compliance with some of the essential criteria. Shortcomings regarding the scope of the activity subject to CDD measures.
Dealers in precious metals and dealers in precious stones	NC	Compliance with some of the essential criteria. Lack of effectiveness
Lawyers	NC	Compliance with some of the essential criteria. Lack of effectiveness
Notaries	PC	Compliance with some of the essential criteria. Indications of effective implementation
Accountants	PC	Compliance with some of the essential criteria. Indications of effective implementation
TCSPs	PC	Large majority of the essential criteria are fully met. Lack of effectiveness

4.3 Regulation, Supervision, and Monitoring (R.24-25)

4.3.1 Description and Analysis

Legal Framework:

1137. The framework for regulation, supervision and monitoring for DNFBPs is set out in the WWFT, the BATWWFT, the Wtt, the Rib Wtt, and the Games of chance act.

Regulation and Supervision of Casinos (c. 24.1, 24.1.1, 24.1.2 & 24.1.3):

1138. Casinos fall within the scope of the WWFT (Article 1 (a) (16) WWFT) and therefore have to comply with all the requirements of that law. The supervisory authority is the Dutch National Bank (DNB). Within DNB there is a special designated unit that is responsible for (among other institutions) casino's. As indicated before, The Games of Chance Act does not allow internet casinos. When providing financial services, casino's also fall within the scope of the Wgt (for money exchange activities) and of the Wft (for the deposits held). Their regulation and supervision is analyzed under section 3 on the preventive measures for financial institutions. The issue of gaming halls is discussed under R.12. While there are no AML/CFT regulation and supervision for gaming halls, the legal framework in place limits the ML/FT risks.

Designated competent authorities for regulation and supervision

1139. The DNB is the designated competent authority for the AML/CFT supervision of casinos pursuant to Article 1 (1) (a) BATWWFT in conjunction with Article 24 (1) WWFT. In this respect the DNB has the same powers to monitor and sanction casinos as described in section 3.

Licensing of casinos

1140. Pursuant to Article 1 (a) of the Games of Chance Act, it is not permitted to compete for prizes or premiums if the winners are selected by any determination of chance on which the participants cannot exert an influence, unless a permit has been ***issued according to*** the Games of Chance Act. At present, the Games of Chance Act does not provide for the granting of permits to organize games of chance via the internet, and so called e-casinos are therefore prohibited. There is only one organization in the Netherlands that is licensed under the Games of Chance Act: Holland Casino. This license is granted by the Minister of Justice (see Article 27h Games of Chance Act). In the *"Beschikking Casinospelen*" requirements are laid down (on the basis of the Games of Chance Act) such as the maximum numbe**r** of establishments or the net profit that must be remitted to the State.

Measures in place to prevent criminals from controlling or operating casinos

1141. The Dutch Games of Chance Act (*Wet op de kansspelen*) states that only one operator can be licensed to exploit casino games in the Netherlands (gaming monopoly) and that all the benefits of casino games are destined for the State budget (Article 27h Games of Chance Act).

1142. Article 3 (3) of the *Beschikking Casinospelen* (the license of Holland Casino) states that de Minister of Finance appoints the chairman and the members of the Supervisory Board. The Minister of Finance has a preliminary consultation with the Minister of Justice. Article 3 (4) states that the Supervisory Board appoints the Board of Directors. The appointment offer has to be notified to the Minister of Finance and the Minister of Justice. Article 6 (1) of the *Beschikking Casinospelen* states that Holland Casino has to take all necessary measures and provisions to guarantee an honest course of the game and that Holland Casino has to take all necessary measures to prevent fraud and abuse. The appointment of the Board of Directors will only take place when the Minister of Finance has not objected to this appointment within eight weeks of notification. During this eight week period, the Minister of Finance will research the background of the candidates in cooperation with the Minister of Justice.

Analysis of effectiveness (R. 24 Casinos)

1143. The supervision of casinos represents one of the functions of the DNB supervisory team for casinos, bureaux de change, payment institutions (money transfer offices) and trust and company service providers. The Unit counts 12 FTE and two FTE are dedicated to the supervision of Holland casino's

gaming activity. Onsite visits are conducted yearly, and no sanction has ever been pronounced against Holland Casino based on the AML/CFT legal framework.

1144. Despite the low level of supervisory resources, and based on interviews with the supervisors and the licensee, the current supervisory arrangements appear effective for the following reasons: i) the risks of ML/FT are limited by the CDD measures in place; ii) the gaming monopoly and the control of the Minister of Finance over Holland's casino supervisory board gives strong incentives to mitigate the reputational risk; and iii) internal controls appear developed and effective.

1145. While the supervision of the licensed casino appears effective, the lack of resources deprives the authorities to adequately fight against illegal gaming activities. Anecdotal evidence and professionals met by the assessors indicate that internet casinos are currently operating (mind and management) from the Netherlands.[97] This was confirmed by the authorities who indicated that a number of measures have been taken to combat illegal internet gambling. This includes the development by the police of a search tool to detect illegal internet gambling operators and intermediaries, investigation of internet gambling operators, communication to the Dutch association of banks of a black list of operators which violate the Games of Chance Act, and engagement with internet providers.

Monitoring Systems for Other DNFBPs (c. 24.2 & 24.2.1):

1146. A supervisory authority has been designated for all DNFBPs. According to Article 24 (2) WWFT, the designated supervisors can exercise supervision in a risk-oriented manner. Each designated supervisor is entrusted with rights and duties based on the Awb. The WWFT gives supervisors the authority to sanction breaches of the WWFT. The table below summarizes the powers of the DNFBPs supervisors on the basis of the Awb and the WWFT. Note that Articles 26 and 27 do not apply to professions that are subject to disciplinary law (lawyers, notaries and accountants).

Supervisory powers	Legal basis
Enter every place, with the exception of a private home	5:15 Awb
Require the provision of information	5:16 Awb
Require inspection of business information and documents, make copies or to take along the information and documents	5:17 Awb
Inspect and measure goods, take samples, open packages or to take along	5:18 Awb
Stop and inspect means of transport that are subject to supervision, cargo thereon, documents related	5:19 Awb
Issue an instruction in order to adhere the institution to a particular line of conduct in respect of the development of internal procedures and controls to prevent money laundering and terrorist financing and the training of employees	32 WWFT
Impose incremental penalty payments	26 WWFT
Impose administrative fines	27 WWFT

1147. On the basis of Article 5:20 (1) Awb everyone is obliged to cooperate fully with a supervisor. Powers to perform sanctions are based on the WWFT and are the same as those for financial institutions, as described and analyzed for Recommendation 17 under section 3.

Real estate agents and dealers in precious metals and stones

1148. Pursuant to Article 1 (d) BATWWFT, the BHM is the designated supervisor for real estate agents and dealers in precious metals and stones. The latter have been subject to AML/CFT supervision since 2001, and the former since 2003. The present staff of BHM consists of 26.1 FTE (Full Time Equivalent). Of this 26, 1 FTE, 20.8 FTE carry out supervisory activities and 2 FTE are dedicated to enforcement issues. The staffing should increase in 2010 to reach a total of 35 FTE's. The total budget of the BHM was

97 As indicated above, the authorities are considering legalization of online poker.

approximately EUR1.5 million in 2009. In addition to the 8 500 real estate agents and 4 800 precious metals and stones dealers, the BHM is supervising 56 800 other professionals (mostly institutions involved in the sale of vehicles and works of arts).

1149. In 2008, BHM developed an enforcement policy for the period 2009–2012 *("Visiedocument 2009-2012"*). Supervision, as described in this policy, is based on a more tailored approach and focus much more on current developments and risks in the field. The approach does not only rely upon repressive instruments but also on pro-active supervision and communication strategy. Subsequently, in the annual plans for 2009 and more in particular 2010 a clear risk-based audit approach was introduced. The selection of on-site inspections is mainly based on earlier detected breaches of the WWFT, information received from FIU-NL or law enforcement agencies, or specific risk patterns.

1150. The BHM develops thematic inspections based on identified risks. Among all the professions supervised by the BHM, the precious stones, metals, jewelry and jewels branch was subject of increased supervision in 2008. Approximately 50 inspections were carried out in this sector. The BHM concluded that the awareness of the AML/CFT legislation in this type of business is significant. Mostly because of the information and guidance provided by the professional organizations. The number of breaches detected during these inspections was low.

1151. The staff of BHM follows courses (internally and externally) on a regular basis and on different areas. This can be a general course like Accounting or Auditing but also a course for specific professional expertise like Money Laundering and Financial Investigation.

Analysis of effectiveness

1152. Between 2007 and 2009, the large majority of inspections performed by the BHM (80 percent) have been directed towards professions that are not considered DNFBPs by the FATF. But the situation is evolving, especially for the real estate agents that made 34 percent of the inspections in 2009. The share of inspections of dealers in precious metals and stones was still low, at around 4 percent of the total. The table below summarized the number of inspections on the DNFBPs supervised by the BHM and their results for the period 2007–2009.

	2007		2008		2009	
	Real estate agents	Dealers in precious metals	Real estate agents	Dealers in precious metals	Real estate agents[1]	Dealers in precious metals
Total number of inspections	0	0	9	47	262	31
No breaches/ Minor breaches without warning	0	0	9	44	262	23
Detected breaches (finally) concluded with a warning	0	0	0	2	0	1
Administrative fines	0	0	0	0	0	0
Incremental penalty payments	0	0	0	1	0	1
Reported for criminal investigation	0	0	0	0	0	6

[1] The main goal of these visits was to provide guidance with regard to the obligations that real estate agents have under the Money Laundering and Terrorist Financing Prevention Act and to make them aware of transactions that should be categorized as "unusual".

1153. While the recent increase in STRs reported by real estate agents may be an early sign of an effective monitoring system of the sector, monitoring of dealers in precious metals and stones still appears to be underdeveloped, both in terms of number of inspections and impact on the reporting behavior.

Lawyers, Notaries and Accountants

1154. Pursuant to Article 1 (c) BATWWFT, the BFT is the designated supervisor for lawyers, notaries and accountants. The BFT is an autonomous administrative authority incorporated by the Notaries' Act. The origins of the BFT dates back to the 1930s when the BFT was established to supervise the notaries' third party bank accounts. The original and existing task of the BFT is financial supervision of civil-law notaries and court bailiffs. The supervision includes that the civil-law notary and/or court bailiff do not use third party funds for private goals.

1155. In addition to 4 500 notaries, 15 547 lawyers and 18 860 accountants, the BFT also supervises 10 800 tax advisers and 10 000 other independent legal advisers and finance economic advisers. This represents a total of more than 50 000 professionals (approximately 32 500 offices). The BFT has 37 employees. Of these 37 employees, around 15 carry out AML/CFT supervision. The employees who carry out this supervision have an accountancy or legal background. Furthermore, the BFT has an information analyst who supports the department for supervision of AML/CFT. The majority of the staff has an (post) academic background. The personnel of the BFT follow courses (internally and externally) on a regular basis on different areas. The majority of the personnel working on the department for supervision of AML/CFT followed a post graduate course on Forensic Accountancy. The budget of the BFT dedicated to AML/CFT supervision was approximately EUR2.2 million in 2009.

1156. In order to investigate whether the professionals comply with AML/CFT legislation, the BFT performs regular and risked-based inspections. For 2006, 2007, and 2008, the BFT focused on civil-law notaries (in particular concerning the risk of money laundering in the real estate sector). For 2009, the BFT focused on forensic accountants. The BFT prepares project plans (including contemplated numbers of inspections). These project plans are shared and discussed with the Ministry of Justice. On a regular basis, this supervisor reports to the Ministry of Justice and frequently meetings are held. The BFT also publishes annual reports.

1157. The BFT is implementing a risk-based supervision model. Due to the number of DNFBP under supervision (approximately 50 000) and number of supervisors, the BFT focused on organized professionals *e.g.*, professionals that are members of a professional organization. The ultimate goal is to create a framework of supervision per category of professionals. By conducting an arrangement with the professional bodies, the quality of the professional services (*e.g.*, Netherlands Bar Association, NIVRA, etc.) is improved and also facilitates self compliance. In addition, the BFT has more capacity to focus on risk-based transactions. Part of the arrangement is that BFT trains internal auditors and advises on internal guidance-papers/electronic training programs. The BFT considers that the professional organizations should be the first gatekeeper and internal supervisor. Hundreds of peer reviews (non-risk based) are conducted annually by the professional organizations (Bar Association (200), Notaries (300), Tax advisors (CB: 50), Administrative service providers (NOAB: 100)). Although BFT cannot check the quality of the results of the Bar Association and Notaries in detail, some results are good (one notary quit his job because of the KNB-audit).

1158. Civil-law notaries, attorneys at law, and accountants are subject to disciplinary law that governs their professional conduct. Consequently, Articles 26 (2) and 27 (2) WWFT exclude the possibility of imposing an order for incremental penalty payments or an administrative fine to these professionals. Civil-law notaries are by law member of the Royal Dutch Notarial Society. Attorneys at law are by law member of the Netherlands' Bar Association. Public chartered accountants are by law member of the

NIVRA: a body governed by public law, appointed by the government. Public chartered accountants-business administration consultants: are by law members of the NOVAA a body governed by public law, appointed by the government.

1159. Civil-law notaries and lawyers may invoke Article 5:20 (2) Awb in relation to professional secrecy and decline to open their books. It is on this basis that lawyers currently refuse AML/CFT supervision by the BFT.

1160. With respect to the supervision of civil-law notaries, it is worth mentioning however, that the BFT can request an investigation with the disciplinary judiciary (Article 96 of the Notaries' Act). The disciplinary judiciary orders on request such disciplinary investigation. The BFT acts in such situations as an expert on behalf of the judiciary. In these cases, the BFT can also file a disciplinary complaint against a civil-law notary. In this type of procedures, the civil-law notary cannot invoke Article 5.20(2) Awb and try to decline to open his books. In addition, the Royal Dutch Notarial Association monitors compliance with the WWFT on behalf of the BFT in its mandatory peer review system.

Analysis of Effectiveness

1161. As mentioned before, BFT carries out regular and risk-based inspections. The tables below show the results of these (general) regular inspections with accountants, business providers, tax advisers and the risk-based inspections with civil-law notaries. From 2006 till 2008, BFT focused on this specific group because of significant AML risks in the real estate sector.

Year	Number of regular inspections of accountants, business providers, tax advisers	Number of risk-based inspections of civil-law notaries	Number of inspections of lawyers	Disciplinary proceedings initiated
2007	13	9	0	12 notaries
2008	38	9	0	9 notaries 1 accountant
2009	43	7	0	Cases pending

1162. The Royal Dutch Notarial Association monitors compliance with the WWFT on behalf of the BFT in its mandatory peer review system. By December 2009, almost two thirds of all firms had undergone a peer review: 562 of the total number of 850 firms. In 98 reviews, improvements were required, almost all concerning administrative issues in complying with the WWFT. In 2009, a few notaries have been suspended or expelled.

1163. The BFT applies the risk based approach on supervision due to the focus on certain group of professionals that constitute a higher risk on money laundering. In the years 2005 up to and including 2008 the BFT focused on notaries with real estate transactions for which a high risk on money laundering exists. Within accountants a selection was made on specific high risk professionals: forensic accountants and similar business advisors/providers The BFT has also recently performed risk based investigations of notaries and accountants based on information supplied by the public prosecutor.

1164. For notaries, the BFT created a risk based approach in order to investigate the so called ABC transactions with real estate: selling real estate from A to B to C in a short time period (usually within 6 months) to obtain extra ordinary capital gains or losses with no apparent legitimate business, economic, tax or legal reason. The BFT also investigated transactions that may include mortgage fraud (individuals or groups that try to obtain a (higher) mortgage/ loan under false pretences such as falsified income data, false valuation reports or fake identity papers). The BFT requested the FIU-NL to investigate the effectiveness of the unusual transactions reported by the notaries, in particular the 464 ABC transactions that were selected by the BFT in 20 special investigations that were performed in the last five years by BFT. In

443 cases (95 percent), the reported unusual transactions were suspicious. In the regular audits that the BFT performed (based on 200 investigations), only in 4 percent of the investigated files non-reported unusual transactions were found. In the risk-based investigations (based on 32 investigations) in 80 percent of the investigated files, non-reported unusual transactions were found, approximately 90 percent of these non-reported unusual transactions were suspicious. The risk-based analysis by the BFT has proved highly successful. In four years' time, the notaries were responsible from 0 percent to 30 percent of all the amount of money reported as STR. Notaries for instance have reported STR's in the last 4 years for the amount of EUR691 713 500. The notaries reported in the last four years 828 UTRs; in more than 50 percent of these UTRs, a link was made by the investigation performed by the BFT. This level of success should certainly encourage the BFT to conduct more risk-based inspections, as there are currently less than 10 risk-based inspections per year with a success rate of 80 percent.

1165. The BFT performed in 2009 and 2010 a number of risk-based investigations at forensic accountants and similar business providers. A number of specific fraud-related transactions were investigated and has resulted in a number of unusual transactions reported to the FIU-NL. A few investigations are still pending. The risk-based monitoring of accountants is more recent than for notaries and it is not yet possible to fully assess its impact in terms of sanctions and reporting.

1166. While there is a legal framework in place, secrecy issues prevent the exercise of supervision of lawyers by the BFT. The Bar association is conducting 150–250 inspections of law firms every year, but the BFT has no direct power of control on the quality of these inspections. The ministries of Justice and Finance are currently in the process of improving the legislative framework.

TCSPs

1167. Pursuant to Article 1 (a) BATWWFT, the DNB is the AML/CFT supervisor for trust offices. The DNB also supervises trust offices' compliance with the Wtt, the Regulations on sound operations under the Wtt (*Regeling integere bedrijfsvoering*, Rib) and the Sanctions Act 1977. There were 167 trust offices in 2009.

1168. Off-site activities/take place before on-site visits and consist in a file study, whereby deficiencies, follow up of deficiencies as identified during previous on-sites as well as recommendations, new developments and other public information is taken into consideration. The purpose of the onsite visits is to assess whether the TCSP is compliant with the AML/CFT legal requirements (as laid down in the Wtt, the Regulation on sound operational management under the Wtt and the Sanctions Act 1977) and as described in its procedure handbook.

1169. At the beginning of each year, a yearly plan for on-site examinations is prepared. The higher the (integrity) risk of a TCSP, the more on-site visits will be executed. Every trust office has a risk profile which is kept in the Financial Institutions' Risk Analysis System (FIRM).

Analysis of Effectiveness

1170. Up to end-2008, the supervision of trust offices focused mainly on gaining insight into their organization, activities and integrity risks. Trust offices function as a gatekeeper and, during that period, they realized quality improvements in their identification procedure for the ultimate beneficial owner (UBO) of client companies and the availability of the underlying data (this is one of the cornerstones of the Wtt). Along with other required Customer Due Diligence information (*e.g.*, on the source of capital, the purpose of the structure), such identification details are now generally available at trust offices.

1171. DNB took action to enforce the Wtt in cases where trust offices failed to make adequate progress. As of early 2009, supervision became more risk based. Examining officers went a step further where

possible and conducted extensive examinations into trust offices' knowledge of the source and destination of their client companies' funds. As of 2010, DNB will carry out examinations on specific themes. The planning for 2010 takes account of the integrity risks at institutional level identified by DNB. In its supervision of trust offices, DNB will focus on three themes in 2010, namely, feeders (foreign third parties that bring customers to TCSPs), real estate, and active operational branches.

1172. The following table gives an overview of the number of inspections, as well as sanctions imposed on trust offices in the period 2007–2009:

	2007	2008	2009
Total number of inspections	155	136	195
Cease and desist order	3	8	1
Administrative fine	1	3	0
Direction/ Instruction	0	0	1

1173. The Wtt has been evaluated by the Ministry of Finance during the course of 2009 and the results have been made public in the first half of 2010; more or less six years after its installation. It was concluded that the Wtt has been largely successful in the task it was charged with, being the regulation and identification of the Dutch trust sector, implementation of FATF and OESO recommendations, and the creation of a level playing field by prescribing the same procedures and requirements for all TCSPs.

Guidelines for DNFBPs (applying c. 25.1):

Real estate agents and dealers in precious metals and stones

1174. The BHM has published a manual for traders in goods in June 2008 and a manual for real estate agents in August 2009. These manuals have been disseminated by professional associations and should be available on the Internet soon. The BHM has provided specific guidance to dealers in precious metals through publication in professional journals and meetings with professional organizations (the latest occurred in March 2008). It has also organized meetings with real estate agents and their associations (two meetings a year on average). Several meetings took place in 2008 and 2009 between FIU-NL, professional organizations, and the BHM

Lawyers, notaries and accountants

1175. The professional bodies of tax advisors, chartered accountants, attorneys at law and (junior) civil-law notaries all have composed manuals (guidelines) on the interpretation of AML/CFT for their professionals. The BFT reviewed these manuals and provided comments on the Manual for lawyers for compliance with the obligations of the WWFT, the Manual for notaries for application of the WWFT, and the Guidelines for the interpretation of the WWFT for tax advisors and accountants. In addition, the Netherlands Bar Association used the basis of the e-learning course/exam of the tax advisers (which has been reviewed by the supervisor BFT), added the information relevant for lawyers and made the course available for all lawyers.

1176. In cooperation with the Ministry of Finance, the BFT published a manual for lawyers, notaries, tax advisers, and accountants. This brochure and other contributions have been spread via the professional organizations and professional journals. Furthermore the professional bodies of tax advisors and chartered accountants composed an e-learning course/exam. The BFT reviewed and approved this e-learning course. Furthermore, the BFT has a website (http://www.bureauft.nl) with 30 frequently asked questions, a power point presentation on AML and various publications of Articles on AML. In cooperation with FIU-NL BFT organizes private sector outreach meeting (*relatiedag*). On these meetings, the various professionals

(lawyers, accountants) were invited to attend presentations. The BFT issues three times in a year its own newsletter in which actual developments are described. This newsletter is distributed to the various professionals and also available on the website.

1177. In order to increase awareness and thus create more compliance of the anti-money laundering/combating of terrorist financing legislation, the BFT also focused on providing information to professionals to allow them to easily meet obligations arising out of this legislation. A large number of presentations are provided to professionals every year. In 2009, a total of 33 regional presentations have been attended by 1 700 professionals.

TCSPs

1178. Staff members of DNB division that performs integrity supervision on TCSPs, organized four seminars, workshops and presentations with professional associations and trust offices' staff, between 2003 and 2009. The latest seminar for trust offices has been organized in May 2009 to clarify the legal framework and present relevant cases. It was attended by approximately 300 persons.

1179. The DNB also publishes on its website the relevant laws and regulations, as well as a Q & A for trust offices and a guideline for preparation of procedures manual for trust offices. Moreover, regular meetings are organized with two associations representing the interests of trust offices, VIMS (12 larger trust offices), and DFA (64 small and medium size trust offices) in which current issues, experiences and developments in relation to trust offices are discussed.

Feedback to DNFBPs (applying c. 25.2):

1180. Regarding general feedback, the FIU provides statistics on the number of disclosures with appropriate breakdowns by type of DNFBPs. Information on current techniques methods and trends as well as sanitized examples of actual money laundering cases has been made available through reports and public presentations. Additional information could be given on the results of the disclosures, and the FIU publications could include a breakdown of the subjective and objective UTRs by type of DNBFPs.

1181. Regarding specific feedback, the information provided by the FIU to DNFBPs is generally limited to the acknowledgement of the receipt of the report, and to the information that a transaction has been considered suspicious by the FIU. The DNFBPs met by the authorities did not mention feedback received on cases closed or completed.

4.3.2 Recommendations and Comments

With respect to Recommendation 24

- Ensure that lawyers are subject to an effective system for ensuring compliance with AML/CFT requirements.
- Increase the effectiveness of the measures in place concerning illegal internet casinos that have their mind and management in the Netherlands.
- Increase effectiveness in the monitoring of precious metals dealers, lawyers and accountants.

With respect to Recommendation 25

- The FIU should provide DNFBPs with a more specific feedback on reported transactions.

4.3.3 Compliance with Recommendations 24 and 25

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.24	**PC**	• Secrecy issues prevent the exercise of supervision of lawyers by the designated supervisor. • Effectiveness of the measures in place regarding internet casinos illegally operating from the Netherlands could not be fully established. • Effectiveness issues in relation to the monitoring of precious metals dealers, lawyers and accountants.
R.25	**PC**[1]	• Specific feedback is not regarded as sufficient by reporting institutions. •

[1] This is a composite rating, taking account of other comments relating to Recommendation 25, *e.g.*, in section 3.

Indicative table of compliance with Recommendation 24 by type of DNFBPs

1182. In order to enable better fine-tuning of the risk-based system, and to take into consideration the specificities of each businesses and professions, the following compliance breaks-down the ratings by different types of DNFBPs.

DNFBP	Indicative rating	Rationale
Casinos	LC	Large majority of the essential criteria are fully met. Indications of effective implementation
Real estate agents	LC	Large majority of the essential criteria are fully met.
Dealers in precious metals and dealers in precious stones	PC	Large majority of the essential criteria are fully met. Lack of effectiveness
Lawyers	NC	Compliance with some of the essential criteria. Lack of effectiveness
Notaries	LC	Large majority of the essential criteria are fully met. Indications of effective implementation
Accountants	PC	Large majority of the essential criteria are fully met. Lack of effectiveness
TCSPs	LC	Large majority of the essential criteria are fully met. Indications of effective implementation

4.4 Other Non-Financial Businesses and Professions—Modern, Secure Transaction Techniques (R.20)

4.4.1 Description and Analysis

Legal Framework:

1183. Provisions regarding other non-financial business and professions are contained in Article 1 (a) (11) WWFT, Article 1 (a) (15) WWFT and Article 1 (a) (18) WWFT. In addition, as for the DNFBPs, some provisions of the UBWWFT and URWWFT also apply to these businesses and professions.

Other Vulnerable DNFBPs (applying R. 5, 6, 8-11, 13-15, 17 & 21 c. 20.1):

1184. The authorities have decided to expand the scope of non-financial businesses and professions subject to AML/CFT preventive measures to a number of professions. Based on discussion with the authorities, the perimeter of the non-financial businesses and professions has been expanded on the basis of risks, and has been reviewed over the time.

1185. **Tax advisors:** They are subject to AML/CFT preventive measures pursuant to Article 1 (a) (11) WWFT, insofar they act in the course of their professional activities. Contrary to lawyers, notaries or accountants, the profession of tax advisor has no statutory regulation. In this context, the scope of Article 1 (a) (11) is extended to any natural person who performs comparable activity in a business capacity.

1186. While this scope appears large at first sight, it is limited by the same exemptions related to the legal privilege which apply to lawyers and notaries. The extent of the preventive measures applying to tax advisors is similar to the one applying to lawyers. Tax advisors are supervised by the BFT.

1187. **Sellers of high value goods:** Pursuant to Article 1 (a) (15) WWFT, all seller of goods acting in the course of a business or profession are subject to the requirements of the law, insofar as payment for these goods is made in cash for an amount of EUR 15 000 or more, regardless of whether the transaction takes place in one operation or in several related operations. The extent of the preventive measures applying to the high value goods sellers is similar to the ones applying to dealers in precious metals and stones. Sellers of high value goods are supervised by the BHM insofar the transaction conducted by that seller of goods relates to the sale, or the provision of intermediary services in respect of the sale of vehicles, ships, works of art and antiques.

1188. **Other natural or legal persons:** Pursuant to Article 1 (a) (18) WWFT, natural or legal persons belonging to a category or profession or business, to be designated by order in council, can also have to apply the preventive measures. There has not yet been an order in council designating other natural or legal persons.

Modernization of Conduct of Financial Transactions (c. 20.2):

1189. The use of cash in the retail trade (share in nominal value of turnover) has decreased quickly in the past 25 years. In 1987, cash amounted for 75 percent of the retail trade turnover. It was 60 percent in 2000, 50 percent in 2004 and around 40 percent in 2008.

1190. In order to promote the efficiency of the Dutch payment system for consumers, retailers and banks, a national forum on the payment system (MOB) has been created. The forum meets twice a year. Its participants represent payment providers and customers. The Forum also has three observers. The Forum is chaired by DNB, which also provides secretarial back-up. In addition to the core group, the Forum has working groups focusing on particular issues and a special consultative platform. Among these issues is the Introduction of 3-D Secure for credit card payments over the Internet, in order to increase the safety of internet-based transactions.

1191. As the Netherlands are a member of the European Monetary Union (EMU), the largest banknote circulating in the country is the EUR500 (US $695) note, issued by the ECB. While aggregate statistics on the stock of such notes are published by the ECB, reliable statistics are not available on the share of such banknotes that circulates within the Netherlands.

1192. The authorities indicated that law enforcement agencies do not report significant use of large denomination euro banknotes in criminal cases. In addition, they indicated that in almost all shops the, EUR50 note is the highest denomination that is being accepted.

1193. The central bank provided the assessors with statistics on the number of EUR500 notes it issues and withdraws (see table below). In the recent years (2007–2009), the DNB tends to issue less EUR500 notes than it withdraws. Additional research would be necessary to identify if and which share of this pattern may be explained by the placement of cash in the formal financial sector. But interestingly, the share of EUR500 banknotes issued and withdrawn by the Netherlands has decreased over the period. The percentage of banknotes issued by the DNB went from 4.2 percent in 2007 to 2.4 percent in 2009. This is to compare with the weight of the Netherlands in the Eurozone GDP, which was 6.4 percent in 2009.

Number of EUR 500 banknotes issued and withdrawn (million of notes)						
	Banknotes issued			Banknotes withdrawn		
	Euro area	Netherlands	Percentage of total	Euro area	Netherlands	Percentage of total
2007	112	4.7	4.2%	106	6.1	5.8%
2008	148.4	4.3	2.9%	109.7	5.8	5.3%
2009	122.9	2.9	2.4%	95.3	5.2	5.5%

Source European Central Bank and DNB

1194. Consequently, based on statistical information and information from law enforcement agencies, the existence of the EUR500 banknote does not appear to pose a major risk for the Netherlands. While the measures taken by the retail businesses may explain this situation, the consequences of a recent recommendation by the European Commission would have to be closely monitored. This recommendation 2010/191/EU dated March 22, 2010 on the scope and effects of legal tender of euro banknotes and coins, refers to the issue of acceptance of high denomination banknotes in retail transactions. It indicates that "high denomination banknotes should be accepted as means of payment in retail transactions. A refusal thereof should be possible only if grounded on reasons related to the 'good faith principle' (for example, the face value of the banknote tendered is disproportionate compared to the amount owed to the creditor of the payment)". The recommendation comprises a review clause, and the Commission will assess its implementation in three years and examine whether regulatory measures are needed.

4.4.2 Recommendations and Comments

1195. There are no recommendations with regard to Recommendation 20.

4.4.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	**C**	• This recommendation is fully observed.

5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANIZATIONS

5.1 Legal Persons—Access to Beneficial Ownership and Control Information (R.33)

5.1.1 Description and Analysis

Legal Framework:

1196. Dutch legal entities are subject to the provisions of Book 2 of the Civil Code, the Commercial Register Act 2007, and the Commercial Register Decree 2008. In addition, Section 3 of the WWFT is relevant with respect to Recommendation 33 as Dutch law requires involvement of a notary when establishing a legal entity, except for religious communities and public legal persons.

1197. Book 2 of the Dutch Civil Code regulates the establishment, management and dissolution of legal entities established under Dutch law. Pursuant to Article 3 of Book 2 of the Civil Code, legal persons in the Netherlands may take the form of an (1) association (2) cooperative (3) public limited company ("NV") (4) private limited company ("BV") or (5) foundation. In addition, European Companies (SE) and European Cooperative Societies may be established and registered in the Netherlands. Both are subject to the same registration requirements as BVs and NVs. Pursuant to Article 3, legal persons may also take the form of a religious community or a public legal person. Pursuant to Book 5 of the Dutch Civil Code, communities of property owners are also legal persons. Foreign companies are registered with the Chamber of Commerce only if they have a branch or commercial undertaking and an establishment (branch or head office) in the Netherlands.

Measures to Prevent Unlawful Use of Legal Persons (c. 33.1); Access to Information on Beneficial Owners of Legal Persons (c. 33.2):

1198. The following measures facilitate the availability of beneficial ownership information:

- The obligation by all legal entities established under Dutch law or operating in the Netherlands to register with the Chamber of Commerce.
- The requirement to involve a public notary when establishing a legal entity under Dutch law, except for religious communities and public legal persons whereby public notaries are subject to and supervised for compliance with the provisions of the WWFT as outlined in section 4 of this report.
- For BVs and NVs, the requirement to obtain a "no objection" declaration from the Ministry of Justice before the entity may be set up and to file shareholder information with the tax authorities as part of an annual tax return.
- For Dutch BV's, the obligation to register the transfer of shares with the company and to have such a transfer certified by way of notarial deed.

- For separate private assets (such as for example foundations that serve as asset management vehicles or foreign legal arrangements or legal persons such as *Stiftungen* and *Anstalten*), the obligation under Dutch tax laws for the contributor and beneficiaries of the assets to be disclosed.

- For all Dutch legal entities or legal entities operating in the Netherlands, the obligation to maintain documents and records.

- In addition, law enforcement bodies may use their investigative powers as outlined in great detail under Recommendations 28 of this report to get access to and seize company documents located in the Netherlands. This measure is facilitated by the obligation of any natural person holding an interest of 5 percent or more in a Dutch or foreign company or association to file an annual tax return.

The obligation by all legal entities to register with the Chamber of Commerce

1199. BVs, NV's, foundations, associations with full legal personality, cooperatives, communities of property owners, charges (at the highest organizational level) and public legal persons are all subject to a registration requirement with the Chamber of Commerce pursuant to Article 6 of the Commercial Register Act 2007. The information to be provided includes the name of the legal entity, its legal type and its postal address or visiting address, its telephone, fax number and email address and its date of commencement.

1200. In addition, the Commercial Register Decree 2008, which was issued on the basis of the Commercial Register Act, stipulates that for all legal persons except religious communities and public legal persons, and certain European legal companies, the personal particulars of each director and supervisory board member, including the date on which the person started or ceased to act in such a capacity, the particulars of each member of the executive or managing body, and the particulars of persons other than directors to whom the Articles confer authority of representation and the authority of representation itself have to be provided. In addition, in cases where 100 percent of the shares are held by one owner, the personal particulars of the shareholder have to be provided as well. Private sector representatives indicated that in many cases, foundations were set up exclusively for the purpose of holding 1 percent of shares of a Dutch BV or NV so as to avoid this registration requirement.

1201. For associations, cooperatives and foundations, the personal particulars of each board member and supervisory board member, including the date on which he started or ceased to act in such a capacity, as well as the particulars of all persons other than directors to whom the articles of association confer authority of representation and the authority for representation itself have to be registered. Ownership information of these legal entities does not have to be provided since there are no shareholders.

1202. In addition to the above mentioned information, the notarial deed establishing a legal entity is registered, except in case of a church or a public legal person.

1203. Legal entities are under a legal obligation to inform the Registry within one week of any changes to the registered information. Article 4 of the Commercial Register Decree gives the Chamber of Commerce the authority and obligation to investigate the completeness and accuracy of updated information and to request further documentary evidence if needed. The authorities stated that for natural person, directors, or trustees that are residents of the Netherlands, the Chamber would also resort to a database with all residents maintained by the municipalities to obtain the relevant particulars. Any changes to this database automatically results in an update of the Chamber's Registry.

1204. Under Article 21 of the Commercial Register Act, all information and documents maintained by the Chamber of Commerce Registry is publicly available. Notarial deeds may be reviewed on the premises of the Registry or received by mail upon request.

1205. Under Article 47 of the Commercial Register Act it is prohibited to breach or not comply with the provisions of the Act, including the obligation to file updated information with the Registry, whereby the MOJ and the Dutch Tax Authorities may apply sanctions ranging from a fine to dissolution of the legal entity. Pursuant to Article 19a Book 2 of the Dutch Civil Code, the Chamber of Commerce may dissolve a legal person which is no longer deemed active and that is not meeting at least two out of four administrative obligations.

The requirement to involve a public notary when establishing a Dutch legal entity

1206. As indicated above, under Article 4 of the Dutch Civil Code all legal entities established under Dutch law require a notarial deed, except religious communities and public legal persons. Notaries, as outlined under section 4 of this report, are covered by the obligations under the WWFT, including the requirement to obtain and keep records of beneficial ownership information, and are also monitored for compliance with these obligations. However, as outlined under section 3 of this report, in practice the obligation under the WWFT only requires identification of those persons that hold 25 percent or more of an entity's shares. Notaries are not required to identify all shareholders and ultimate beneficial owners and to verify their identities.

1207. Law enforcement authorities generally do not have access to information held by public notaries due the application of legal privilege to this profession. Access may only be gained in certain limited situations as discussed under Recommendation 28 above. For all legal entities, the articles of association are filed with the Commercial Register, which in turn allows law enforcement authorities to link a specific entity with the relevant notary since the Articles are normally filed by the notary on behalf of the legal person.

1208. While the measure seems to ensure that certain beneficial ownership information is obtained at the time the legal entity is set up, it should be noted that in general, only the transfer of shareholder rights to Dutch BVs require involvement of a notary. Subsequent changes to the shareholder rights of any other legal entity are not subject to notarial oversight. For entities other than BVs, the information obtained by such professions is thus merely a partial snapshot of the situation as it exists at the time of establishment of the legal entity and can therefore not be considered complete and accurate in most cases. In addition, notaries are covered by legal privilege and access to such information may thus not be "timely" in all instances.

For Dutch BVs and NVs, the requirement to obtain a "no objection" declaration from the Ministry of Justice before the entity may be set up and to provide shareholder information as part of an annual tax declaration;

1209. Article 4 of the Dutch Civil Code stipulates that notarial deeds establishing a BV or NV may only be executed after issuance of a "no objection" certificate by Ministry of Justice. The *Justis* Office on behalf of the Ministry of Justice issues such a certificate after reviewing the criminal and financial records of the company founders, the first managing and supervisory directors and their relatives, and the information publicly available through the Commercial Register.

1210. Any information obtained by the Ministry in the course of this process that is not already publicly available through the Commercial Register may be shared with LEAs pursuant to Articles 2, 5 and of the

Documentation of Partnerships Act and could be used in the context of criminal investigations. From interviews with LEAs it seems that in practice, such information is not often utilized.

1211. Furthermore, BVs and NVs incorporated in or managed or controlled from the Netherlands are required under the General Tax Code to provide certain shareholder information, including the name, address, place and country of residence, as well as income and loss statements to the tax authorities as part of their obligation to file annual tax returns. For stock registered NVs, information only has to be provided on shareholder with an interest of 5 percent or more. Sanctions for failure to provide the required information or to maintain underlying documentation are set out under Article 68 of the General Tax Code. Legal entities such as for example foundations only have to pay corporate income tax if they are conducting business, which is defined to mean "participation in commerce with the intention to gain a profit."

1212. Information maintained by the Tax Authorities may be shared with other competent authorities based on Article 43c of the Implementation Regulation of the General Tax Code, including in cases where there is no concrete suspicion of any criminal conduct.

1213. As tax returns are filed on an annual basis, the information maintained by the tax authorities may not be up-to-date in all cases. Furthermore, the obligation to provide information on shareholders to the tax authorities does not extend to usufructuaries and other share beneficiaries.

1214. It should, however, be noted that under the Civil Code, complete and updated shareholder registers have to be maintained by legal entities as indicated below.

For Dutch BV's, the obligation to register the transfer of shares with the company and to have such a transfer certified by a notary

1215. According to Article 194 of the Civil Code, any transfer of title or right with respect to registered share of BV and the issuance of such new shares has to be performed before a public notary. As outlined above, information held by notaries is subject to legal privilege and access to it may thus not always be "timely."

For separate private assets, the obligation under Dutch tax laws for the contributor and beneficiaries of such assets to be disclosed.

1216. In January 2010, the Dutch authorities through Article 2.14a Law on Income Tax introduced a new mechanism to increase transparency in relation assets which have been legally separated from the private assets of a person in order to serve a private interest. The most common vehicles used to accomplish this goal and that are thus subject to this mechanism in the Netherlands are foundations, foreign trusts and, to a more limited extent, foreign *Anstalten und Stiftungen.*

1217. Under this new mechanism, pure asset management vehicles are no longer treated as fiscal entities. Rather, the contributor of the assets (such as for example trust settlor or the founder or owner of the legal person) remains responsible, liable and taxable for the legal person and the possession, debts and proceeds of the legal person are accounted to the contributor or his/her heirs. In addition, in cases where a concrete beneficiary has already been determined, the expenditures, possession, income and debts of the legal person are also attributed to the beneficiary in accordance with his rights and entitlements. Accordingly, in relation to separated private assets that have no determine beneficiary, the details of the ownership of such asset management vehicles have to be reported to the tax authorities on an annual basis. Where one or more beneficiaries have already been determined, information on such persons has to be reported to the tax authorities as well. The sanctions applicable to other tax violations or tax crimes, including administrative fines and in more severe cases criminal sanctions, are also available in relation to

non-compliance with the reporting obligation under Article 2.14a Law on Income Tax. Seperated private assets that existed already prior to the coming into force of this measure are subject to a transitional regime.

1218. Information received by the tax authorities as part of this process may be utilized by law enforcement authorities in the context of a criminal investigation. However, as tax returns are filed on an annual basis, the information maintained by the tax authorities in relation to the owners, founders, contributors or beneficiaries of asset management vehicles may not be up-to-date in all cases.

Documents and Records maintained by the Legal Entities

1219. For BVs and NVs, Article 194 of Book 2 of the Civil Code requires that a register indicating the names and addressed of all holders and beneficiaries of registered shares is being maintained. The provision sets out an obligation to keep such registers updated and to maintain the shareholder register at the office of the company, which may but does not necessarily have to be located in the Netherlands. For NVs, holders of bearer shares must only be registered if 100 percent of all company shares are held by one person.

1220. For all other forms of legal entities, Article 10 of the Civil Code requires that "administrative records of the financial position and everything relating to the work of the legal person" are kept for a period of at least seven years. These records have to be sufficient to allow the rights and obligations of the legal entity to be verified at all time. It is unclear to what extent such records have to include beneficial ownership information.

1221. Furthermore, there is no legal obligation to maintain shareholder records in the Netherlands. It is, therefore, questionable to what extent this measure would warrant the timely availability of accurate and complete beneficial ownership information.

Prevention of Misuse of Bearer Shares (c. 33.3):

1222. Shares of NVs serve to divide the authorized capital as mentioned in the articles of association. NVs are the only legal person that may issue bearer shares under Dutch law, whereby there is no limitation in the percentage of capital stock that may be issued in the form of such shares. Article 82 of the Civil Code requires that the articles of association indicate whether shares will be issued on name or bearer. The transfer of tile to such shares is generally not regulated or limited. However, where 100 percent of all bearer shares are held by one person, Article 91a of the Civil Code requires that the company has to be informed thereof within eight days.

1223. Ownership to bearer share certificates may be transferred merely by way of handing over the share certificate. As of December 31, 2009, about 3 600 NVs were incorporated under Dutch law. The authorities stated that at the time of the assessment, the value of bearer shares in circulation was estimated to be around EUR13.2 million, which represents only about 0,004 percent of all shares issued by Dutch legal entities. This estimate is further supported by figures published by DNB, which show that the number of banks with deposit desks needed to exchange physical certificates has decreased drastically.

1224. The Netherlands has started a process in which bearer shares will be ultimately dematerialized. The first phase was mobilization. The second phase was centralization, which entailed setting up a central depository for bearer securities to mitigate the risks of abuse of such instruments for ML purposes. The third phase is the dematerialization phase, which will be completed by January 1, 2013. From this time on, legal rights associated with bearer shares can no longer be transmitted merely by handing over the share certificates but require deposition on a nominative bank account. This date runs in parallel with the closure

of the transition phase in neighboring Belgium so that any shortcut, should it exist, will be made impossible.

1225. In addition, a RIS-list was created, which facilitates the centralized registration of lost and stolen physical bearer securities by reflecting all police reports on stolen or missing bearer securities. The authorities also indicated that over the last few years, frequent use has been made of the global note, which together with the central share register at the depository institution Necigef (central securities depository) is considered conclusive in relation to the rights associated with such shares.

1226. The estimates provided by the authorities suggest that in practice, bearer shares are not widely used in the Netherlands. In addition, certain measures as outlined above have been taken to mitigate the risk for such bearer securities to be abused for money laundering or terrorism financing purposes. However, given that at the time of the assessment there was no legal obligation to utilize the depository in relation to bearer shares and that until January 2013, the issuance of new and the free transfer of existing bearer shares is still permitted, a limited risk remains that such instruments are being abused for criminal purposes.

Additional Element—Access to Information on Beneficial Owners of Legal Persons by Financial Institutions)(c. 33.4):

1227. As indicated above, information maintained by the Chamber of Commerce Registry is publicly available, including for financial institutions. Information maintained by notaries or the companies themselves, however, is available to law enforcement authorities in only very limited circumstances as discussed under Recommendation 28.

Analysis of effectiveness

1228. In summary, the registration requirement for legal entities seems to warrant that updated, complete and accurate information on the control structure of legal entities is obtained and maintained by the Commercial Registry in all cases.

1229. In relation to information on owners, beneficiaries and other persons who ultimately own or control a legal person, however, some gaps remain. In particular, BVs and NVs are required to maintain an updated shareholder register but not to keep this register located in the Netherlands. Law enforcement authorities may thus not have access to such registers in all cases. The requirement to indicate shareholder information on tax returns is not subject to an updating requirement and generally does not extend to the ultimate beneficial owners of the shares. The information received as part of this measure may thus not be complete and/or up-to-date in all cases.

1230. Equally, the obligation under Dutch tax laws to declare the contributors, founders and beneficiaries of separated private assets applies only on an annual basis and may thus not be up-to-date in all cases.

1231. At the time of the assessment, Dutch law still permitted the issuance and free transfer of bearer shares. However, a dematerialization process has been put in place that will be completed by 2013. Based on estimates provided by the authorities, it seems that bearer shares are no longer widely used in the Netherlands.

5.1.2 Recommendations and Comments

- Information on ultimate beneficial owners of Dutch legal persons should be accessible and up-to-date in all cases.

- The dematerialization process should be completed as soon as possible to ensure that bearer shares issued by Dutch NVs are not abused for ML or TF purposes.

5.1.3 Compliance with Recommendation 33

	Rating	Summary of factors underlying rating
R.33	**PC**	• Information on the ultimate beneficial owners of Dutch legal persons is not accessible and/or up-to-date in all cases. • The measures that have been put in place to ensure that bearer shares issued by Dutch NVs are not abused for ML or FT purposes are not yet fully effective.

5.2 Legal Arrangements—Access to Beneficial Ownership and Control Information (R.34)

5.2.1 Description and Analysis

Legal Framework:

1232. Dutch law does not provide for the establishment of express trusts or similar legal arrangements. However, with respect to foreign trusts, the provisions of the WWFT are relevant as trusts established under foreign jurisdictions may be and in practice are administered in the Netherlands.

Measures to Prevent Unlawful Use of Legal Arrangements (c. 34.1):

1233. Dutch legislation does not provide for the constitution of legal arrangements such as *Trusts* or *Treuhand*. Nevertheless, the Netherlands has ratified The Hague Convention on the Law Applicable to Trusts and their Recognition on November 28, 1995 and therefore recognizes that trusts set up under foreign law have legal effect within the Dutch system. The number of trusts registered in the Netherlands with an undertaking and a branch or a head office in the Netherlands or that operate as single shareholders are limited. Information on the amounts of trust assets administered in the Netherlands is not available. Anecdotal evidence does however suggest that the numbers are rather low. Trusts operating an undertaking in the Netherlands are subject to certain registration requirements. Under Article 10 of the Commercial Register Act 2007, any undertaking belonging "neither to a legal person nor to a natural person" shall provide details regarding the person to whom the undertaking belongs to, including the name, legal type and the details of its constituents, members or partners, whether they are natural or legal persons. While this obligation seems to extend to trustees and settlors, it does not encompass trust beneficiaries.

1234. Trusts may be created in the Netherlands under a foreign law, the trust deeds and their signatures may be authenticated by Dutch notaries and trust funds may be held and/or administered by Dutch financial and non-financial intermediaries, some of which confirmed that they handle trusts set up abroad.

1235. Express trusts constitute separate private asset vehicles and thus fall under the measures set out in great detail under criterion 1 of Recommendation 33. Accordingly, information regarding the settlor and any determined beneficiaries has to be provided to the tax authorities on an annual basis. In the absence of a more regular updating requirement, however, this information may not be up-to-date in all cases.

1236. In addition, Dutch legislation through Article 3 of the WWFT requires financial and non-financial intermediaries to "identify the ultimate beneficial owner" and in cases involving "trusts" as referred to in the Convention on the Law Applicable to Trusts and on their Recognition to "take risk based and adequate measures to gain insight into the customer's ownership and control structure." However, as indicated under Recommendation 5 above, the definition of "beneficial owner" falls short the FATF standard as it does not extend to "the natural person(s) who ultimately own or controls" a legal arrangement.

1237. In cases where a trust is administered by somebody other than FIs and DNFBPs; however, no additional measures are in place to ensure that adequate and accurate beneficial ownership information on such arrangements is available and can be accessed by the authorities in a timely manner.

Access to Information on Beneficial Owners of Legal Arrangements (c. 34.2):

1238. Beneficial ownership information obtained by financial and non-financial intermediaries pursuant to Article 3 of the WWFT may be accessed by law enforcement authorities under the circumstances outlined in great detail under Recommendations 4 and 16 of this report. Access to information maintained by lawyers, notaries and accountants is however difficult to gain based on legal privilege, as discussed under Recommendation 28 of this report. In general, information maintained by FIs and DNFBPs is available to law enforcement on the basis of a prosecutorial decision. Information maintained by the Commercial Register in relation to trust undertakings is publicly available. Information maintained by the tax authorities may accessed by law enforcement authorities in the context of a criminal investigation.

Additional Element—Access to Information on Beneficial Owners of Legal Arrangements by Financial Institutions)(c. 34.3):

1239. Information held by FIs and DNFBPs is not available to other financial institutions.

Analysis of effectiveness

1240. In sum, information on the settlors of foreign trusts seems to be available through the Commercial Register in cases where the trust is operating an undertaking in the Netherlands.

1241. In relation to pure asset management vehicles, information on the settlor and beneficiaries has to be provided to the tax authorities on an annual basis. In the absence of a more regular updating requirement, however, such information may not be complete and accurate in all cases. Neither Dutch tax laws nor the registration requirement provide for the disclosure of information on persons other than the settlor who can exercise ultimate effective control over a legal arrangement.

1242. In relation to trusts administered by professional Dutch FIs or DNFBPs, beneficial ownership information has to be provided as part of the customer due diligence process under the WWFT. As noted above, however, the relevant provisions under the WWFT fall short of the FATF standard as they do not include the control structure of legal arrangements and thus are not be sufficient to ensure that adequate and accurate beneficial ownership information is available to law enforcement authorities in all cases. In addition, beneficial ownership information obtained by lawyers, notaries and accountants may not be accessible due to the legal privilege as discussed under Recommendation 28 above.

5.2.2 Recommendations and Comments

- The definition of the “beneficial owners” as contained in the WWFT should extend to “the natural person(s) who ultimately own or controls a legal arrangement.”

- For trusts not administered by a Dutch FI or DNFBP, put in place additional measures to ensure that timely, accurate, and complete beneficial ownership information is available in all cases.

5.2.3 Compliance with Recommendation 34

	Rating	Summary of factors underlying rating
R.34	PC	• For trusts administered by licensed Dutch FIs or DNFBPs, the definition of the "beneficial owners" as contained in the WWFT does not extend to "the natural person(s) who ultimately owns or controls a legal arrangement." • Scope of legal privilege hinders the possibility for law enforcement authorities to access beneficial ownership information regarding trusts held by lawyers, accountants and notaries. • For trusts not administered by Dutch FIs or DNFBPs, the annual updating requirement for beneficial ownership information as required under the Law on Income Tax is not sufficient to ensure that timely, accurate and complete beneficial ownership information is available in all cases.

5.3 Non-Profit Organizations (SR.VIII)

5.3.1 Description and Analysis

Legal Framework:

1243. NPOs in the Netherlands may take the form of "associations", "foundations", NVs, and BVs, whereby the latter two may be NPOs only if they qualify as ANBIs (*Algemeen Nut Beogende Instellingen*) as indicated below and do not conduct any commercial activity. NPOs thus have legal personality and are subject to registration with the Chamber of Commerce Register. The Dutch Civil Code does not provide for a definition of the term "non-profit organization."

Review of Adequacy of Laws & Regulations of NPOs (c. VIII.1):

1244. The Dutch authorities have conducted several studies of the NPO sector as a result of which weaknesses in existing legislation have been identified and addressed by way of proposed legislative amendments to enhance the supervision and transparency of the NPO sector.

1245. Since 2004, the Ministry of Finance, the Financial Expertise Centre, the Ministry of Justice as well as the Public Prosecutor's Office in cooperation with the Tax and Customs Administration have conducted a number of reviews of the size, activities and other features of the domestic NPO sector to identify and assess the potential TF risks. In particular, the reviews sought to identify the number and size of NPOs operating from or established in the Netherlands, the amounts of assets held or managed by such NPOs, the level of organization and to a limited extent also the identification of gaps in laws and regulations pertaining to NPOs.

1246. Since 2004, two reviews conducted by the FEC, one review commissioned by the Ministry of Finance, two reviews commissioned by the MOJ, and one review conducted by the public prosecutor's office and the tax and customs administration were carried out. While the reports resulting from these reviews were not available to the assessors, the authorities indicated that the main finding of all these reviews was that the charity sector is vulnerable but that there is no concrete evidence of abuse by criminal organizations. In summary, it was concluded that the number of foundations and associations that are linked to criminal activities is relatively low. It was further found that the level of transparency could be improved for most charities and that control mechanisms with respect to NPOs should be strengthened. It is unclear what information and sources were used to conduct these reviews and what information on the activities, size and other relevant features of the NPO sector has been taken into account.

Outreach to the NPO Sector to Protect it from Terrorist Financing Abuse (c. VIII.2):

1247. The Central Bureau for Fundraising (CBF) is an independent and privately-run accrediting and oversight agency in the Netherlands that promotes responsible fundraising by charitable organizations. In addition to issuing a seal of approval to organizations qualifying an extensive set of criteria, the CBF offers a "statement of no objection" to new organizations which fulfill basic standards of credibility but have not yet met all standard criteria. NPOs under the monitoring of the CBF have obtained some guidance on risks of criminal abuse and guidance on how to mitigate such risk as part of a tool kit which was distributed to all 350 sealed members. The tool kit also contains a component on TF but no typologies. In 2008, a seminar on terrorist financing was held for all CBF member NPOs.

1248. To enhance transparency, accountability, integrity and public confidence in the administration and management of NPOs under supervision of the CBF, NPOs are required to keep information on the identities of donors and the identity, background and reliability of beneficiaries. Such records must be held by the NPO for at least seven years and is accessible by law enforcement authorities based on prosecutorial decision. However, it should be noted that these principles are applicable only for sealed NPOs.

1249. For NPOs outside the scope of the CBF, no guidance has been given or awareness raising initiatives been launched to protect the sector from terrorist financing abuse and no typologies have been issued.

Supervision or Monitoring of NPOs that Account for Significant Share of the Sector's Resources or International Activities (c. VIII.3):

1250. The Public Prosecutor's Office and the Tax and Customs Administration are the two main government agencies with responsibilities to supervise NPOs operating in or from the Netherlands. In addition, the CBF has mechanisms in place to monitor the activities of its members.

1251. While scientific numbers are not available, based on two surveys as outlined below, it is estimated that about 85 percent of all funds raised in the Netherlands are subject to supervision by the Tax authorities and monitoring by the CBF. In addition, all NPOs in form of foundations or 60 percent of all NPOs incorporated under Dutch law are supervised by the Public Prosecutor. The international NPO sector in the Netherlands accounts for 36 percent of the total fundraising income, all of which is monitored by the CBF.

1252. All NPOs established in the form of a foundation are supervised by the Public Prosecutor's office, whose task it is to ensure that information provided by NPOs is accurate and reliable. The powers entrusted in the Public Prosecutor's Office to carry out this mandate are civil in nature and are based on Articles 297 to 299 of the Civil Code. Pursuant to these provisions, if there is serious doubt about whether a foundation is complying in good faith with statutory requirements or its constitution the Public Prosecutor's Office may request information from the management board and, in cases where the requested information is not provided, may apply for the court to compel the production of such records.

1253. The Public Prosecution Service may also request the court to dismiss or suspend a member of the management board if there are reasons to do so. A dismissed member of the management board may not hold a similar position for the first five years after dismissal. Representatives of the Public Prosecutor's Office stated that they would conduct inquiries both upon information disclosed by the public or the media and information received by the intelligence service or law enforcement authorities. The authorities stated that so far it has never been necessary to refer any cases to law enforcement authorities for further investigation.

1254. Apart from the responsibilities of the Public Prosecution Service the Netherlands have two main mechanisms in place to monitor the activities of NPOs: (i) preventive fiscal supervision of charities and other NPOs that would like to take advantage of certain tax benefits and (ii) a voluntary seal of approval or statement of no objection for fundraising institutions provided by the CBF.

ANBI Supervision Mechanism

1255. Any legal entity with a charitable purpose, including NPOs from Member States of the EU or EEA that seek tax benefits under the Law on Gift and Inheritance Duties and the Law on Income Tax may apply to the Tax and Customs Administration for certification of the NPO as "ANBI." To qualify as such, the NPO needs to show that (1) it does not intend to make a profit, has a charitable character and that 90 percent of its activities serve a general purpose (2) that a natural or legal person cannot control the assets of the NPO as if it was his/her own capital (3) that the institution is not allowed to have more assets than reasonably necessary to accomplish its charitable goal (4) that managers and policy making bodies of the NPO do not receive an unreasonable fee for their daily activities and (5) that the NPO provides an insight into its activities, fundraising, and administration of funds and expenses. In addition, managers of NPOs may not have a criminal record.

1256. The Tax and Customs Administration reviews each NPO for compliance with these requirements before granting ANBI status and, in the course of doing so, may also require a full overview of the NPO's financial administration, including all revenues. The right to access and request such information remains with the Tax and Customs Administration even after ANBI status has been granted. ANBI information may be shared with law enforcement authorities in the case of a criminal investigation, with the prosecutor's office where civil powers are used to dissolve a legal entity and on the basis of an agreement with other authorities to counter a common enforcement deficit pursuant to Article 43c (1)(m) of the Implementation regulation of the General Tax Code. Sharing of information with the CBF is not possible as the CBF is not a government authority.

1257. NPOs may apply for ANBI status individually or as a group. Application of as a group is possible for NPOs that have the same goal, such as for example churches. At the time of the onsite mission, about 20 000 individual and 100 groups ANBIs, which in turn covered about 30 000 member NPOs, had been awarded. In total, 50 000 or 16 percent of all Dutch NPOs were thus subject to the Tax and Customs Authorities supervision mechanism. The authorities stated that all CBF sealed companies would also be ANBIs. Based on the surveys explained below, at least 85 percent of the total assets held and administered by NPOs in the Netherlands are thus estimated to be under the control of ANBIs.

CBF Supervision Mechanism

1258. The CBF plays a two-fold role with respect to NPOs:

1259. First, 421 of the 430 municipalities in the Netherlands require NPOs that intend to make cash collections to obtain permission by the municipalities. In deciding whether permission will be granted, the 421 municipalities obtain advice by the CBF. In formulating its advice, the CBF, upon request by the municipalities collects data on the applicant from the Chamber of Commerce Register and from publicly available sources on the NPO. Unless any evidence of irregularities or possibly illicit behavior is identified, it is recommended to grant the permission. NPOs may but are not required to file information as part of this process. The CBF has set up a database to keep information collected as part of this process, whereby a significant part thereof is publicly available. Representatives of the CBF stated that about 5 percent of all donations in the Netherlands would be made in cash. NPOs that fail to obtain the permission are acting in violation of the law of the municipality.

1260. Secondly, NPOs, to enhance their credibility and improve their fund raising opportunities, may apply to the CBF for a "seal of approval" or, for NPOs that have not yet met these high standards for a continuous period of three years, a "statement of no objection." At the time of the on-site missions, about 300 NPOs had been sealed and another 50 NPOs has obtained a statement of "no objection."

1261. To obtain a "seal of approval", NPOs have to meet rather stringent requirements, including "know your donors" and "know your beneficiaries" principles for a continuous period of three years. NPOs have to establish that members of the highest decision-making body such as the board of directors do not receive compensation for their services, are not related or otherwise tied to each other, and are not employees, shareholders, founders or board members of entities that benefit from the NPO's activity or funds. Safeguards to avoid and deal with conflicts of interests by NPO directors, employees or supervisors, a multi-year policy outlining the NPO's financial estimates and procedures for receiving and spending monetary resources must be in place as well.

1262. To verify that a specific NPO meets the above criteria, the CBF conducts an assessment of the NPO's records and information prior to awarding the seal of approval. Subsequent annual assessments are conducted to ensure ongoing compliance.

1263. As a result of this process, for all sealed NPOs the CBF maintains a database with board meeting minutes, the particulars of all board members, managers and trustees, the purpose, and expenditures based on category. The majority of this information is publicly also available on the CBF homepage. Only the particulars of board members (other than the names) and the board meeting minutes are confidential.

1264. Representatives of the CBF stated that sharing of confidential information with the Tax Administration would not be possible as the CBF is a private entity and not a public agency. It was stated that in two cases the CBF filed a report with the police with respect to fraudulent behavior. In one of the two cases, a criminal investigation was initiated and is ongoing. The CBF is also not part of FEC and could thus not use this platform to share information.

1265. At the time of the onsite mission, about 350 or 0.05 percent of all Dutch NPOs had been under the monitoring mechanisms of the CBF. While this number seems rather low, it should be noted that these 350 NPOs are estimated to account for about 85 percent of all public fundraising income in the Netherlands. The estimate is based on two surveys; one conducted by a university the other by the CBF, both of which reached the same conclusions. The CBF survey was conducted through application of a sample testing of about 1 500 fundraising organizations that are also ANBIs. Based on the responses of these 1 500, it was estimated that about 85 percent of all funds raised in the Netherlands every year were raised by CBF sealed NPOs. Furthermore, the international NPO sector in the Netherlands accounts for 36 percent of the total fundraising income, and is completely monitored by the CBF.

Information maintained by NPOs and availability to the public thereof (c. VIII.3.1):

1266. Information registered at the Commercial Register includes name, seat and purpose of the NPO as well as particulars of directors and other persons to whom the articles of the legal entity confer authority of representation and the contents of such authority and is publicly available. Any changes to this information have to be registered within one week. Information with respect to the purpose of and control over CBF certified NPOs is also publicly available via the CBF's homepage, whereby only the name but not the particulars of directors and trustees is publicly available.

1267. NPOs that have the status of ANBIs or have obtained the seal of approval by the CBF have an ongoing duty to be able to establish that the various certification requirements as outlined above are met. In both cases, these requirements also relate to the purpose of the NPO. ANBI requirements only address the

control structure but not the ownership of NPOs whereas the requirements of "know your donor" and "know your beneficiaries" under the CBF measures address both control and ownership of NPOs.

1268. Under Article 10 of the Civil Code, all legal entities, including foundations and associations with a charitable purpose, further have to maintain records for a period of seven years that allow the rights and obligations of the NPO to be established at all time. The Civil Code, through Article 10, requires that at a minimum, balance sheets and statements of accounts, and expenses are maintained.

Measures in place to sanction violations of oversight rules by NPOs (c. VIII.3.2):

1269. The MOJ has the power to sanction any violations of the registration requirements applicable to legal entities, whereby sanctions may range from a fine to dissolution of the legal entity. In addition, the Public Prosecutor's Office as the supervisory authority for foundations may apply to the civil court for dismissal or suspension of a director of the foundation in cases of violations of Dutch law and for dissolution of the foundation if its activity violates public order. As outlined under Recommendations 1 and 2 of this report, legal entities are also subject to criminal liability under Dutch law and its assets subject to criminal confiscation.

1270. For ANBIs and certified NPOs, both the Tax and Customs Authority and the CBF may withdraw certification in case of non-compliance with the relevant certification requirements. In addition, the regular sanctioning powers under the Tax Code are available.

1271. Since 2007, the CBF has unsealed five NPOs and has issued public warnings with respect to several other NPOs. Neither of these cases related to TF but to failure to fulfil the seal requirements. The Tax Administration has withdrawn ANBI status in about 1 750 cases after the law setting out fixed ANBI criteria was introduced in 2008. It is unclear whether such action was ever taken due to TF activities of or through an NPO.

Licensing or registration of NPOs and availability of this information (c. VIII.3.3):

1272. Every legal entity, including foundations and associations with a non-charitable purpose, has to be registered with the Dutch Chamber of Commerce. In addition, registration with the Tax and Customs Authority and/or the CBF is possible as outlined in great detail under criterion 3 above.

Maintenance of records by NPOs and availability to appropriate authorities (c. VIII. 3.4):

1273. Under Article 10 of the Civil Code, all legal entities, including foundations and associations with a charitable purpose, have to maintain records for a period of seven years. The records have to be sufficient to allow the rights and obligations of the NPO to be established at all time. The Civil Code, through Article 10, requires that at a minimum, balance sheets, statements of accounts, and expenses are maintained.

1274. NPOs that have ANBI status are required to give insight into "the foundation's activities, fundraising, and administration of funds and expenditures." The authorities confirmed that this language would require ANBIs to keep transaction records that are specific enough to verify that funds have been spent in a manner consistent with the purpose and objectives of the NPO.

1275. NPOs certified by the CBF are required to have in place "procedures" regarding the receiving and spending of money. While this language does not warrant that detailed transaction records are kept in all cases, the additional requirement for certified NPOs to present an audited financial report and an annual report approved by the board and reviewed by the CBF allows for such a requirement to be implied. CBF

sealed NPOs are required to make transaction records available to the CBF upon request, whereby representatives of the CBF stated that no such request has ever been made in the past.

Measures to ensure effective investigation and gathering of information (c. VIII.4):

1276. The Netherlands have the following avenues for sharing of information in relation to NPOs:

1277. ANBI information may be shared with law enforcement authorities in the case of a criminal investigation, with the prosecutor's office where civil powers are used to dissolve a legal entity and on the basis of an agreement with other authorities to counter a common enforcement deficit. The Tax and Customs Administration is also explicitly authorized to share information with all AML/CFT supervisors, including in situations where there is no concrete suspicion of criminal conduct.

1278. The FEC offers another platform for the exchange of information between the relevant FEC partners. The Tax Administration based on strict secrecy provisions may however not share information through FEC in the absence of a concrete suspicion of criminal behavior.

1279. Information can also be shared through the Counter Terrorism ("CT")-infobox. This CT-Infobox is a formalized partnership of the AIVD, the Immigration and Naturalization Service (IND), the KLPD, the Military Intelligence and Security Service (MIVD), the Public Prosecution Service (OM), the FIOD-ECD (part of the Tax and Customs Authority) and FIU-NL, with the AIVD as lead agency. Its objective is to combat terrorism by centrally compiling and comparing information. This concerns people and networks involved in some way with terrorism, particularly Islamist violence, and associated radicalization.

1280. All information held by the Chamber of Commerce is publicly available. It should however be noted that the information held by the Chamber of Commerce is limited.

1281. Finally, information held by the CBF may be accessed by law enforcement authorities based on a prosecutorial decision. The CBF may however file a report with the police on its own initiative, which the authorities indicated has happened in the past.

1282. Upon existence of any suspicion that any legal entity was involved in or participated or aided or prepared the commission of a criminal offense, law enforcement powers as outlined under Recommendation 28 of this report are available to gather information and investigate NPOs.

Domestic cooperation, coordination, and information sharing on NPOs (c. VIII.4.1):

1283. In the absence of a concrete suspicion of criminal conduct, cooperation, and information sharing, either indirectly or directly, between the Tax Authorities, the Chamber of Commerce and relevant supervisors is possible through the avenues outlined above. However, given that the CBF is a private entity, it is not integrated into the information sharing and cooperation mechanisms of the public sector. This is a significant limitation in that the CBF supervises about 85 percent of all funds raised in the Netherlands and all Dutch NPOs that operate internationally.

Access to information on administration and management of NPOs during investigations (c. VIII.4.2);

1284. In addition to the general information sharing mechanisms as indicated above, the Tax Authorities may share information with law enforcement authorities in the course of a criminal investigation.

1285. Information held by the CBF may be accessed by law enforcement authorities only based on a prosecutorial decision.

Sharing of information, preventative actions, and investigative expertise and capability, with respect to NPOs suspected of being exploited for terrorist financing purposes (c. VIII.4.3):

1286. As indicated above, the Netherlands have a range of mechanisms in place that allow for the sharing information in relation to NPOs.

1287. However, given that the CBF is a private entity and, thus, is not part of any of these mechanisms, the effectiveness thereof is questionable. In addition, representatives of the FEC stated that the commission would currently not be utilized for purposes of taking preventive or investigative measures with respect to NPOs.

Responding to international requests regarding NPOs—points of contact and procedures (c. VIII.5):

1288. The Netherlands have not designated specific focal points to receive and respond to requests from abroad for information regarding NPOs that are suspected of FT. However, Dutch authorities may receive and respond to requests from foreign counterparts on specific NPOs. The general information sharing and mutual legal assistance procedures as outlined under Recommendations 36 to 40 of this report also apply in relation to NPOs.

1289. The CBF is part of the International Committee on Fundraising Organizations (ICFO) and is able to share information on suspected NPOs with foreign NPO supervisors through the ICFO network. However, as indicated above, the CBF is a private entity and thus not integrated into the international information sharing procedures of the public sector.

Analysis of effectiveness

1290. The measures in place with respect to NPOs operating in or from the Netherlands warrant a high level of transparency. From meetings with the private sector it appears that the level of compliance by NPOs with these measures is significant. The level of interest and scrutiny Dutch NPOs encounter both from the public and the media provides a further incentive for NPOs to ensure that they are transparent, accountable and integer.

1291. Based on meetings with Dutch law enforcement authorities and in light of the scope of the various reviews conducted by the MOJ, the MOFI and the Prosecutors' Office; however, it seems that the authorities' focus lies more on the detection of criminal activity in specific cases rather than on the prevention of terrorism financing through the NPO sector. In particular, it is unclear whether and to what extent information maintained by the CBF is used by the authorities in conducting sector specific risk reviews.

1292. Information available with respect to NPOs is generally comprehensive, in particular with respect to NPOs within the CBF seal mechanism.

1293. Information sharing and cooperation mechanisms are in place but do not integrate the CBF, which poses a limitation as the CBF maintains detailed information on a significant share of the sector.

5.3.2 Recommendations and Comments

- For NPOs outside of the CBF's seal mechanism, undertake outreach initiatives to enhance NPO's awareness about the risks of terrorist abuse and the mechanism available to mitigate such risks, and to promote transparency, accountability, integrity and public confidence in the NPO sector.

- For CBF approved NPOs, ensure that all information available is used by the Dutch authorities to review the activities, size, and other features of the NPO sector and to formulate appropriate preventive measures.

- Develop coordination and information exchange mechanisms that involve the CBF to facilitate the effectiveness of the supervisory framework and to warrant the application of preventive and investigative action in all cases where a particular NPO may be abused for ML or TF purposes.

5.3.3 Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
SR.VIII	**LC**	• For NPOs outside the CBF seal mechanism, no outreach initiatives to enhance NPO's awareness about the risks of terrorist abuse and the mechanism available to mitigate such risks have been conducted. • No coordination and information exchange mechanisms involving the CBF are in place.

6. NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 National Co-Operation and Coordination (R.31 & R. 32)

6.1.1 Description and Analysis

Legal Framework:

1294. WWFT establishes confidentiality rules and the scope for disclosure. Article 22 of the WWFT forbids any authority from disclosing confidential information except where necessary for the performance of that party's duties or as required under the Act. There is also explicit provision for information exchange between the FIU and the supervisory authorities in Articles 13g and 25 of the WWFT. In addition, there are provisions relating to the disclosure of information between domestic and foreign supervisory authorities in the Wft (Articles 1.51 and 1.90), to prosecutors (Article 1.92) and to others. The Wgt also provides for appropriate disclosures.

Mechanisms for Domestic Cooperation and Coordination in AML/CFT (c. 31.1):

1295. The Ministry of Justice and The Ministry of Finance are responsible for the AML/CFT policy and this structure is designed to ensure a coordinated approach. To enhance coordination, a series of bodies have been established:

- **Financial Expertise Center (FEC)** which is concerned with financial sector integrity and consists of the police, public prosecutor, the supervisory bodies (DNB and AFM only), the intelligence agencies and the tax administrators.

- **WWFT coordination meeting**, at which the competent supervisors for the WWFT (DNB, AFM, BFT and BHM) and the FIU meet, every two months, to share information and views.

- **The Indicators Working Group** which considers the indicators for making objective unusual transaction reports. This group is led by the Ministries of Finance and Justice and includes representatives of the private sector.

- **The Committee on Money Laundering** established by Article 21 (1) of the WWTF formally has the duty to consider indicators and has, in the past exercised oversight over the FIU but has subsequently become a more general coordinating body acting as a discussion partner for the responsible Ministries as regards the functioning of the duty to disclose in practice and the determination of the indicators.

- **Project based groups such as the task force on real estate.** This task force has been created following a recent investigation involving the use of real estate transactions to commit financial fraud. It is co-chaired by the Ministries of Justice and Finance and includes a wide range of administrations and supervisors.

1296. The FEC has three tasks:

- Create conditions for a structural exchange of information between the partners. The FEC unit's Information platform plays a key role in this process. Its two employees push and pull information flows to and from FEC partners contributing to a continuous exchange of information.

- Set up a joint knowledge center aiming at strengthening mutual cooperation through knowledge sharing between the FEC partners.

- Support and execute projects to produce concrete and operationally useful results. In this regard, the FEC is currently working on a national threat assessment (NTA) on money-laundering. The NTA should be finalized in February 2011 and will inform the priorities of the whole AML-chain.

1297. The Coordination meeting between the FIU and the supervisors takes place every two months and has an open agenda. The FIU reports that the supervisors (and especially the DNB) play an active part in this process. The FIU reports that DNB receive data on the reporting institutions that are subject to their supervision but that the AFM does not (largely because there are so few reports). The group discusses risks arising from different entities.

1298. The private sector representatives stated that the Committee on Money Laundering and the Indicators Working group have not met for some years. However, the authorities have informed the mission that the Committee met in May 2010.

1299. Additional Element - Mechanisms for Consultation Between Competent Authorities and Regulated Institutions (c. 31.2):

1300. The Committee on ML and TF, which is referred to above consists of representatives of the reporting institutions, the supervisors and investigative bodies. In addition, there are other mechanisms for consulting the private sector:

- Private sector outreach meetings organized by the FIU and the relevant supervisory authority designed to discuss case studies and provide information on new developments.

- AFM led discussion groups with the private sector, including the Integrity Platform (where investigations are discussed) and round table sessions (where fraud cases are discussed).

- The Bankers Association sanctions working group.

Review of the AML/CFT system's effectiveness (applying R.32):

1301. The authorities use the statistics they maintain to review the effectiveness of their system to combat ML and FT. Statistical information is used by the authorities in a number of ways. For example: by the FIU to adapt the objective indicators for reporting UTRs; by the FEC to support exchange of information and cooperation between the FEC partners; into project based groups such as the task force on real estate; and for national threat assessments.

Analysis of effectiveness

1302. The authorities are clearly willing to establish domestic coordinating bodies so as to bring together the various parties involved in developing the defenses against money laundering. There is clearly

a strong intent to share information and maximize the use of the expertise available. It is surprising, therefore, that there is disappointment about the extent of coordination in practice. In particular:

- The parties report that there is relatively little discussion of current trends in ML and TF in the Netherlands—a discussion that could arise from the knowledge of law enforcement, intelligence or other agencies and which could assist the supervisors and reporting entities to focus attention.

- Although some guidance has been given on the patterns of expenditure of certain terrorists and other matters, the private sector does not consider that it is useful and believes this to be in part because of the absence of consultation on what would be useful.

- Some initiatives (for example an analysis of risks posed by insurance businesses) are started by and conducted by individual institutions (in this case the FIU) without always involving other parties with expertise to contribute.

6.1.2 Recommendations and Comments

1303. The authorities are recommended to:

- Make greater use of existing coordination bodies and, if appropriate, combine some of the bodies so as to focus the resources of the participating parties.

- Encourage the supervisors and the FIU to make greater use of the information on reporting patterns and to consider benchmarking the Dutch experience against that of other countries so as to establish a risk-based awareness program to tackle those sectors where reporting is minimal.

- Make greater use of the private sector's desire for greater feedback from the FIU so as to maximize the value of the reporting process.

6.1.3 Compliance with Recommendations 31 & 32 (criterion 32.1 only)

	Rating	Summary of factors underlying rating
R.31	**LC**	• Coordination mechanisms not all used effectively.
R.32	**LC**[1]	• Criterion 32.1 is observed.

[1] This is a composite rating, taking account of other comments relating to Recommendation 32, see section 7.1.

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1 Description and Analysis

Ratification of AML-Related UN Conventions (c. 35.1):

1304. The Netherlands has ratified the United Nations Convention against Transnational Organized Crime (the Palermo Convention) on May 26, 2004 and the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention) on September 9, 1993.

Ratification of CFT-Related UN Conventions (c. I.1):

1305. The Netherlands has ratified the International Convention for the Suppression of the Financing of Terrorism on February 7, 2002 and has ratified all of the other 11 international conventions and protocols on terrorism. The remaining three instruments, namely the Nuclear Terrorism Convention, the

Amendments to the Nuclear Material Convention and the Protocol to the Maritime Convention have been signed but not yet been ratified by the Netherlands.

Implementation of Vienna Convention (Articles 3-11, 15, 17 & 19, c. 35.1):

1306. Dutch law complies with many provisions of the Vienna Convention.

1307. ML is criminalized in line with the Vienna Convention, confiscation and seizing measures are available for all offenses under the Convention and the power of law enforcement agencies to identify and trace property that is or may become subject to confiscation is generally not hindered by financial secrecy. Access to information held by lawyers and other legal professionals is however limited in most cases.

1308. Furthermore, the Netherlands may provide a number of different types of mutual legal assistance with respect to drug-related ML offenses. However, assistance in searching or seizing of property or evidence may only be granted in relation to extraditable offenses. Given that drug related ML is not an extraditable offense under Dutch law, the mentioned forms of assistance may thus not be provided in relation to ML offenses under the Vienna Convention.

Implementation of Palermo Convention (Articles 5-7, 10-16, 18-20, 24-27, 29-31 & 34, c. 35.1):

1309. Dutch law complies with most provisions of the Palermo Convention. ML offenses involving organized crime are criminalized fully in line with the Palermo Convention and confiscation and seizing measures in relation to proceeds obtained through the commission of such offenses are available.

1310. The Netherlands may also provide a wide range of different types of mutual legal assistance with respect to ML offenses involving transnational organized crime. As ML offenses involving transnational organized crime are extraditable offenses under Dutch law, assistance in searching or seizing for property or evidence in relation to such offenses may be granted.

1311. Preventive measures and a supervisory regime are in place for banks and non-bank financial institutions. However, the legal framework setting out the various obligations is still subject to a number of shortcomings as discussed under section 3 of this report. In particular, customer due diligence measures, record keeping, and STR reporting requirements could be strengthened further.

1312. The Netherlands have established an FIU and apply the EU's cross border declaration system.

Implementation of CFT Convention (Articles 2-18, c. 35.1 & c. I.1):

1313. Dutch law criminalized terrorist financing conduct by way of the preparation offense under Article 46 of the Penal Code or, in relation to terrorist organizations, as participation in a terrorist organization under Article 140a of the Penal Code.

1314. As indicated in the analysis for Special Recommendation II, the cited provisions do not cover all requirements as set out in Article 2 of the CFT Convention. In particular, the financing of terrorist acts and individual terrorists is not criminalized in all cases and the financing of terrorist organizations is not fully in line with the requirements under the CFT Convention.

1315. Preventive measures are in place for banks and non-bank financial institutions. However, the legal framework setting out the various obligations is still subject to a number of shortcomings as discussed under section 3 of this report. In particular, customer due diligence measures, record keeping, and STR reporting requirements could be strengthened further.

1316. TF is an extraditable offense under Dutch law as indicated under Recommendation 39 below.

Implementation of UN SCRs relating to Prevention and Suppression of TF (c. I.2)

1317. As outlined in detail under SR III, the Netherlands's response to UNSCR 1267 and 1373 is generally adequate even though some minor and technical shortcomings have been identified.

Additional Element—Ratification or Implementation of other relevant international conventions (c. 35.2):

1318. The Netherlands have ratified the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (Strasbourg Convention) and the European Convention on the Suppression of Terrorism.

6.2.2 Recommendations and Comments

- Implement fully the Vienna and Palermo Conventions.
- Implement fully the CFT Convention, in particular by addressing the shortcomings identified in SR II.[98]
- Address the shortcomings identified in relation to the implementation of UNSCRs 1267 and 1373.

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35	**PC**	• The Netherlands have ratified and implemented many provisions of the Palermo and Vienna Conventions. • The Netherlands have ratified but have not fully implemented the CFT Convention as outlined in the various sections of the report. •
SR.I	**PC**	• The Netherlands have ratified but not fully implemented the CFT Convention as outlined in the various sections of this report. • Minor shortcomings remain in respect of the implementation of UNSCR 1267 and 1373.

6.3 Mutual Legal Assistance (R.36-38, SR.V)

6.3.1 Description and Analysis

Legal Framework:

1319. The Netherlands do not have in place overarching legislation for the provision of mutual legal assistance in criminal matters but may grant such assistance directly based on the provisions of Title 10 of the Penal Code, whereby for certain forms of assistance, an international or bilateral treaty basis is required. The provisions of the Enforcement of Criminal Judgments (Transfer) Act further regulate assistance in the identification, tracing, seizing and confiscation of proceeds and instrumentalities of crime upon foreign request.

98 A clear ministerial commitment to pursue the criminalization of terrorist financing (TF) in line with FATF Special Recommendation II (SR II) has been communicated by the Dutch authorities.

1320. The Netherlands have ratified the Vienna, Palermo and TF Conventions as well as a large number of other conventions and treaties for the provision of MLA as indicated below. All of these conventions and agreements may serve as a treaty basis under Title 10 of the Penal Code:

- European Convention on Mutual Assistance in Criminal Matters.
- Additional Protocol to the European Convention on Mutual Assistance in criminal matters.
- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from crime.
- European Convention on the Suppression of Terrorism.
- United Nations Convention against Transnational Organized Crime.
- International Convention for the Suppression of the Financing of Terrorism.
- International Convention for the Suppression of Terrorist Bombings.
- United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.
- United Nations Convention against Corruption.
- Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.
- Framework decision on the European arrest warrant and the surrender procedures between Member States of the European Union.
- Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism.
- Protocol to EU Convention on Mutual Legal Assistance.
- Second Protocol to European Convention on Mutual legal assistance.
- Schengen Implementation Agreement 1990.
- Prüm Treaty (within EU).
- Senningen treaty (with Belgium and Luxemburg).
- Bilateral treaties with the United States of America, Germany, Canada, Australia, Surinam, Hong Kong, Argentina, Mexico, Bahamas, Pakistan, Liberia, Kenia, India, New Zealand, Uganda, Malawi, Tanzania, Trinidad and Tobago.

Widest Possible Range of Mutual Assistance (c. 36.1):

1321. The types of assistance the Netherlands may grant in criminal investigations based on a request from abroad are set out under Title 10 of the Criminal Procedure Code ("CPC").

1322. Pursuant to Article 552h of the CPC Code, requests by foreign authorities for assistance in criminal cases may relate to the carrying out of or cooperation with investigative activities, for example, the sending of documents, dossiers or evidence, the provision of information or the serving or issuing of documents, notices or communications to third parties. Assistance may be granted if a criminal investigation has been initiated in the requesting country and the various legal requirements under Dutch law as set out below are met.

(a) The compelled production, search and seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons

1323. The production of documents and other evidence may be compelled based on a foreign request pursuant to Article 552oa (2) in conjunction with Articles 126nc, 126nd and 126ne of the CPC. Neither a treaty basis nor the involvement of an extraditable offense is required for the taking of such measures. If a request relates to an offense under paragraph 67 of the CPC, which covers a number of offenses punishable with imprisonment for four years or more, the production order may be based on a prosecutorial decision. In all other cases, production orders must be issued by an examining judge upon request by the public prosecutor.

1324. Article 552n in conjunction with Article 552o (3) of the CPC allows for the seizing of evidence, including documents and evidence held by financial institutions. Information and documents held by lawyers, notaries or tax accountants is however subject to legal privilege, which can be lifted in only very limited cases as outlined under Recommendation 28 above. Seizing orders may be issued by the examining judge upon application by the prosecutor's office. Following the seizure, a court order is required before the documents may be handed over to the requesting jurisdictions, whereby the court does not review the case on its merits but merely checks whether the legal requirements for the provision of MLA are met. A treaty basis as well as involvement of an extraditable offense is required in all cases.

1325. Requests for the search of premises may only be ordered by an examining magistrate on the basis of Articles 552n and 552o of the CPC and in all cases require a treaty basis and involvement of an extraditable offense. Article 552oa of the Penal Code also provides that the premises of financial institutions may be subject to search and financial and transaction records be subject to seizures just like any other evidence or premises.

1326. In the absence of a treaty base or an extraditable offense, requests for the seizing of evidence and/or the search of premises may only be granted if a financial investigation can be initiated in the Netherlands based on Article 126 of the CPC.

(b) The taking of evidence or statements from persons

1327. Upon request by a foreign authority, Dutch law enforcement authorities may take evidence or voluntary witness statements from persons based on Articles 552i and 552n (2) of the CPC. Such measures may be taken even in the absence of a treaty basis or dual criminality. The authorities stated that guidelines issued by the Ministry of Justice would also address this point.

1328. In cases where a person is not prepared to appear voluntarily to make the requested declaration, or the foreign authority expressly requests a sworn declaration by the witness or a suspect, the prosecutor may apply to the examining judge for issuance of an order based on Articles 552n (1) and 552o (1) CPC. A treaty basis and dual criminality is required for the judge to issue such an order.

(c) Providing originals or copies of relevant documents and records as well as any other information and evidentiary items

1329. Information and evidence obtained or compelled by law enforcement authorities based on a prosecutorial decision or a decision by the examining magistrate may be provided to the requesting authorities without any restrictions or conditions. Copies of financial transaction records may thus also be provided in such cases.

1330. Where evidence and documents were seized, however, such evidence may be provided to foreign authorities only based on judicial consent by a Dutch court. Article 552p (3) of the CPC provides that the court may grant its consent only if the foreign authorities agree to return the documents and data as soon as possible. In cases where a person with rights to such evidence is not residing in the Netherlands, the original documents or evidence may be provided even in the absence of judicial consent.

(d) Effecting service of judicial documents

1331. Article 552q CPC allows for foreign documents to be served in the Netherlands upon request by a foreign authority. The Dutch rules and regulations for the serving and issuing of domestic documents apply. No treaty basis or dual criminality is required.

(e) Facilitating the voluntary appearance of persons for the purpose of providing information or testimony to the requesting country

1332. As indicated above, requests involving solely the obtaining of information and not requiring any coercive measures may be enforced directly by law enforcement authorities without requiring court or prosecutorial involvement based on Articles 552i and 552n(2) of the CPC. The taking of evidence or statements from persons therefore does not require a treaty basis and may be carried out even in the absence of dual criminality.

(f) Identification, freezing, seizure, or confiscation of assets laundered or intended to be laundered, the proceeds of ML and assets used for or intended to be used for TF, as well as the instrumentalities of such offenses, and assets of corresponding value

1333. See discussion under Recommendation 38 below.

Provision of Assistance in Timely, Constructive, and Effective Manner (c. 36.1.1):

1334. The Minister of Justice in the Netherlands is the central authority in international cooperation on criminal matters and receives all requests for MLA either directly or through diplomatic channels. However, the Netherlands receive a large part (about 40 percent) of its requests from other EU countries. These may be sent directly to the Dutch prosecutorial authority.

1335. Upon receipt of a request, the MOJ verifies that all legal requirements under Dutch law, such as dual criminality and the existence of a treaty basis, are met and forwards the request to one of the International Assistance Centres (IRC's) for execution. Requests that fall within the competence of the regional prosecutor are be forwarded to the relevant regional IRC for execution. Cases that fall within the competency of the national prosecutor are within the national IRC's mandate.

1336. Eight IRCs (seven IRCs with regional competence and one IRC with national competence) have been set up in the Netherlands exclusively to register, deal with and coordinate the execution of MLA requests in criminal matters. Structurally IRCs are part of the public prosecutor's office, even though IRC staff consists of both law enforcement officers and public prosecutors. The authorities stated that every

IRC would be staffed by about 20 professionals, totalling about 160 persons in the Netherlands that work exclusively on MLA.

1337. There are no formal timeframes in place for the processing of MLA requests and statistics on the actual time it took to process MLA requests in the past were not available. The authorities stated that MLA requests would however be executed within two to three months if no coercive measures are requested. It is not clear within what timeframes requests for coercive measures are typically responded to and executed.

No Unreasonable or Unduly Restrictive Conditions on Mutual Assistance (c. 36.2):

1338. As indicated above, in the absence of a treaty base, the types of assistance the Netherlands is able to provide is limited to the obtaining of publicly available information, the obtaining of evidence that is provided by a suspect or witness voluntary or on the basis of a production order. Coercive measures such as searches and seizures of evidence may be taken only on the basis of a multilateral or bilateral treaty providing for search and seizure, or in relation to an extraditable offense as outlined under Recommendation 39 below.

1339. Where a treaty basis is required, MLA cannot be provided merely on the basis of assurance of reciprocity, for example, through a letter rogatory. The authorities stated that in relation to requests for coercive measures or cooperation in fiscal matters, the requirement for a treaty basis is absolute and that requests from non-treaty countries could not be granted. Given the Netherlands's ratification of the Palermo, Vienna and TF Conventions, it seems that in practice, a large number of countries around the world would be considered to have a treaty basis. The statistics provided by the authorities indicate that the absence of a treaty basis has in the past not provided grounds for refusal of MLA requests.

1340. Article 552l sets out further grounds for refusal, none of which seem to be unreasonable or unduly restrictive. MLA requests may be refused if:

- There are grounds to suspect that the investigation for which the request was made was instituted in the foreign country based on religious, philosophical (*i.e.* humanitarian or other beliefs),or political motives or based on the suspect's nationality, race or ethnicity.

- Granting the request would incur double jeopardy.

- The suspect is currently prosecuted in the Netherlands.

1341. Article 552m further lists a number of offenses which would not constitute politically motivated crimes. While offenses under the TF Convention are not expressly listed in this Article, the authorities stated that they will not consider any requests involving TF for refusal based upon political motivation and that MLA is being and has in the past been provided in relation to TF investigations, including in relation to requests submitted by the United States and Morocco. All terrorism offenses are thus considered "de-politicized" by the Netherlands.

1342. For certain forms of MLA, dual criminality is also required. The issue is discussed in great detail under Recommendation 37 below.

1343. The existence of any grounds for refusal is determined by the MOJ. In cases where the execution of a request requires a judicial order, such as for example in relation to search warrants, the court may also deny a requested measure based on grounds for refusal as indicated above.

1344. Statistics provided by the authorities indicate that only few request for MLA in ML or terrorism cases have been refused in the past, whereby double jeopardy posed grounds for refusal in three cases, the existence of an ongoing domestic investigation in one case and lack of dual criminality in only one case (related to terrorism).

Efficiency of Processes (c. 36.3):

1345. Overall, the existence of the eight IRCs seems to warrant an efficient process for dealing with and executing MLA requests through concerted efforts by law enforcement and prosecutorial authorities. Representatives of the MOJ stated that the establishment of IRCs in 2003 significantly improved the efficiency with which MLA requests were handled, as IRC staff is now fully devoted to the issue of MLA whereas before prosecutors dealt with the provision of MLA as part of their regular jobs.

1346. The statistics provided by the authorities do not indicate the number of MLA requests received and processed each year or the timeframes required to execute requests.

Provision of Assistance Regardless of Possible Involvement of Fiscal Matters (c. 36.4):

1347. The authorities stated that the involvement of fiscal matter would not be a ground for refusal of requests. However, requests concerning fiscal issues could only be carried out under Dutch law on the basis of an applicable treaty and after seeking advice of the Minister of Finance. Between 2007 and 2009, 438 requests for MLA were forwarded to the MOF for advice, none of which were denied based on the involvement of fiscal matters.

Provision of Assistance Regardless of Existence of Secrecy and Confidentiality Laws (c. 36.5):

1348. For a detailed discussion on this point see criterion 1 above. Information and documents held by notaries, lawyers and other legal professionals may be accessed only in limited circumstances as indicated under Recommendation 28

Availability of Powers of Competent Authorities (applying R.28, c. 36.6):

1349. Where a request complies with the requirements under Dutch law as outlined above, the full range of powers required under Recommendation 28 are available for use in response to MLA requests. Article 552o specifies that in such situations a request for MLA may have “the same legal consequences as a demand to institute a preliminary judicial investigation as regards to the powers of the public prosecutor.”

Avoiding Conflicts of Jurisdiction (c. 36.7):

1350. The Netherlands have no statutory or formal mechanisms in place dealing with conflicts of jurisdiction. However, should the case arise, the Minister of Justice may on an *ad-hoc* basis determine the best venue for prosecution. In cases involving another EU Member State, Eurojust can mediate and help establish in which country prosecution can best take place.

Additional Element—Availability of Powers of Competent Authorities Required under R28 (c. 36.8):

1351. As indicate above, EU Member States may send a request for MLA directly to the Dutch prosecutorial authorities and in such situations Article 552o would apply. In all other cases, requests have to be sent though the MOJ.

International Cooperation under SR V (applying c. 36.1-36.6 in R. 36, c. V.1):

1352. The analysis under Recommendation 36 applies equally to ML and TF conduct.

Additional Element under SR V (applying c. 36.7 & 36.8 in R.36, c. V.6):

1353. The analysis under Recommendation 36 applies equally to ML and TF conduct.

Dual Criminality and Mutual Assistance (c. 37.1 & 37.2):

1354. Some but not all forms of MLA are subject to dual criminality in the Netherlands. Requests involving solely the obtaining of information (including through a production order) may be enforced directly by the prosecutor's office including in the absence of dual criminality.

1355. Search and seizing measures, however, may only be taken with respect to offenses that meet dual criminality. Dual criminality is defined differently in the Criminal Procedure Code and the Enforcement of Criminal Judgments (Transfer) Act ("ECJTA").

1356. It is worth noting at the outset that the dual criminality as applied by Article 552o (3) of the CPC is not in line with the international standard as it not only requires conduct to be criminalized under both Dutch law and the law of the requesting country but also to qualify as an extraditable offense in relation to the requesting country as indicated below.

1357. As a general rule, requests under Article 552n of the CPC for the searching and seizing of evidence may only be granted if the request relates to conduct which would be an extraditable offense in relation to the requesting country. As outlined under Recommendation 39 below, in relation to requests received from non-Council of Europe countries or countries with which the Netherlands has not entered into a multilateral or bilateral extradition treaty with, only ML involving transnational organized crime or corruption constitute an extraditable offense. Other forms of ML are generally not extraditable offenses. Accordingly, requests for assistance in searches or seizing of evidence may not be granted in relation to such cases.

1358. As an exception to the rule, Article 552o (4) allows for the taking of searching and seizing measures if an explicit treaty provides for it. The Dutch authorities explained that the Schengen Agreement 1990, the Council Framework decision on Confiscation of Crime related Proceeds, Instrumentalities and Property, the Strasbourg Convention on Money Laundering and Confiscation, the Warsaw Convention on the Financing of Terrorism, Money Laundering and Confiscation and a number of bilateral treaties would qualify under Article 552o (4). Thus, requests received from Member States to these treaties would be granted also in relation to ML cases that would otherwise not be extraditable.

1359. Terrorist financing conduct covered under Dutch law is extraditable as indicated under Recommendation 39 below. However, the shortcomings identified under Special Recommendation II may limit the Netherlands ability to assist in the seizing and searching of evidence in TF cases.

1360. Assistance in tracing, seizing and confiscating proceeds and instrumentalities of crime under the ECJTA is available only with respect to criminal offenses for which a financial investigation could have been instituted in the Netherlands.

1361. For requests under the ECJTA, it is required that the offenses in relation to which the request is made could have triggered a financial investigation had the conduct taken place in the Netherlands. Article 126 of the CPC provides that such investigations may be initiated with respect to any crime for which a fine of up to EUR76 000 may be imposed and from which financial benefit of any significance

may be obtained. Both ML under Articles 420bis and 420 quater and participation in a terrorist organization pursuant to Article 140a are punishable with up to EUR76 000. As outlined under Special Recommendation II, the sanctions applicable for offenses under Article 46 depend on the sanction applicable to the prepared criminal offense. Whether or not terrorism financing conduct prosecuted under Article 46 could meet dual criminality under the ECJTA would thus have to be determined on a case-by-case basis.

1362. The authorities stated that in establishing whether a request meets the dual criminality requirements as outlined above, mere technical differences between the law of the requesting state and Dutch law would not pose an impediment to the provision of MLA.

1363. Statistics provided by the authorities indicate that only one request for MLA (FT related) was rejected since 2006 based on a lack of dual criminality

International Cooperation under SR V (applying c. 37.1-37.2 in R. 37, c. V.2):

1364. The analysis under Recommendation 36 covers both ML and TF conduct.

Timeliness to Requests for Provisional Measures including Confiscation (c. 38.1):

1365. Articles 13 and 13a of the ECJTA allows for the Netherlands to assist foreign countries with the identification, freezing, seizing and confiscation of criminal proceeds and instrumentalities. In addition, Section 1 of Title XI of the Penal Code sets out specific rules governing the execution of seizing and confiscation orders by other EU Member States in the Netherlands.

Request for execution of foreign seizing or confiscation order

1366. As a general rule, confiscation orders issued by non-EU Member States may not be registered and directly executed in the Netherlands but have to be transformed by way of an “exequatur” decision by a domestic court order. Seizing orders issued abroad may form the basis for issuance of a domestic seizing order but may otherwise not be given effect to the Netherlands.

1367. Confiscation and seizing measures issued by the court of another EU Member State may be directly executed by Dutch law enforcement authorities based on 552jj.

Request for issuance of domestic seizing or confiscation order

1368. Under Articles 13 and 13a of the ECJTA, upon receipt of a foreign request under the ECJTA, the Dutch authorities may pursue one or both of two avenues to execute the request: They may either initiate a criminal financial investigation to determine the extent of the benefits located or obtained by the suspect in the Netherlands (Article 13) or execute the request by seizing the requested proceeds or instrumentalities (Article 13a).

1369. Both measures under Articles 13 and 13a require a treaty basis. To initiate a financial investigation in the Netherlands under Article 13, it is furthermore required that the relevant conduct would have constituted a criminal offenses punishable with up to EUR76 000 under Dutch law. Article 13a merely requires that the offense in relation to which a measure was requested is a criminal offense under Dutch law.

1370. As outlined above, both ML under Articles 420bis and 420 quater and participation in a terrorist organization pursuant to Article 140a are punishable with up to EUR76 000 and would thus fall within the scope of Article 13 and 13a. The sanctions applicable for offenses under Article 46 are however dependent

on the sanctions applicable to the prepared criminal offense. Whether or not terrorism financing conduct prosecuted under Article 46 of the Penal Code could meet dual criminality under the ECJTA would thus have to be determined on a case-by-case basis.

1371. Under Article 13a, requests for the seizing of proceeds or instrumentalities in the Netherlands may be granted to ensure that objects are available for confiscation under the law of the requesting state or to demonstrate an unlawfully obtained benefit, whereby the requesting country has to show that an order has been given by the competent authorities of the requesting state to seize the relevant objects or that such an order would have been given had the property been located in the requesting country. In cases where a confiscation order has already been issued abroad, there also have to be well-founded reasons to expect that the foreign confiscation order will be enforced in the Netherlands in the short term. Where a foreign order has not yet been issued, the second requirement ("the order for the seizure would have been given") has to be met. The authorities stated that this requirement is not subject to a high threshold but would generally be assumed if so stated by the requesting country. In all cases, he requested seizure has to be possible under Dutch law.

1372. Domestic financial investigation may be initiated under Article 13 based on the foreign request, if it would be possible to initiate such an investigation under Dutch law under Article 126 of the CPC as indicated above. Seizing orders under Articles 94 and 94a of the CPC may be issued if there are well founded reasons to expect that a confiscation order is expected to be made in the foreign proceedings and that enforcement of this order is expected to be requested in the Netherlands with respect to the seized objects. It is not required that a seizing order has been made or that the requesting country shows that a seizing order would have been made under the foreign law.

Property of Corresponding Value (c. 38.2):

1373. Both under Articles 13 and 13a seizing measures are carried out based on Article 94a of the CPC. As outlined under Recommendation 3 above, Article 94a allows for the seizing of any objects to secure the deprivation of the estimated benefit of a crime under Article 36e. The seizing measure may thus be applied to any funds and property, regardless of whether they stem from illicit or legitimate sources. Equivalent value of proceeds may thus be both seized and confiscated upon foreign request.

Coordination of Seizure and Confiscation Actions (c. 38.3):

1374. No formal procedures are in place to coordinate seizure and confiscation actions with other countries. However, the authorities stated that if such case was to arise, the Netherlands may cooperate and liaise with other countries on a case-by-case basis. The Netherlands are also a founder and participant of the CARIN-network of confiscation agencies.

International Cooperation under SR V (applying c. 38.1-38.3 in R. 38, c. V.3):

1375. The analysis under Recommendation 36 covers both ML and TF conduct.

Asset Forfeiture Fund (c. 38.4):

1376. The Netherlands have not set up an asset forfeiture fund. Confiscated funds flow directly to the treasury and thus to general public funds. Although the possibility of setting up such a fund was discussed, there are no plans to do so in the near future.

Sharing of Confiscated Assets (c. 38.5):

1377. Article 13 (c) (2) of the ECJTA provides that assets confiscated or seized based on Articles 13 or 13a may be provided to the requesting authority under the condition that they will be returned to and eventually be transferred into the ownership of the Netherlands. The authorities stated that this process would allow foreign authorities to conduct in rem proceedings. It is possible to deviate from this provision based on a Ministerial decision and to arrange on different sharing proportions.

1378. The authorities stated that within the European Union (Council Framework Decision on mutual recognition of confiscation orders) and countries with which the Netherlands have an asset sharing agreement, such as the United States and the United Kingdom, assets could be shared equally between the requesting and the requested states. In addition, multilateral conventions such as the Council of Europe Convention on Money Laundering 2005, the UN Convention against Transnational Organized Crime 2000 and the UN Convention against Corruption 2004 could serve as a legal basis to share assets with other countries.

Additional Element (R 38)—Recognition of Foreign Orders for a) Confiscation of assets from organizations principally criminal in nature; b) Civil forfeiture and c) Confiscation of Property which Reverses Burden of Proof (applying c. 3.7 in R.3, c. 38.6):

1379. Assets from organizations principally criminal in nature may be confiscated under Articles 13 and 13a ECJTA in combination with Article 36e of the Penal Code.

1380. Confiscation without a prior criminal conviction is generally not possible in the Netherlands. As noted in the analysis section 2 above, in certain cases proceeds can however be confiscated even if they do not result from the offense for which the conviction was obtained.

1381. At the time of the assessment, Dutch law did not yet provide for a reversed burden of proof in confiscation proceedings. However, the authorities advised that a new draft law which would introduce such a reversed burden was submitted to and was in the process of being discussed by parliament.

Additional Element under SR V (applying c. 38.4-38.6 in R. 38, c V.7):

1382. The analysis under Recommendation 36 covers both ML and TF conduct.

Statistics (applying R.32):

It should be noted at the outset that the statistics provided below were received by the assessors at a rather advanced stage of the assessment process. The assessors thus had only little opportunity to discuss these statistics as well as the implementation of the various legal provisions with the authorities but had to form their conclusions mostly based on the information already provided in the report.

1383. According to the statistics provided, between 2006 and 2009, the Netherlands have received 1 727 MLA requests in ML cases and 582 requests in terrorism cases. Of these, 1 687 or 73 percent were granted and processed. The most common ground for refusal or requests was double jeopardy. It is unclear how many requests involved the seizing and confiscation of funds.

1384. Overall, the assessment team considers the statistics sufficient to establish that the Netherlands provides MLA in both ML and Terrorism cases and that few requests have been rejected, usually based on reasonable grounds. Nothing in the provided materials indicate a significant effectiveness issues and the existence of the ICRs seems to facilitate the MLA process.

Money laundering MLA requests		
Total incoming	1 727	
-without coercive measures		1 131
-coercive measures		596
Positive result		1 282
No information about result		185
No result		159
Double request		56
Withdrawn		12
Refused for reasons of lack of dual criminality		0
Refused for reasons of ongoing investigations in the same case in the Netherlands (552l CCP)		1
Refused for reasons of bis in idem		3

Note: Terrorism MLA requests (no distinction is made between different terrorist offences).

Table 2		
Total incoming	582	
-without coercive measures		449
-coercive measures		133
Positive result		405
No information about result		75
No result		73
Double request		18
Withdrawn		2
Refused for reasons of lack of dual criminality		1
Refused for reasons of ongoing investigations in the same case in the Netherlands (552l CCP)		0
Refused for reasons of bis in idem		0

Number of incoming (I) and outgoing (U) requests per offense and per year					
Year	Terrorism	Terrorism	ML	ML	
Type	I	U	I	U	Total
2006	174	82	464	280	1 000
2007	139	66	408	329	942
2008	152	52	443	473	1 120
2009	117	47	412	443	1 019
Total	582	247	1 727	1 525	

Total number of incoming (I) and outgoing (U) requests			
Offense	Type		
	I	U	Total
Terrorism	582	247	829
Money Laundering	1 727	1 525	3 252
Total	2 309	1 772	4 081

Number of incoming and outgoing requests per country over the years 2006-2009	
Country	**Total**
Afghanistan	2
Albania	5
Algeria	2
Andorra	15
Argentina	7
Armenia	1
Aruba[1]	9

Number of incoming and outgoing requests per country over the years 2006-2009	
Australia	18
Austria	62
Azerbaijan	1
Bangladesh	1
Belarus	1
Belgium	940
Belize	1
Bermuda	3
Bolivia	1
Bosnia en Herzegovina	7
Brazil	17
BVI	2
Bulgaria	25
Canada	28
Cape Verde	1
Chile	7
China	19
Colombia	47
Costa Rica	1
Croatia	
Cuba	1
Cyprus	8
Czech Republic	16
Denmark	16
Dominican Republic	7
Ecuador	11
Egypt	3
Estonia	4
Fiji	1
Finland	4
France	247
Gambia	1
Germany	576
Ghana	2
Gibraltar	8
Greece	8
Guatemala	2
Guinea	1
Guyana	1
Hungary	11
Hong Kong, China	4
Ireland	36
Iceland	3
India	5
Indonesia	6
Isle of Man	1
Israel	10
Italy	68

Number of incoming and outgoing requests per country over the years 2006-2009	
Jamaica	3
Japan	1
Jersey	1
Jordan	2
Kazakhstan	6
Kenya	1
Kosovo	2
Kyrgyzstan	3
Latvia	9
Lebanon	1
Liechtenstein	35
Lithuania	2
Luxembourg	51
Macedonia	1
Malta	7
Morocco	72
Mexico	8
Moldavia	1
Monaco	7
Montenegro	1
Netherlands	59
Netherlands Antilles[2]	74
Nicaragua	1
New Zealand	2
Nigeria	8
Norway	27
Ukraine	10
Pakistan	11
Panama	6
Peru	3
Philippines	6
Poland	35
Portugal	35
Romania	31
Russia	37
Rwanda	2
Saudi Arabia	1
Scotland	1
Serbia	4
Serbia en Montenegro	2
Singapore	3
Slovenia	9
Slovakia	13
Soudan	4
South-Africa	3
Spain	317
Sri Lanka	2
Suriname	59

Number of incoming and outgoing requests per country over the years 2006-2009	
Sweden	13
Switzerland	174
Syria	1
Thailand	12
Trinidad and Tobago	2
Tunisia	3
Turkey	110
United Arab Emirates	18
United Kingdom	311
United States	145
Unknown country	1
Uruguay	3
Venezuela	16
Vietnam	1
Zimbabwe	1
Total	**4081**

[1] Aruba is part of the Kingdom of the Netherlands and assistance provided to Aruba is thus technically not considered to be international cooperation.
[2] The Dutch Antilles are part of the Kingdom of the Netherlands and assistance provided to this country is thus technically not considered to be international cooperation.

6.3.2 Recommendations and Comments

- Amend the dual criminality as applied by Article 552o (3) of the CPC to ensure that the Netherlands can assist any foreign country in searching and seizing of evidence in relation to any ML case.

- Address all shortcomings identified under Special Recommendation II to ensure that the dual criminality requirements as applied under the ECJTA and the CPC do not limit the Netherlands' ability to provide MLA.

- Ensure that access to information held by notaries, lawyers and accountants can be granted in all cases, including in the context of MLA.

- To establish the effective application of the existing framework, maintain statistics on the number of requests received and granted in relation to the seizing and confiscation of assets and the total number of assets seized and confiscated based on foreign request.

- Consider putting in place measures to ensure that all forms of assistance may also be granted in the absence of a treaty basis, for example based on reciprocity.

6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.3 underlying overall rating
R.36	**PC**	• In relation to a large number of countries, the Dutch authorities may provide assistance in searching and seizing of evidence only in ML cases involving transnational organized crime or corruption but not any other types of predicate offenses. • Although the statistics do not imply that there are significant difficulties in practice, the shortcomings identified under Special Recommendation II may limit the Netherlands ability to provide MLA. • Scope of legal privilege hinders the possibility for law enforcement authorities to access information and documents held by notaries, lawyers and accountants.
R.37	**LC**	• For non-Council of Europe members and countries with which the Netherlands have not signed a multilateral or bilateral extradition treaty with, the dual criminality as applied by Article 552o (3) of the CPC is not fully in line with the international standard in that it is not sufficient for conduct to be criminalized under both Dutch law and the law of the requesting country but with some exceptions also requires for conduct to qualify as an extraditable offense.
R.38	**PC**	• Although the statistics do not imply that there are significant difficulties in practice, the shortcomings identified under Special Recommendation II may limit the Netherlands ability to provide MLA. • Scope of legal privilege hinders the possibility for law enforcement authorities to access information and documents held by notaries, lawyers and accountants. • It was not established that the Netherlands effectively seizes and confiscates funds based on foreign request.
SR.V	**PC**	• Although the statistics do not imply that there are significant difficulties in practice, the shortcomings identified under Special Recommendation II may limit the Netherlands ability to provide MLA. • Scope of legal privilege hinders the possibility for law enforcement authorities to access information and documents held by notaries, lawyers and accountants.

6.4 Extradition (R.37, 39, SR.V)

6.4.1 Description and Analysis

Legal Framework:

1385. Extradition procedures in the Netherlands are governed by the Extradition Act and any relevant extradition treaty that may apply to a certain case. As a general rule, extradition from the Netherlands may only be granted based on a treaty.

1386. The Netherlands has entered into relevant multilateral extradition instruments (European Convention on Extradition–Council of Europe), EU Council Framework Decision on Arrest Warrant, Kingdom of the Netherlands Statute (Aruba, Netherlands Antilles, St. Maarten) and bilateral extradition treaties with Australia, Canada, Hong Kong SAR, Suriname, Trinidad and Tobago, and the United States. In relation to those approximately 60 countries, the more specific provisions of the agreement supersede Article 51a of the Extradition Act.

1387. In relation to all other countries, only offenses specifically listed in Article 51a of the Extradition Act are extraditable based on the consent by the person concerned. In relation to ML, Article 51a lists the following offenses:

- The crimes that were penalized in Articles […] 420bis up to and including 420quater of the Criminal Code Law in so far as the fact is described in Articles 5, 6, 8 and 23 of the coming about of the Convention Against Organized Crime.

- The crimes that were penalized in Articles […] 420bis, 420ter and 420quater of the criminal code in so far as the fact is described in […] of the Convention Against Corruption.

- Crimes that are covered by the European Convention on Extradition.

1388. In relation to TF, Article 78 of the CPC, which makes the crime of "preparation" applicable whenever the law makes reference to any specific crime, in combination with 51a of the Extradition Act make the financing of any offense defined in the nine conventions and protocols annexed to the TF Convention an extraditable offense. Article 140 of the CPC, which criminalizes the financing of a criminal organization, is also expressly listed as an extraditable offense under Article 51a of the Extradition Act. Furthermore, with respect to Council of Europe countries, any conduct punishable with one year or more qualifies as an extraditable offense under the European Convention on Extradition.

Dual Criminality and Mutual Assistance (c. 37.1 & 37.2):

1389. Articles 2 and 3 of the Extradition Act provide that extradition may only be granted on the basis of a treaty. In the absence of a specific extradition treaty as indicated above, Section 51a of the Extradition Act determines whether or not a specific offense is extraditable. This is not fully in line with the international standard, which requires that "for extradition, the requested state should have no legal impediment to render assistance where both countries criminalize the conduct underlying the offense". In the context of the Netherlands, conduct would not only have to be criminalized but also fall within Article 51a of the Extradition Act for it to qualify as extraditable.

1390. The authorities stated that in establishing whether a request meets the dual criminality requirements as outlined above, mere technical differences between the law of the requesting state and Dutch law would not pose an impediment to the provision of MLA.

1391. Between 2006 and 2009, two extradition requests were denied based on lack of dual criminality.

Money Laundering as Extraditable Offense (c. 39.1):

1392. For requests from other Council of Europe Member States based on the European Convention on Extradition or countries with which the Netherlands has entered into a multilateral or bilateral extradition treaty with both ML and TF qualifying as extraditable offenses. Both the Convention and the listed extradition treaties apply to offenses that are punishable with imprisonment of twelve months or more. The ML offenses in the Dutch Penal Code and Articles 140a and 46 of the Penal Code, which may be used to prosecute some forms of TF, exceed this threshold and are thus extraditable offenses. However, the financing of individual terrorists is not sufficiently criminalized in the Netherlands and the shortcomings identified under Special Recommendation II with respect to Article 140 of the CPC may have a limiting effect on the Netherlands' ability to extradite in certain cases.

1393. With respect to extradition requests in ML cases received from any other country, Article 51a establishes ML as an extraditable offense only if it involves situations within the scope of the Palermo Convention (ML cases involving transnational organized crime) or of the Merida Convention (ML cases involving bribery and corruption). Any other forms of ML, including drug and terrorism related ML, are not expressly covered by Article 51a and are thus not extraditable offenses under Dutch law.

1394. The authorities argued that in drug related ML cases, extradition could take place based on the receiving of stolen goods provision, which is an extraditable offense under Article 51a. However, given that the receiving of stolen goods offense is limited compared to the ML offense under the Vienna

Convention both in terms of scope and material elements, this argument does not fully address the identified shortcoming.

1395. With respect to extradition requests for TF from non-Council of Europe member states or countries with which the Netherlands has no multilateral or bilateral extradition treaty, Article 78 of the CPC in combination with 51a of the Extradition Act make the financing of any offense defined in the nine conventions and protocols annexed to the TF Convention an extraditable offense. Article 140 of the CPC, which criminalizes the financing of a criminal organization, is also expressly listed as an extraditable offense under Article 51a of the Extradition Act. As already stated above, however, the financing of individual terrorists is not expressly covered and the shortcomings identified under Special Recommendation II may limit the Netherlands' ability to extradite in TF cases.

Extradition of Nationals (c. 39.2):

1396. Section 4 of the Extradition Act prohibits the extradition of Dutch nationals unless the Minister of Justice obtains an adequate guarantee from the requesting country that if the extradited Dutch national was to be sentenced to imprisonment by the foreign court, the person would be allowed to serve the sentence in the Netherlands. Extradition for the execution of a sentence is therefore not possible.

1397. The Extradition Act makes no reference to any obligation of the Dutch authorities to initiate domestic proceedings in cases where extradition is denied purely on the basis of nationality. With respect to TF offenses committed in another country, such an obligation exists pursuant to Article 552hh of the Penal Code. Between 2006 and 2010, four out of 539 extradition requests were refused due to Dutch nationality. In the absence of any statistics on the total number of requests received in relation to Dutch nationals and the number of such requests granted, it is not possible to put this number in context and to determine whether the Netherlands successfully extradites its own nationals.

Cooperation for Prosecution of Nationals (applying c. 39.2(b), c. 39.3):

1398. See information on 39.2. The assessors could not verify that there is a requirement under Dutch law to submit the case to the authorities for the purpose of prosecution if an extradition request is denied purely on the basis of nationality. The authorities indicated, however, that there would be a general willingness to cooperate with foreign authorities should the requesting state wish to transfer criminal prosecution to the Netherlands.

Efficiency of Extradition Process (c. 39.4):

1399. The Minister of Justice is the central authority in extradition cases. Extradition requests may be sent directly to the Ministry of Justice and do not have to be sent through diplomatic channels.

1400. Upon verification that the legal requirements under the Extradition Act are met, the MOJ sends a request to the public prosecutor's office who in turn will apply to court for execution of the request. The court will either approve the request or not, taking into account the legal requirements under Dutch law.

1401. If the court approves its execution, the request will be sent back to the MOJ who may then issue a formal decision to grant the request. The court's decision may also be appealed before the Supreme Court and the Minister of Justice's decision may be appealed as an administrative decision. If the court decides that the request may not be executed under Dutch law or international treaties, such as the ECHR, the request must be rejected by the Minister of Justice.

1402. Detailed provisions on how and the timeframes within which extradition requests are to be dealt with as well as the requirements such requests must meet are set out in Part B of the Extradition Act. Once

the court has decided whether a specific request meets the requirements under Dutch law, the Minister of Justice is required under Section 33 of the Extradition Act to decide "as soon as possible" whether a request is to be granted. The authorities stated that extradition proceedings would take about one year in relation to non-EU countries and a maximum of 60–90 days in relation to Council of Europe countries. The length of an extradition procedure with regard to a non-Council of Europe country invariably depends on whether the person appeals against the decision of the court and the MOJ. In the absence of any statistics in relation to extradition, however, the assessors could not determine that the extradition proceedings in the Netherlands are dealt with efficiently and in a timely manner.

1403. Grounds for refusal of extradition requests are set out in the Extradition Act and include the following:

- The offense with respect to which the request is made is punishable with the death penalty in the requesting state and the MOJ has not received an undertaking from the requesting state that the death penalty will not be imposed.
- Criminal proceedings are pending in the Netherlands.
- The person has been prosecuted and either been acquitted or convicted under Dutch law.
- The statute of limitation on the penalty has lapsed.
- The Minister of Justice is of the view that the prosecution abroad is motivated by the suspect's religious or political convictions, his nationality, race or population group, or that the suspect would suffer from exceptional hardship due to his youth, age or ill-health.
- The investigation seems to be in relation to a political offense.

1404. Section 11 of the Extradition Act sets out the types of offenses which may not be considered "political offenses." The provision expressly lists the European Convention for the Suppression of Terrorism.

Additional Element (R.39)—Existence of Simplified Procedures relating to Extradition (c. 39.5):

1405. As indicated above, all requests for extradition may be sent directly to the MOJ. There is no need to go through diplomatic channels. Furthermore, simplified procedures are available under Part E of the Extradition Act for cases in which a person agrees to be extradited.

Additional Element under SR V (applying c. 39.5 in R. 39, c V.8)

1406. The provisions described above apply equally to ML and TF.

Statistics (R.32)

1407. The authorities provided an excerpt of "The Standard Questionnaire on Quantitive Information Relating to the Practical Operation of the European Arrest Warrant", which indicates that in 2009 the Netherlands have extradited 408 individuals to 26 countries based on a European arrest warrant. Of the 408 individuals, 99 were Dutch nationals. It is however unclear how many of those requests related to ML or TF cases.

1408. For extradition outside the context of the European Arrest Warrant, statistics provided by the authorities indicate that between 2006 and August 2010, the Netherlands received a total number of 586 extradition requests. Of the 586 requests, 4 related to ML (from Colombia, Switzerland, the UK and Armenia) and 17 related to terrorism offenses (from Turkey, Morocco, Sudan, Bosnia and Herzegovina, the USA and Uzbekistan). These statistics are however not complete as for 172 of those requests, the crime in relation to which the request was made was not registered. The actual number of extradition requests in ML cases could thus be higher. Furthermore, the statistics do not indicate how many of those cases were granted and rejected, and the time required to complete extradition proceedings in each case.

6.4.2 Recommendations and Comments

- In relation to non-Council of Europe members and countries with which the Netherlands have not signed a multilateral or bilateral extradition treaty, ML should be an extraditable offense in all cases, including drug related cases.

- The shortcomings identified under Special Recommendation II should be remedied so as to allow for extradition in all cases relating to the FT, and the financing of individual terrorists become an extraditable offense.

- Amend the law to set out a legal obligation by Dutch authorities to prosecute a suspect domestically in cases where an extradition request is denied purely on the basis of nationality.

- Maintain more detailed statistics on the number of extradition request received in ML and TF cases and the numbers of cases rejected and granted as well as the time required to complete extradition proceedings to ensure that extradition proceedings in the Netherlands are dealt with efficiently and in a timely manner.

6.4.3 Compliance with Recommendations 37 & 39, and Special Recommendation V

	Rating	Summary of factors relevant to s.6.4 underlying overall rating
R.39	**PC**	• In relation to non-Council of Europe members and countries with which the Netherlands have not signed a multilateral or bilateral extradition treaty, only ML offenses involving transnational organized crime or corruption are extraditable offenses under Dutch law. • There is no obligation by Dutch authorities to prosecute a suspect domestically in cases where an extradition request is denied purely on the basis of nationality. • Statistics were not sufficiently detailed to determine that the extradition proceedings in the Netherlands are dealt with efficiently and in a timely manner.
R.37	**LC**	• In relation to non-Council of Europe members and countries with which the Netherlands have not signed a multilateral or bilateral extradition treaty, the dual criminality as applied in the Netherlands is not in line with the international standard in that it is not sufficient for conduct to be criminalized under both Dutch law and the law of the requesting country but also requires for conduct to fall under an offense listed in Article 51a of the Extradition Act.
SR.V	**PC**	• The shortcomings identified under Special Recommendation II may limit the Netherlands' ability to extradite in certain TF cases. • Statistics were not sufficiently detailed to determine that the extradition proceedings in the Netherlands are dealt with efficiently and in a timely manner.

6.5 Other Forms of International Co-Operation (R.40 & SR.V)

6.5.1 Description and Analysis

Legal Framework:

1409. WWFT establishes confidentiality rules and the scope for disclosure. Article 22 of the WWFT forbids any authority from disclosing confidential information except where necessary for the performance of that party's duties or as required under the Act. There is also explicit provision for information exchange between the FIU and the supervisory authorities in Articles 13g and 25 of the WWFT. In addition, there are provisions relating to the disclosure of information between domestic and foreign supervisory authorities in the Wft (Articles 1.51 and 1.90), to prosecutors (Article 1.92) and to others. The Wgt also provides for appropriate disclosures.

Widest Range of International Cooperation (c. 40.1):

Supervision

1410. Article 22 of the WWFT allows disclosure of information for the purpose of fulfilling duties under the WWFT. It is likely that such information as requested from a foreign supervisor would relate to the performance of a regulated entity with its AML/CFT obligations and this would be consistent with Article 22, since the assistance of a foreign supervisor in enforcing such compliance would be consistent with the responsibilities of the DNB and AFM to monitor compliance by regulated financial entities. In addition, Article 1.51 (2) of the Wft gives the supervisory authorities in The Netherlands the power to provide information to supervisory authorities in other Member States where this is necessary for the performance of their duties. Section 1.65 gives similar authority with respect to supervisory authorities in non-Member States. These powers extend to AML/CFT matters such as the compliance of individual institutions with their regulatory obligations provided that the argument is accepted that the Wft powers

1411. can be used in respect of AML/CFT obligations (for a fuller discussion of this matter refer to the legal framework section of the report on supervision). The authorities are able to provide information without the need for a formal agreement such as a memorandum of understanding (MoU) although it seeks to conclude such agreements where appropriate. In practice, supervisor to supervisor cooperation in the context of AML/CFT would be most likely about the compliance by international financial entities with their AML/CFT obligations. The authorities state that there are very few requests of this nature.

FIU-Netherlands

1412. The FIU of the Netherlands is one of the founding members of the Egmont Group and cooperates actively in the exchange of information. Within the European Union FIU-NL is the FIU that receives the largest number of EU FIU requests. These requests are made via the FIU.NET web and covers the years 2007 (707), 2008 (1.032), 2009 (874).

FIU.NET Requests RECEIVED by NL				
	2007	2008	2009	
COUNTRY	SUBJECTS	SUBJECTS	FILES	SUBJECTS
Belgium	581	837	234	656
Cyprus			2	3
Finland	1	3	15	87
France	36	43	9	39
Germany		1	3	3
Greece			2	6

FIU.NET Requests RECEIVED by NL				
Italy			2	14
Luxembourg	53	74	13	53
Poland			2	2
Slovakia			3	3
Slovenia	2			
Spain	23	74	6	18
United Kindom	11			
TOTAL	**694**	**1 032**	**291**	**884**

FIU.NET Requests SENT by NL				
	2007	2008	**2009**	
COUNTRY	**SUBJECTS**	**SUBJECTS**	**FILES**	**SUBJECTS**
Belgium	76	47	22	110
Czech Republic	8			
Denmark			4	4
France	20	1	3	4
Germany	49	10	4	15
Greece		3	1	1
Italy	9		2	7
Latvia	3			
Luxembourg	5	2		
Poland	1			
Slovenia			1	1
Slovakia	1		1	1
Spain	23	12	5	21
United Kingdom	10			
TOTAL	**205**	**75**	**43**	**164**

Egmont Secure Web requests received			
	2007	**2008**	**2009**
Belgium	100	121	85
Bulgaria	10	6	10
France	5	3	9
Guernsey	-	10	9
Luxembourg	34	33	26
Netherlands Antilles	7	9	10
Spain	10	8	9
Switzerland	10	5	8
UK	26	16	19
Ukraine	12	8	11
Other countries	136	155	124
TOTAL	**350**	**374**	**320**

Egmont Secure Web requests sent			
	2007	**2008**	**2009**
Belgium	11	22	15
Bulgaria	1	-	3
Cyprus	1	1	3
Germany	2	9	7
Ireland	-	3	5
Norway	1	12	5
Spain	3	6	4
Sweden	3	21	30
Switzerland	6	2	4
UK	3	5	20
Other countries	26	39	41
TOTAL	**57**	**120**	**137**

Provision of Assistance in Timely, Constructive, and Effective Manner (c. 40.1.1):

Supervision

1413. As noted above, the supervisors are able to give information without the need for an MoU and are able to give information in a timely manner. Their experience with respect to all supervisory cooperation is that information can be exchanged in a timely manner but there is little call for supervisory exchange of information on AML/CFT matters.

FIU-Netherlands

1414. The Dutch FIU provides information in a rapid, constructive and effective manner. A random check done during the onsite visit on a sample of requests received/responses provided through the Egmont Secure Web, indicated that the information is provided in a reasonable timeframe (an average of five days, two when the request was urgent).

Law enforcement

1415. Law enforcement agencies are able to provide information in a rapid, constructive and effective manner. They use mechanisms such as Europol, Eurojust, Interpol, administrative mutual assistance on customs issues.

Clear and Effective Gateways for Exchange of Information (c. 40.2):

FIU-Netherlands

1416. The Dutch FIU has a policy to exchange information only with FIUs that are members of the Egmont Group.

Supervision

1417. The MoU template used by the DNB covers AML/CFT matters and the multilateral MoU of the International Association of Insurance Supervisors (IAIS) covers AML/CFT cooperation. The AFM is a

signatory to the International Organisation of Securities Commission (IOSCO) Multilateral MoU, although this does not relate directly to AML/CFT matters except where information relevant to AML/CFT were part of a request for information on securities regulation enforcement. These MoUs are gateways for information exchange but otherwise, the mechanism is direct supervisor to supervisor contact for information exchange between counterparts.

1418. The authorities state that they are able to provide rapid assistance. No information from third countries on supervisory cooperation was received.

Law enforcement

1419. There are a number of mechanisms and channels facilitating prompt exchanges of information directly between counterparts. These are:

- **The BOOM international contact point:** The Netherlands has had a central unit for the confiscation of the proceeds of crime since 1993, the Proceeds of Crime Bureau (BOOM), which is part of the Public Prosecution Service. Under EU Council Decision 2007/845/JHA, all EU Member States must establish a National Assets Recovery Office (ARO) and the BOOM was designated by the Minister of Justice as the Netherlands' ARO, and has been operational as such since January 1, 2010. It serves as the Dutch center of expertise and national office dealing with legal assistance in respect of the confiscation of the proceeds of crime. Requests from EU countries for legal assistance falling into this category may be sent directly to the ARO. Requests from outside the European Union must be channeled via the Central Authority, *i.e.* the Ministry of Justice. The Dutch ARO also has other duties concerning the provision of information to foreign countries and the management of pre-judgment seizures.

- **CARIN:** The Netherlands are part of the Camden Assets Recovery Inter-Agency Network (CARIN) which aims to enhance the effectiveness of efforts in depriving criminals of their illicit profits. This is now a major law enforcement tool in targeting organized crime gangs with particular reference to financial deprivation. There is added value in that membership of the group will improve cross-border and inter-agency cooperation as well as information exchange, within and outside the European Union. The Official start of CARIN took place in 2004.

- **KLPD liaison officers:** They are usually stationed in countries that maintain considerable criminal contacts with the Netherlands or countries whose legal systems are strongly different. Liaison officers maintain contact with investigation services and their local procedures. They solve problems and communication disturbances, exchange information and by doing so look after the Dutch interests in requests for formal legal aid in criminal cases and a number of investigation procedures. There are liaison officers from the KLPD in 16 countries.

- Other channels such as Interpol, Europol and Eurojust.

Spontaneous Exchange of Information (c. 40.3):

FIU-Netherlands

1420. Except with regard to the exchange of law enforcement-related information (that, outside the EU, can only be provided to FIU of law enforcement-type) there would appear to be no barrier to exchanges of information either spontaneously, or on request.

Supervision

1421. The exchange of information between supervisors on the compliance with AML/CFT obligations by financial institutions can take place under Article 22 of the WWFT without a request for information and therefore could be spontaneous. For exchange of information under the Wft, there is no reference to a request for information when the disclosure is to a non Member State under Article 1.65. With no need for a request, the disclosure could be spontaneous. Article 1.51 in respect of Member States includes a reference to requests for information in Article 1.51(2). However, the overarching authority to collaborate in Article 1.51 does not refer to requests and it is unlikely that the intention of the law would be to have stricter conditions for Member States than non Member States. The natural interpretation is that this disclosure also does not require a request and could be spontaneous. The authorities state that there are relatively few requests for information on AML/CFT compliance and the incidence of spontaneous information exchange is even rarer. Nevertheless, the powers exist for such exchanges.

Law enforcement

1422. For cooperation among members of the EU, pursuant to Article 7 of the EU‘s Framework Decision, information and intelligence can be provided by law enforcement agencies, without the need for any prior request, in cases where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention, or resolution of a concluding catalogue of offenses (among which ML is included).

Making Inquiries on Behalf of Foreign Counterparts (c. 40.4):

1423. The power of the supervisory authorities to make enquiries and demand information rests on Chapter 5.2 of the Awb which are granted to the supervisory authorities for monitoring compliance with AML/CFT obligations by Article 24 (4) of the WWFT. This gives powers to obtain information for the performance of the duties of the supervisor in monitoring compliance. It is likely that most requests for supervisory cooperation would be in connection with compliance by regulated financial entities with their AML/CFT obligations and, in such a case, the investigation powers in Article 24 (4) would permit the authorities to investigate on behalf of foreign supervisory authorities.

1424. In practice, the only enquiries that would be appropriate for the supervisory authorities to make would concern the compliance behavior of supervised institutions. Such enquiries would be perfectly proper under the powers of the supervisors under the Wft.

FIU Authorized to Make Inquiries on Behalf of Foreign Counterparts (c. 40.4.1):

1425. The Dutch FIU can search its own database and other databases on behalf of foreign counterparts. However, Criminal-related information and information that can be obtained through access to law enforcement databases can only be provided to FIU that are of law enforcement-type (unless they are FIUs of an EU member country). With regard to the information provided—from the sample of responses seen by the assessors—the information was mainly related to confirm whether the requested person was in the UTR database or information from the Commercial Register.

1426. In order to be able to provide information from the UTR database (which, as explained earlier is classified as personal data) the FIU transforms automatically the requests received from foreign FIU into STR. The relevant information (personal and transaction-related data) is loaded in the STR database, without any reference that the request comes from a foreign FIU.

Conducting of Investigations on Behalf of Foreign Counterparts (c. 40.5):

Law enforcement

1427. One way the Netherlands cooperates with other countries in a criminal investigation is with the instrument of the Joint Investigation Team (JIT). The JIT has been used several times with different countries (*i.e.* Belgium, France, Germany, and the United Kingdom). The legal base is Article 13 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of May 29, 2000 (OJ C 197, 12.7.2000, p. 3) and the Council Framework Decision of June 13, 2002 on joint investigation teams (OJ L 162, 20.6.2002, p. 1). The main objective of a JIT is to obtain information and evidence about the crime for the investigation of which it has been established.

1428. Moreover, the Police and the National Prosecution Service work together on international requests in the so called *Internationale Rechtshulp Centra*, IRC's. This ensures that no time is lost in the execution. There is also a national computer tracking system used by police and prosecutors for international legal assistance.

Supervision

1429. The observations made above with respect to making enquiries on behalf of foreign supervisory authorities would also apply to investigations, since they would rest on the same powers in Article 24 of the WWFT.

1430. No Unreasonable or Unduly Restrictive Conditions on Exchange of Information (c. 40.6):

FIU

1431. There are no unreasonable conditions on providing assistance. The only condition for the provision of information that appears to be unduly restrictive is that criminal and law enforcement information to which the Dutch FIU can have access to can only be provided, outside the EU, to FIUs that are of law enforcement nature.

Supervision

1432. The same observation applies to supervisory cooperation. The main restriction is that the purpose of collaboration must be for the purpose of fulfilling duties under the WWFT or Wft. This would allow for information to be exchanged on regulated entities' compliance with their obligation. The WWFT and Wft both require that the protection given to information must match that given in the EU Directives. Neither seems unreasonable conditions.

Law enforcement

1433. No unduly or unreasonable restrictive conditions have been noticed in the legal framework on exchange of information, except in relation to the scope of legal professional secrecy, as evidenced in the analysis for R.28.

Provision of Assistance Regardless of Possible Involvement of Fiscal Matters (c. 40.7):

Supervision

1434. The list of reasons for refusing assistance does not include the possibility that the matter under investigation is related to fiscal matters. However, it would not be appropriate for a supervisory authority

to make enquiries that were solely for fiscal investigations, since such enquiries should be conducted by the appropriate tax authority.

Law enforcement

1435. The fact that the request is also considered to involve fiscal matters is not a ground for refusal of request. Requests that solely concern fiscal (tax) issues can only be carried out if a treaty is applicable and if the Minister of Finance gives permission to execute the request in question.

Provision of Assistance Regardless of Existence of Secrecy and Confidentiality Laws (c. 40.8):

Supervision

1436. Article 22 of the WWFT imposes a confidentiality obligation but allows disclosure where this is necessary for the performance of duties. Article 1.51 (2) of the Wft gives the supervisory authorities in the Netherlands the power to provide information to foreign supervisory authorities in Member States where this is necessary for the performance of their duties, notwithstanding the confidentiality obligation. Article 1.65 provides the same powers for non-Member States.

Law enforcement

1437. Secrecy provisions cannot be used to deny requests of law enforcement authorities, except where legal professional privilege applies.

Safeguards in Use of Exchanged Information (c. 40.9):

General framework–including law enforcement agencies

1438. The Dutch Data Protection Authority (*College Bescherming Persoonsgegevens*, CBP) supervises the fair and lawful use and security of personal data. The DPA supervises the compliance with acts that regulate the use of personal data. This means that the Dutch DPA supervises the compliance with and application of the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*, Wbp;), the Police Data Act (*Wet politiegegevens gegevens*, Wpg), and the Municipal Database (Personal Records) Act (*Wet gemeentelijke basisadministratie*, Wgba).

Supervision

1439. Article 1.89 of the Wft explicitly extends confidentiality protection to information received from a foreign supervisory body. Article 22 of the WWFT extends confidentiality protection to information received by virtue of the Act and it is unlikely that information received from a foreign supervisory authority would be so regarded. In practice, it is unlikely that the supervisory bodies would receive information from foreign supervisors that was not subject to the protection of the Wft, since the only information likely to be received would be relevant to the supervision of regulated bodies.

FIU

1440. All the information received by the Dutch FIU, including from foreign FIUs is securely protected. See analysis under criterion 26.7.

Additional Element—Exchange of Information with Non-Counterparts (c. 40.10 & c. 40.10.1):

1441. Article 22 of the WWFT permits exchanges of confidential information with other domestic authorities who are not the counterparts of the supervisory bodies.

1442. However, the international information exchange provisions in Wft apply only to foreign supervisory bodies. There would be no scope for the supervisory authorities in The Netherlands to exchange confidential information with foreign authorities who were not supervisors. However, the Dutch supervisors can exchange information with other domestic authorities who would be in a position to exchange information with their counterparts in foreign countries.

Additional Element—Provision of Information to FIU by Other Competent Authorities pursuant to request from Foreign FIU (c. 40.11).

1443. Article 22 of the WWFT allows disclosure of confidential information by any party with responsibilities under the WWFT (including the supervisory bodies. This applies where the disclosure is required for the performance of an authority's duties. The FIU is under a duty to cooperate with foreign FIUs and thus any information held by a supervisory authority that was requested by a foreign FIU could be disclosed. The only limitation, as described earlier, is with regard to criminal or law enforcement-related information that can only be disclosed outside the EU, to a law enforcement-type FIU.

International Cooperation under SR V (applying c. 40.1-40.9 in R. 40, c. V.5 and additional element):

1444. All of the observations above apply with equal validity to SR V. But shortcomings identified under Special Recommendation II have a limiting effect on the Netherlands ability to provide information in TF investigations

Analysis of effectiveness

1445. The Dutch FIU provides effectively and proactively information required by foreign FIUs, except for law enforcement related information, that can only be disclosed, outside the EU, to law enforcement-type FIUs.

1446. The authorities are willing to engage in international cooperation. They have the powers to do so and, although the powers do not require a memorandum of understanding to be in place, the DNB has concluded a number of such agreements.

1447. The use of the international cooperation powers on AML/CFT matters by the supervisory authorities is relatively rare. This is understandable, given their role. It would not be appropriate for them to use their powers to obtain information for law enforcement in the Netherlands or elsewhere. The powers were not provided for that purpose and there are other authorities with appropriate powers to gather and share information for law enforcement. It might be expected that there would be more sharing of information between the DNB/AFM and foreign supervisors about the diligence of particular regulated entities in implementing AML/CFT defenses. In practice, this is not so. It may be that this is because the Netherlands' supervisory authorities are perfectly prepared to permit foreign supervisors to carry out direct on-site visits in Holland, just as the Dutch supervisors will conduct on-site visits abroad. Moreover, where information on implementation is required, home-based supervisors are able to obtain much of the necessary information from the head office of an international group.

1448. Notwithstanding the limited use of the information sharing powers, the mission was satisfied that the powers were sufficient and that the supervisors were willing to use them. The supervisory authorities have the normal powers of supervisors to cooperate with international counterparts and with domestic

authorities where this is necessary for the performance of their duties. These powers meet the terms of Recommendation 40.

6.5.2 *Recommendations and Comments*

- The authorities should review the scope of professional secrecy obligations and consider amending the CPP to make sure that it does not subject exchange of information to unduly restrictive conditions.

- The authorities should maintain statistics on international cooperation by law enforcement agencies.

6.5.3 *Compliance with Recommendation 40 and Special Recommendation V*

	Rating	Summary of factors relative to s.6.5 underlying overall rating
R.40	**LC**	• The broad scope of legal professional secrecy introduces an unduly restrictive condition to exchange of information. • Lack of statistics to assess the effectiveness of international cooperation by law enforcement agencies.
SR.V	**PC**	• Shortcomings identified under Special Recommendation II have a limiting effect on the Netherlands ability to provide information in TF investigations.

7. OTHER ISSUES

7.1 Resources and Statistics

	Rating	Summary of factors underlying rating
R.30	**LC**	• Staff training is not required on an annual basis and there are insufficient data on the nature of training received by supervisory staff • Level of training of some police officers and ability to deal with complex cases critically assessed by members of the judiciary
R.32	**LC**	• Accurate and complete statistics are not maintained on: (1) the number and types of predicate offenses committed in the Netherlands; (2) the number of investigations conducted for ML and FT, including information on how these cases where initiated and the types of crime these cases relate to, the number of investigations terminated and the reasons for the termination, and the number of cases pending; (3) types of predicate offenses involved in ML prosecutions and convictions; (4) the number of ML and TF investigations in which assets were seized and the amounts seized in each case; (5) the total amounts requested to be seized and eventually realized in each case should be maintained; (6) the number of MLA requests received and granted in ML and TF cases in relation to the seizing and confiscation of assets and the total number of assets seized and confiscated based on foreign request; (7) the number of extradition request received in ML and TF cases and the numbers of cases rejected and granted as well as the time required to complete extradition.

7.2 Other relevant AML/CFT Measures or Issues

7.3 General Framework for AML/CFT System (see also section 1.1)

Table 1. Ratings of Compliance with FATF Recommendations		
Forty Recommendations	**Rating**	**Summary of factors underlying rating**
Legal systems		
1. ML offense	**LC**	• Although it is clear that a significant number of investigations, prosecutions, and convictions have been obtained, incomplete statistics in some important areas and the lack of information on the types of predicate offenses to which the ML provisions are being applied make it impossible to determine that the ML provisions are applied in a fully effective manner.
2. ML offense—mental element and corporate liability	**LC**	• Due to the assessors' lack of access to statistics on the exact amount of fines and the duration of prison sentences imposed in ML cases, it is not possible to establish that the sanctions regime is fully effective. • Although it is clear that a significant number of investigations, prosecutions, and convictions have been obtained, incomplete statistics in some important areas and the lack of information on the types of predicate offenses to which the ML provisions are being applied make it impossible to determine that the ML provisions are applied in a fully effective manner.
3. Confiscation and provisional measures	**LC**	• The scope of legal privilege hinders appropriate access to information and documents held by lawyers and other legal professionals. • While the application of the confiscation framework seems to yield some results, in the absence of more comprehensive statistics the assessors are not in a position to conclude that the provisions are applied in a fully effective manner.
Preventive measures		
4. Secrecy laws consistent with the Recommendations	**C**	• This recommendation is fully observed.
5. Customer due diligence	**PC**	• There is no direct obligation in the WWFT or related legislation requiring financial institutions to determine whether the customer is acting on behalf of another person. • For foreign legal persons "not based in the Netherlands," there is no indication that documents used to verify the identity of a legal entity should be from an "independent" source. • The WWFT does not obligate financial institutions to verify that a person purporting to act on behalf of the legal entity is so authorized. • There is no requirement to obtain a "foreign legal person's" address and legal form or to obtain the name of trustees or directors or to obtain provisions regulating the power to bind the legal person or arrangements. • The definition of the beneficial owner falls short of the FATF standard as it only refers to legal persons and trusts, and not, more broadly, to the natural person(s) who ultimately owns or controls "a

Table 1. Ratings of Compliance with FATF Recommendations		
		customer." The definition does not refer to the person that can exercise ultimate effective control over a legal arrangement. • The requirement to verify the identity of the beneficial owner and to understand the ownership and control structure of the customer are subject to a risk-based approach and are only applicable in high-risk scenarios. • Rather than identifying circumstances in which simplified CDD can be conducted, Article 6 WWFT provides a list of customers/scenarios exempt from the CDD requirements stipulated by Article 3(1) (the obligation to undertake customer due diligence, which, as the authorities confirmed, includes the measures detailed in paragraph 2), Article 3 (3) (a)(b)(d) and (4) and Article 4 (1). • There are no obligations for financial institutions to ensure that data and information obtained under the CDD process, such as the client risk profile and contact information, are kept up-to-date. • No enforceable obligation to consider filing a suspicious transaction report in the case of failure to satisfactorily complete CDD/terminate business relationship. • There are no provisions in the WWFT obligating financial institutions to apply CDD to existing customers. Transitional provision exists that consider by default the customers identified under the previous AML/CFT regime as identified under the WWFT. • Effectiveness issues in the implementation of preventive measures, regarding: the identification and verification of the beneficial owner.
6. Politically exposed persons	**PC**	• There is no requirement for institutions to ascertain source of wealth and to identify the beneficial owner when the source of wealth is a PEP. • The PEP-related requirements do not apply to non-Dutch PEPs resident in the Netherlands. • The obligation for financial institutions to have risk based procedure to determine whether a customer is a PEP, does not extend to the case of the beneficial owner. • There is no requirement to obtain senior management approval to continue business relationship when a customer/beneficial owner becomes a PEP or is found to be a PEP during the course of an already established business relationship. • The notion of close associate in the Explanatory Memorandum is limited to those who are "publicly known".

Table 1. Ratings of Compliance with FATF Recommendations		
7. Correspondent banking	**LC**	• Enhanced due diligence does not apply to correspondent relationships involving financial institutions headquartered in an EU Member State. • No enforceable requirements in the case of "payable-through accounts."
8. New technologies & non face-to-face business	**LC**	• The option envisaged by Article 8, para 2 c) of the WWFT may not ensure effective CDD procedures in the case of non face-to-face transactions. • No specific obligation to prevent the misuse of new technology.
9. Third parties and introducers	**NC**	• No direct obligation for financial institutions to: o immediately receive necessary customer information and; o satisfy themselves that copies of CDD documents and data will be available without delay. • No obligation for financial institutions to satisfy themselves that the third party is regulated or supervised. Presumption that all EU and EEA countries adequately apply the FATF recommendations. • No enforceable requirement that ultimate responsibility for CDD should remain within the FI relying on the third party.
10. Record-keeping	**LC**	• The ambiguity caused by the contradiction between general record-retention requirements of seven years and specific requirements relating to financial entities that are of five years of less. • The record-keeping provisions do not explicitly require that records of transactions should be sufficient to permit reconstruction of transactions sufficient for a prosecution; • The authorities have no power to extend the retention period if necessary in particular cases.
11. Unusual transactions	**LC**	• Some elements of the obligation are implicit and do not apply to all financial institutions. • No enforceable requirement for financial institutions to examine as far as possible the background and purpose of unusual transactions and to keep the findings in writing.
12. DNFBP–R.5, 6, 8–11	**PC**	**All DNFBPs (except TCSPs)** • The shortcomings identified under Recommendation 5 and 10 in section 3 also apply **All DNFBPs** • The shortcomings identified under Recommendation 6, 8, 9 and 11 in section 3 also apply. Effectiveness issues. **Real estate agents** • CDD required only on one party to the transaction is covered, not both the buyer and the seller. **Lawyers and Notaries** • Exemption of CDD requirements in relation

Table 1. Ratings of Compliance with FATF Recommendations		
		to the first meeting with the client. **TCSPs** ● No requirements for providing a registered office; business address for a company, a partnership or any other legal person or arrangements, when this service is provided on a standalone basis. ● No requirements in relation to the identification of the customer other than the beneficial owner, and enhanced due diligence. ● No indication to when the retention period should start for records of customer information (if different from the beneficial owner) and business correspondence.
13. Suspicious transaction reporting	**LC**	● The 14-day period to report after a transaction has been established suspicious does not comply with the requirement of prompt reporting and raises an effectiveness issue in relation to the recovery of criminal assets. ● Reporting by insurance agents, life insurance companies and bureaux de change is particularly low, which raises concerns regarding the effectiveness of the reporting regime.
14. Protection & no tipping-off	**PC**	● Protection from criminal liability for STR reporting applies in the absence of good faith. ● Protection from civil liability for STR reporting is subject to inappropriate conditions. ● Tipping-off prohibition does not apply to directors, officers, and employees. ● Tipping-off prohibition does not apply to information in the process of being reported.
15. Internal controls, compliance & audit	**PC**	● The internal control requirements are mostly to be found in the Wft rather than the WWFT. The coverage of the Wft is not the same as that of the WWFT and some of the requirements in the Wft (including the requirements for internal controls, internal audit and compliance functions) do not apply to certain categories of regulated financial entity as described above. ● There is no requirement relating to the seniority or access to managers of the head of the compliance function. ● The detailed requirements in the Wft for compliance functions, relating to their access to resources and documents, their reporting requirements and other matters do not apply to banks with no investment functions and there are no comparable requirements in the Wgt. ● The requirements for employee training on AML/CFT in the WWFT are limited to the obligation that employees be instructed in the provisions of the WWFT and trained to recognize unusual transactions. The broad and general provisions in the Wft regarding the provision of information to employees and to business units are not accompanied by any guidance that makes it clear

Table 1. Ratings of Compliance with FATF Recommendations		
		that training should cover internal policies, procedures and controls, new developments and current ML and TF techniques, methods and trends, as well as all aspects of AML/CFT laws and obligations, including, in particular requirements on CDD and reporting.
16. DNFBP–R.13–15 & 21	**PC**	**All DNFBPs** The shortcomings identified under Recommendation 13, 14, and 21 in section 3 also apply to DNFBPs. **All DNFBPs (except TCSPs):** ● No requirement of internal policies, procedures and controls (except lawyers). ● No requirement to establish an appropriate ongoing employee training. ● No obligation of an independent audit function to test compliance with the procedures, policies, and controls. **Real estate agents** ● Reporting requirement only in relation to one party to the transaction, not both the buyer and the seller. **Lawyers** ● Inadequate awareness of potential ML vulnerabilities contributing to underreporting. **TCSPs** ● No reporting requirements for providing a registered office; business address for a company, a partnership or any other legal person or arrangements, when this service is provided on a standalone basis. ● Inadequate awareness of potential ML vulnerabilities contributing to underreporting.
17. Sanctions	**LC**	● Punitive sanctions are available which, for the most part are capable of being used in an effective, proportionate and dissuasive manner but there is limited use of such sanctions in practice. ● In respect of their impact on the largest institutions, administrative fines remain modest and may, in some instance, be insufficiently effective or dissuasive.
18. Shell banks	**C**	● This recommendation is fully observed.
19. Other forms of reporting	**C**	● This recommendation is fully observed.
20. Other NFBP & secure transaction techniques	**C**	● This recommendation is fully observed.
21. Special attention for higher risk countries	**PC**	● No specific enforceable obligation for financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. ● No requirement for financial institutions to examine as far as possible the background and purpose of unusual transactions. ● The existing countermeasures are limited in scope.

Table 1. Ratings of Compliance with FATF Recommendations		
22. Foreign branches & subsidiaries	**PC**	• There are no provisions requiring the institutions subject to the WWFT to apply Dutch standards to branches and subsidiaries in member states of the EU (or EEA). • The requirement to apply Dutch standards applies only to CDD and not to all appropriate AML/CFT measures. • There is no requirement that institutions subject to the Act should pay particular attention to the principle that foreign branches and subsidiaries apply Dutch standards in countries which do not or which insufficiently apply FATF Recommendations. • The WWFT does not require an institution subject to the Act to apply higher host country standards if they exist.
23. Regulation, supervision and monitoring	**LC**	• There are doubts about the effectiveness of supervision for independent insurance businesses (although the DNB has been addressing this since 2008); and • The approach of the AFM gave particular concern that they were not ensuring that institutions in the relatively minor part of the financial services business within their jurisdiction were effectively implementing their AML/CFT obligations.
24. DNFBP—regulation, supervision and monitoring	**PC**	• Secrecy issues prevent the exercise of supervision of lawyers by the designated supervisor. • Effectiveness of the measures in place regarding internet casinos illegally operating from the Netherlands could not be fully established • Effectiveness issues in relation to the monitoring of precious metals dealers, lawyers and accountants.
25. Guidelines & Feedback	**PC**[1]	• Guidance issued to financial institutions is at too high a level of generality to ensure that implementation of AML/CFT defenses is adequate and there is a need for more detailed guidance on the nature of AML/CFT risks in the Netherlands, the importance of establishing a profile and monitoring, and the training and screening of staff. • Guidance is, in some respects, out of date, incomplete, and inaccurate. • Feedback to reporting institutions from the FIU is not regarded as sufficient by those institutions. • Specific feedback is not regarded as sufficient by reporting institutions.
Institutional and other measures		
26. The FIU	**PC**	• The FIU-NL has been a project organization for almost five years, and the Netherlands have undertaken steps towards the final merger between MOT and BLOM only after the onsite visit. The legal framework for the FIU-NL is not yet fully complete. • Instances in which access to data does not allow the FIU to properly undertake its functions.

Table 1. Ratings of Compliance with FATF Recommendations		
		• Shortcomings in the secure protection of data. • Governance issues affecting the operational independence of the FIU. • Effectiveness issues concerning: o operational analysis (lack of prioritarization techniques in a context characterized by large amounts of reports); o dissemination of financial information to law enforcement (the role of the "STRs' in triggering ML investigations and prosecutions, as well as in ongoing cases, is very minimal; authorities cannot establish how many of the STRs contribute to the opening of ML/FT criminal investigations; access to STR-information is available to law enforcement for investigation of any type of crime, not just ML/FT).
27. Law enforcement authorities	**C**	• This recommendation is fully observed.
28. Powers of competent authorities	**LC**	• Scope of legal privilege hinders the ability for law enforcement authorities to locate and trace assets and property**.** • Absence of statistics on investigations does not enable to fully assess effectiveness.
29. Supervisors	**LC**	• The observations on the administrative sanctions noted in the rating for R.17 are equally relevant here.
30. Resources, integrity, and training	**LC**	• Staff training is not required on an annual basis and there are insufficient data on the nature of training received by supervisory staff. • Level of training of some police officers and ability to deal with complex cases critically assessed by members of the judiciary.
31. National co-operation	**LC**	• Coordination mechanisms not all used effectively.
32. Statistics	**LC**	• l Statistics on inspections and enforcement not comprehensive **(From section 7.1.)** Accurate and complete statistics are not maintained on: (1) the number and types of predicate offenses committed in the Netherlands; (2) the number of investigations conducted for ML and FT, including information on how these cases where initiated and the types of crime these cases relate to, the number of investigations terminated and the reasons for the termination, and the number of cases pending; (3) types of predicate offenses involved in ML prosecutions and convictions; (4) the number of ML and TF investigations in which assets were seized and the amounts seized in each case; (5) the total amounts requested to be seized and eventually realized in each case should be maintained; (6) the number of MLA requests received and granted

Table 1. Ratings of Compliance with FATF Recommendations		
		in ML and TF cases in relation to the seizing and confiscation of assets and the total number of assets seized and confiscated based on foreign request; (7) the number of extradition request received in ML and TF cases and the numbers of cases rejected and granted as well as the time required to complete extradition proceedings.
33. Legal persons–beneficial owners	**PC**	• Information on the ultimate beneficial owners of Dutch legal persons is not accessible and/or up-to-date in all cases. • The measures that have been put in place to ensure that bearer shares issued by Dutch NVs are not abused for ML or FT purposes are not yet fully effective.
34. Legal arrangements – beneficial owners	**PC**	• For trusts administered by licensed Dutch FIs or DNFBPs, the definition of the "beneficial owners" as contained in the WWFT does not extend to "the natural person(s) who ultimately owns or controls a legal arrangement. • Scope of legal privilege hinders the possibility for law enforcement authorities to access beneficial ownership information regarding trusts held by lawyers, accountants and notaries. • For trusts not administered by Dutch FIs or DNFBPs, the annual updating requirement for beneficial ownership information as required under the Law on Income Tax is not sufficient to ensure that timely, accurate and complete beneficial ownership information is available in all cases.
International Cooperation		
35. Conventions	**PC**	• The Netherlands have not ratified and implemented some provisions of the Palermo and Vienna Conventions. • The Netherlands have ratified but have not fully implemented the CFT Convention as outlined in the various sections of the report.
36. Mutual legal assistance (MLA)	**PC**	• In relation to a large number of countries, the Dutch authorities may provide assistance in searching and seizing of evidence only in ML cases involving transnational organized crime or corruption but not any other types of predicate offenses. • Although the statistics do not imply that there are significant difficulties in practice, the shortcomings identified under Special Recommendation II may limit the Netherlands ability to provide MLA. • Scope of legal privilege hinders the possibility for law enforcement authorities to access information and documents held by notaries, lawyers and accountants.
37. Dual criminality	**LC**	• For non-Council of Europe members and countries with which the Netherlands has not signed a multilateral or bilateral extradition treaty with the dual criminality as applied by Article 552o (3) of the CPC is not fully in line with the

Table 1. Ratings of Compliance with FATF Recommendations		
		international standard in that it is not sufficient for conduct to be criminalized under both Dutch law and the law of the requesting country but with some exceptions also requires for conduct to qualify as an extraditable offense. ● In relation to non-Council of Europe members and countries with which the Netherlands have not signed a multilateral or bilateral extradition treaty, the dual criminality as applied in the Netherlands is not in line with the international standard in that it is not sufficient for conduct to be criminalized under both Dutch law and the law of the requesting country but also requires for conduct to fall under an offense listed in Article 51a of the Extradition Act **(From section 6.4.3).**
38. MLA on confiscation and freezing	**PC**	● Although the statistics do not imply that there are significant difficulties in practice, the shortcomings identified under Special Recommendation II may limit the Netherlands ability to provide MLA. ● Scope of legal privilege hinders the possibility for law enforcement authorities to access information and documents held by notaries, lawyers and accountants. ● It was not established that the Netherlands effectively seizes and confiscates funds based on foreign request.
39. Extradition	**PC**	● In relation to non- Council of Europe members and countries with which the Netherlands have not signed a multilateral or bilateral extradition treaty, ML offenses involving transnational organized crime or corruption are extraditable offenses under Dutch law. ● There is no obligation by Dutch authorities to prosecute a suspect domestically in cases where an extradition request is denied purely on the basis of nationality. ● Statistics were not sufficiently detailed to determine that the extradition proceedings in the Netherlands are dealt with efficiently and in a timely manner.
40. Other forms of co-operation	**LC**	● The broad scope of legal professional secrecy introduces an unduly restrictive condition to exchange of information. ● Lack of statistics to assess the effectiveness of international cooperation by law enforcement agencies.
Nine Special Recommendations		
SR.I Implement UN instruments	**PC**	● The Netherlands have ratified but not fully implemented the CFT Convention as outlined in the various sections of this report. ● Minor shortcomings remain in respect of the implementation of UNSCR 1267 and 1373.
SR.II Criminalize terrorist financing	**PC**	● The “collection” of funds to commit a terrorist act is only criminalized if the perpetrator has acquired or actually possessed the funds. ● Article 46 of the Penal Code does not

Table 1. Ratings of Compliance with FATF Recommendations			
			sufficiently criminalize the financing of conduct covered by the offenses set forth in the nine Conventions and Protocols listed in the Annex to the TF Convention. • The criminalization of financing of an individual terrorist is only limited to the case in which the financed person has been designated under the UN, EC, or Dutch Sanctions Regulations. • Attempt to finance a specific terrorist act is not criminalized. • The absence of an autonomous TF offense has a negative impact on the effective investigation and prosecution of terrorism financing activities.
SR.III	Freeze and confiscate terrorist assets	**LC**	• There is insufficient guidance for persons and entities other than FIs that may be holding targeted funds or assets regarding the freezing obligations stemming from the international standard, including the obligation to check client files and databases against those lists. • FIs other than banks are not always sufficiently supervised for compliance with the EC and Sanctions Regulations. • The freezing obligations under EC Regulation 881/2001 do not expressly extend to funds and assets that are owned or controlled "indirectly" by a designated individual, entity, or organization. • Concerns remain as to whether funds and assets are frozen without delay in all instances.
SR.IV	Suspicious transaction reporting	**LC**	• Technical deficiency in the WWFT definition of TF limits the reporting obligation. Reporting of funds related to those who finance terrorism is not required. • The 14-day period to report after a transaction has been established suspicious does not comply with the requirement of prompt reporting.
SR.V	International cooperation	**PC**	• Although the statistics do not imply that there are significant difficulties in practice, the shortcomings identified under Special Recommendation II may limit the Netherlands ability to seize and confiscate property upon foreign request. • Statistics were not sufficiently detailed to determine that the extradition proceedings in the Netherlands are dealt with efficiently and in a timely manner. • In TF cases, the shortcomings identified under Special Recommendation II may limit the Netherlands ability to seize and confiscate property upon foreign request. • Scope of legal privilege hinders the possibility for law enforcement authorities to access information and documents held by notaries, lawyers and accountants. • Shortcomings identified under Special Recommendation II have a limiting effect on the

Table 1. Ratings of Compliance with FATF Recommendations			
			Netherlands ability to provide information in TF investigations **(From section 6.5.2.)**
SR.VI	AML/CFT requirements for money/value transfer services	**LC**	● The application of the FATF Recommendations to money transfer offices and bureau de change suffers from the same deficiencies as identified in relation to the rest of the financial sector (see sections 3.1 to 3.10 of this report).
SR.VII	Wire transfer rules	**C**	● This recommendation is fully observed.
SR.VIII	Nonprofit organizations	**LC**	● For NPOs outside the CBF seal mechanism no outreach initiatives to enhance NPO's awareness about the risks of terrorist abuse and the mechanism available to mitigate such risks have been conducted. ● No coordination and information exchange mechanisms involving the CBF are in place.
SR.IX	Cross-Border Declaration & Disclosure	**LC**	● No requirements in the case of shipment of currency through containerized cargo or in the case of mailing of currency or bearer negotiable instruments by a natural or legal person. ● Quality of the data made accessible to the FIU affects the effective use of such information by the FIU. ● Sanctions are not always effective.

[1] This is a composite rating, taking account of other comments relating to Recommendation 25, *e.g.*, in Section 3.10.3.

Table 2. Recommended Action Plan to Improve the AML/CFT System	
FATF 40+9 Recommendations	**Recommended Action (in order of priority within each section)**
1. General	
2. Legal System and Related Institutional Measures	
2.1 Criminalization of Money Laundering (R.1 & 2)	• The authorities should review all information available with respect to the fines and prison sentence imposed in ML cases to determine whether the sanctions regime is applied effectively, including in relation to legal persons. • To determine whether the ML provisions are applied effectively in the Netherlands, accurate and complete statistics should be maintained on (1) the number and types of predicate offenses committed in the Netherlands (2) the number of investigations conducted for ML, including information on how these cases where initiated and the types of crime these cases relate to, the number of investigations terminated and the reasons for the termination, and the number of cases pending and (3) the types of predicate offenses involved in ML prosecutions and convictions.
2.2 Criminalization of Terrorist Financing (SR.II)	• Criminalize terrorism financing fully in line with the FATF standard as per Ministerial Commitment. • Amend the law to expressly criminalize in all circumstances the "collection" of funds to commit a terrorist act, including in cases where the financer is neither in possession of nor has acquired the collected funds. • Amend the Penal Code to ensure that the financing of all "terrorist acts" as defined under the FATF standard is criminalized. • Criminalize the financing of individual terrorist including in cases where funds are provided for purposes other than to support the commission of a specific terrorist act or where the financing relates to terrorists other than those designated through the UN, EC and Ministerial Sanctions Regulations. • Criminalize the attempt to finance a specific terrorist act. • Put in place mechanisms to ensure that FT activities are investigated and prosecuted effectively in the Netherlands, for example by providing for TF as a separate criminal offense in line with the UN Convention for the Suppression of the Financing of Terrorism.
2.3 Confiscation, freezing, and seizing of proceeds of crime (R.3)	• Ensure that access to appropriate information and documents held by lawyers and other legal professionals is available in all cases. • To determine whether the confiscation framework is applied effectively better statistics on (1) the number of ML and TF investigations conducted in the Netherlands and the number of cases in which assets were seized and the amounts seized in each case; and the amounts requested to be seized and eventually realized in each case should be maintained.

Table 2. Recommended Action Plan to Improve the AML/CFT System	
2.4 Freezing of funds used for terrorist financing (SR.III)	• Provide more guidance to the private sector, especially the non banking financial industry and DNFBPs, on the freezing obligations stemming from the international standard, including the obligation to check client files and databases against those lists. • Ensure that all FIs, not only banks, are effectively monitored for compliance with the EC and Sanctions Regulations. • Extend the freezing obligations under UNSCR 1267 to funds and other assets owned or controlled "indirectly" by a designated individual, entity, or organization. • Ensure that funds and assets are frozen without delay in all cases.
2.5 The Financial Intelligence Unit and its functions (R.26)	• Complete the legal framework concerning the FIU-Netherlands; • Implement a simplified governance model so that issues that affect the operational independence of the FIU are fully addressed; • Streamline financial analysis, by developing automated-based systems for generating red flags and prioritizing the analysis of the data in a more structured way. • Reconsider the whole "dissemination" system, with a view to emphasize a more streamlined provision of information to law enforcement, on a case-by-case basis, given the minimal role played by the current system of dissemination of STRs in generating new criminal investigations/adding value to existing ones. • Enhance security of information held by the FIU (including the physical security of the information stored in hard copy); • Ensure that the FIU has timely and full access to all data it requires to properly undertake its functions. • Outreach to lawyers to clarify FIU's powers to request additional information. • Extend the legal retention period to match statute of limitation envisaged for ML/TF.
2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28)	• The authorities should review the scope of professional secrecy and privilege obligations, and consider amending the CPP to improve the authorities' ability to obtain documents and information, having regard to the possibilities enabled by the European treaties. • When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain from lawyers, notaries, and tax accountants, documents and information for use in those investigations, and in prosecutions and related actions. The assessment team considers that the current framework on legal privilege in the Netherlands limits the authorities' powers unreasonably The authorities should review the scope of professional secrecy and privilege obligations, and consider amending the CPP to improve the authorities' ability to obtain documents and information, having regard to the possibilities enabled by the European treaties. • Maintain statistics on the number of investigations and on the use of powers to conduct ML or TF investigations.

Table 2. Recommended Action Plan to Improve the AML/CFT System	
2.7 Cross-Border Declaration & Disclosure (SR IX)	• Extend the requirements envisaged in the Dutch system to the case of shipment of currency through containerized cargo or in the case of mailing of currency or bearer negotiable instruments by a natural or legal person; • Establish TF as an autonomous offence, and extend Customs' responsibilities also in this area; • Consider enhancing Customs authorities powers to stop or restraint the currency, when there is a suspicion of ML and when the person has fulfilled the declaration requirements; • Consider updating the international agreements with foreign Customs which entered into force prior to the EC 1889/2005 to specifically provide for the exchange of information also in the area of AML/CFT, if needed. • Improve the quality of the data shared with the FIU.
3. Preventive Measures–Financial Institutions	
3.1 Risk of money laundering or terrorist financing	
3.2 Customer due diligence, including enhanced or reduced measures (R.5–8)	**With respect to Recommendation 5:** • Clarify the issues related to the applicability of the CDD requirements envisaged by the WWFT (in particular those concerning beneficial ownership) to protected accounts opened prior to the entry into force of the updated Regulation on protected accounts; • Make it clear in the Regulation on protected accounts that the compliance officer must have access to the data in the central register of protected accounts. • Clarify that the notion of "customers" is intended to cover also trusts and other legal arrangements. • Consider providing a list of examples of the types of documents that can be used to identify and verify the customers and beneficial owners; • Clarify the obligation (documents should be from independent source) and provide guidance for the verification of the identity of non-Dutch based foreign legal entities (indicate examples of documents that can be used to verify identity); • Require financial institutions to obtain information regulating the power to bind the legal person or arrangement (including the name of trustees and directors); including, in the case of foreign legal persons, the legal form and address. • Bring the definition of beneficial owner in line with the FATF standard (by referring it to the customer and by providing a reference to "actual control' also in the case of trusts and other legal arrangements) • Clarify the obligations to identify and to take reasonable measures to verify the ultimate beneficial owner and to understand the ownership and control structure of the customer in all circumstances regardless of risk, and provide guidance as to how this can be conducted in particular for legal persons formed outside of the Netherlands; • Obligate financial institutions to determine whether the customer is acting on behalf of another person; • Obligate financial institutions to verify that a person purporting to act on behalf of the legal entity so authorized; • Provide further guidance on all CDD measures to financial institutions, including on additional circumstances which may be considered high risk as well as examples of the type of enhanced due

Table 2. Recommended Action Plan to Improve the AML/CFT System	
	diligence measures that could be implemented; • Address the exemptions for low-risk customers as adopted from the Third EC Money Laundering Directive to ensure that all transactions are based on a risk assessment regardless of the location, type of client or product and that regardless of the classification that all transactions are subject to monitoring and periodic review. • Oblige financial institutions to ensure that data and information obtained under the CDD process, such as the client risk profile and contact information, are kept up-to-date. • Introduce an express obligation to consider fling an STR in the case of failure to satisfactorily complete CDD/terminating business relation. • Repeal the transitional provision of the WWFT that deems the identification and record keeping requirements under the previous AML/CFT law as if it were duly fulfilled under the WWFT. **With respect to Recommendation 6:** • Require institutions to ascertain source of wealth and funds in all circumstances and not limited to business relations/transactions; • Review the PEP- related requirements to include non-Dutch PEPs resident in the Netherlands; • Introduce a requirement to obtain senior management approval to continue business relationship when a customer/beneficial owner becomes a PEP or is found to be a PEP during the course of an already established business relationship. • Extend the obligation for financial institutions to have risk based procedure to determine whether a customer is a PEP, also to the case of the beneficial owner. • Clarify that the notion of close associate is not limited to close associates who are publicly known. **With respect to Recommendation 7:** • Extend enhanced due diligence to all correspondent relationships regardless of the location of the respondent; • Introduce enforceable requirements in the case of payable-through accounts. **With respect to Recommendation 8:** • Extend enhanced due diligence required to all non face-to-face relationships; • Reconsider the option envisaged by Article 8, para 2 c) of the WWFT, as it may not ensure effective CDD procedures in the case of non face-to-face transactions. • Create specific obligation to prevent the misuse of new technologies.
3.3 Third parties and introduced business (R.9)	• Revise the obligation that is currently imposed on the third party to provide the information concerning the CDD process, so that this information is immediately obtained by the FI that is relying on the third party. This should be redrafted to impose the obligation on the financial institution • Introduce a requirement for financial institutions to satisfy themselves that a third party located within the EU and EEA is regulated and supervised (in accordance with Recommendation 23, 24 and 29), and has measures in place to comply with the CDD requirements set out in R.5 and 10. Alternatively, the authorities could

Table 2. Recommended Action Plan to Improve the AML/CFT System	
	consider conducting a thorough assessment of the supervisory framework and of the CDD measures in place in the concerned countries where the third parties are located and limit the location of third parties to those countries that have satisfactory supervisory framework and CDD measures. • Introduce enforceable requirements that place the ultimate responsibility for customer identification and verification with the financial institution relying on the third party.
3.4 Financial institution secrecy or confidentiality (R.4)	• Amend the WWFT (Article 22) to make explicit that supervisory authorities may share information collected for the purpose of Article 24 with other domestic authorities and foreign supervisors, where this is necessary for the administration and enforcement of obligations under the WWFT and to include appropriate provisions regarding the use and confidentiality of such information, as are currently provided for in the Wft; • Consider with the Bankers Association the extent to which other regulated financial entities could have access to the customer information shared between banks according to the Code of Conduct.
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	• Remove the ambiguity created by the different and conflicting record-retention provisions in the AW, BWR, WWFT, and Wft and make explicit that the record-retention requirements (including those in the BW and AWR) necessarily apply to all transactions and to business correspondence, account files, customer identification on all legal persons and arrangements and beneficial owners; • Ensure that records of transactions are maintained in a way that permits reconstruction of transactions for the purpose of prosecution; • Extend the record keeping requirement in the BPR Wft and BGFO Wft to the Wft category of financial institution, financial services providers, money transfer offices, investment companies, management companies and custodians; • Give the authorities the power to extend the retention period if necessary in particular cases.
3.6 Monitoring of transactions and relationships (R.11 & 21)	**With respect to Recommendation 11:** • Streamline the legislative and regulatory framework, eventually by introducing a separate obligation for all financial institutions to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions that have no apparent or visible economic or lawful purpose, autonomous from the obligation to report suspicious transactions. Introduce an explicit obligation for financial institutions to examine as far as possible the background and purpose of unusual transactions. **With respect to Recommendation 21:** • Consider re-introducing the practice of issuing detailed circulars to financial institutions after each FATF Plenary; • Introduce an enforceable obligation for financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. • Introduce more specific provisions to implement all aspects of R21.

Table 2. Recommended Action Plan to Improve the AML/CFT System	
3.7 Suspicious transaction reports and other reporting (R.13, 14, 19, 25, & SR.IV)	**With respect to Recommendation 13 and Special Recommendation IV:** ● Ensure that suspicious transactions are reported promptly to the FIU; ● Enhance the effectiveness of the reporting system, including by raising awareness of financial institutions on the detection of suspicious transactions. **With respect to Recommendation 14:** ● Ensure that protection from criminal liability only applies if suspicions are reported in good faith. ● Ensure that demonstrating good faith is sufficient to be protected from civil liability, without having to prove that disclosure has reasonably been made in view of all facts and circumstances. ● Extend the tipping-off prohibition to apply to directors, officers and employees. ● Extend the tipping-off prohibition to cover cases where transactions are being reviewed internally to determine whether an STR should be filed. **With respect to Recommendation 25:** ● The authorities are recommended to reconvene the Article 21 Committee or the Indicators Working Group to establish with the representatives of the reporting institutions how best to disseminate the analysis that is currently produced. They are further recommended to consider issuing alerts to institutions when new information is available on the FIU web site. Some off the difficulties in providing feedback relate directly to the decision to require institutions to make unusual rather than suspicious reports, the way in which those unusual reports are deemed suspicious and the method of dissemination of the reports to law enforcement. Such matters are discussed elsewhere in the context of the FIU.
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)	The authorities are **recommended** to make the following amendments to the WWFT, Wft, and Wgt with the overall objective of ensuring that all of the relevant obligations apply to all of the relevant institutions: ● amend the Wft to clarify that the policies, procedures and controls required by the Wft must apply to the implementation of the obligations in the WWFT; ● amend the WWFT to include a direct requirement to train staff , on a regular basis, on policies, procedures and controls and in particular on requirements on CDD and reporting of unusual transactions, and on new developments, including information on current ML and TF techniques, methods and trends; ● amend the final reference to the predecessor AML/CFT statutes in the Wgt Regulation, so that the requirement for internal controls applies to the WWTF; ● amend the Wft and Wgt to create a requirement for all regulated entities to have a compliance officer with adequate seniority, access to senior management, full access to documents, adequate resources and independence and with a requirement to make regular reports to management; ● amend the Wft or implementing regulations to require screening of all employees to ensure high standards; ● amend the Wft or implementing obligations to apply the ongoing obligations on internal controls, compliance units, internal audit, training, and employee screening to all regulated financial entities covered by the WWFT; ● consider the publication of guidance on what might be expected

Table 2. Recommended Action Plan to Improve the AML/CFT System	
	with regard to training, employee screening and other matters relating to compliance units and internal controls without diluting the primary responsibility of regulated financial entities to determine the precise level of training to be provided; • amend Article 2(1) of the WWFT (or provide in implementing regulations) to ensure that regulated entities with foreign branches and subsidiaries should apply all AML/CFT measures (not just CDD) that are equivalent to Dutch standards or applying local standards where these are higher; • amend Article 2 of the WWFT to apply its provisions to EU and EEA Member States; • amend the WWFT to create a requirement that regulated entities should pay particular attention to the principle that foreign branches and subsidiaries apply Dutch standards in countries which do not or which insufficiently apply FATF Recommendations.
3.9 Shell banks (R.18)	• The absence of any requirement to determine whether EU correspondent banks may have accounts with shell banks leaves a potential gap in the framework, although, in practice, this is unlikely to create a major risk. Nevertheless, the authorities are recommended to amend Article 8(3) of the WWFT so that it applies to all correspondent banks.
3.10 The supervisory and oversight system–competent authorities and SROs Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)	While the supervision process is mature and appropriately integrated in the general supervision of all financial institutions, the mission would make the following recommendations: • the authorities should collect more comprehensive and detailed data by sector and by year, on the use of their inspection and enforcement powers with respect to AML/CFT matters and on the nature of the weaknesses being identified, so as update their understanding of ML and TF risks and to satisfy themselves that appropriate and effective action is taken in this area; • the AFM should review their approach to AML/CFT and increase their focus on monitoring the procedures put in place by regulated entities to detect and deter money laundering and terrorist financing and should implement increased monitoring of CDD practices by the large number of smaller businesses that are brokers; • the DNB should formally withdraw the guidance issued with the Bankers Association in 2006 and issue revised guidance based on; • the useful material currently in the DNB staff manual and underlining the importance of ongoing customer monitoring as well as the formal identification and verification obligations together with advice on staff vetting and training (the authorities have indicated an intention to complete both tasks by February 2011; • the staff training program should be reviewed to ensure that each member of staff receives adequate training on AML/CFT (preferably on an annual basis) and comprehensive data should be maintained on this; • the authorities should use the powers they state are available to ascertain the source of funds and wealth as one of their measures to make sure that financial institutions are not controlled or owned by criminals or their associates and the implementing decree for the relevant provisions in the Wft should be amended to make explicit that this information should be supplied.

Table 2. Recommended Action Plan to Improve the AML/CFT System	
3.11 Money value transfer services (SR.VI)	• The FIU data shows that reports from money transfer offices form the large majority of all reports submitted to the FIU and the offices' own records show that few of these reports have been deemed suspicious in recent years. Although the data provided by the FIU suggested a higher proportion were deemed suspicious, the fact remains that none of those interviewed by the assessors considered that the money transfer offices represented the main ML or TF risk faced by the Netherlands. The level of reporting, therefore, appears to be out of proportion to the likely ML/TF activity. The DNB is recommended to review its advice to the money transfer offices on reporting on the basis of the subjective indicator, in consultation with the FIU, so as to maximize the value of the reporting system and seek a level of reporting that accurately reflects the presumption of money laundering. As noted above, the authorities are also recommended to apply the provisions of Article 3:99 to payment services providers, so that the owners may be subject to fit and properness tests.
4. Preventive Measures–Nonfinancial Businesses and Professions	
4.1 Customer due diligence and record-keeping (R.12)	Extend the scope of the CDD requirements to: • both the buyer and the seller of a transaction performed by a real estate agent; • the services designated by the WWFT for lawyers and notaries, when related to the first meeting with the client. This requirement should be set out in primary or secondary legislation; • TCSPs when providing a registered office; business address for a company, a partnership or any other legal person or arrangements, when this service is provided on a standalone basis. **With respect to Recommendation 5** **All DNFBPs** • Provide further guidance on all CDD measures. **All DNFBPs (except TCSPs)** The recommendations made in section 3 for financial institutions also apply to DNFBPs (except TCSPs). **TCSPs** • Adopt measures consistent with the standards regarding the identification of the customer other than the beneficial owner and enhanced due diligence. **With respect to Recommendation 6, 8, 9 and 11** • The recommendations made in section 3 for financial institutions also apply to DNFBPs. **With respect to Recommendation 10** **All DNFBPs (except TCSPs)** • Remove the ambiguity created by the different and conflicting record-retention provisions in the AW, BWR and the WWFT, and make explicit that the record-retention requirements necessarily apply to all transactions and to business correspondence, account files, customer identification on all legal persons and arrangements and beneficial owners. • Ensure that records of transactions are maintained in a way that permits reconstruction of transactions for the purpose of prosecution.

Table 2. Recommended Action Plan to Improve the AML/CFT System	
	• Give the authorities the power to extend the retention period if necessary in particular cases. **TCSPs** • Ensure that record keeping requirements on information on the customer (if different from the beneficial owner) and business correspondence, are kept for five years from the date the relationship with the customer ceases.
4.2 Suspicious transaction reporting (R.16)	**With respect to Recommendation 13:** • Extend the scope of the reporting requirement to : o both the buyer and the seller of a transaction performed by a real estate agent; o TCSPs for providing a registered office; business address for a company, a partnership or any other legal person or arrangements, when this service is provided on a standalone basis. • Ensure that suspicious transactions are reported promptly to the FIU; • Enhance the effectiveness of the reporting system. • Keep statistics on suspicious transactions reports related to the financing of terrorism. **With respect to Recommendation 14:** • Ensure that protection from criminal liability only applies if suspicions are reported in good faith. • Ensure that demonstrating good faith is sufficient to be protected from civil liability, without having to prove that disclosure has reasonably been made in view of all facts and circumstances. • Extend the tipping-off provision to cover cases where transactions are being reviewed internally to determine whether an STR should be filed. **With respect to Recommendation 15:** **All DNFBPs (except TCSPs)** • Require DNFBPs to develop internal policies, procedures and controls (except lawyers); • Require DNFPBs to establish an appropriate ongoing employee training; • Introduce the requirement of an independent audit function to test compliance with the procedures, policies and controls. **TCSPs** Introduce the requirement of an independent audit function to test compliance with the procedures, policies and controls. **With respect to Recommendation 21:** **All DNFBPs** • Re-introduce practice of issuing detailed circulars to reporting entities after each FATF Plenary; • Introduce an enforceable obligation for DNFBPs to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF

Table 2. Recommended Action Plan to Improve the AML/CFT System	
	Recommendations. ● Introduce enforceable provisions for the application of countermeasures in the case in which a country continues not to apply or insufficiently applies the FATF Recommendations.
4.3 Regulation, supervision, monitoring, and sanctions (R.17, 24, & 25)	**With respect to Recommendation 24:** ● Ensure that lawyers are subject to an effective system for ensuring compliance with AML/CFT requirements; ● Increase the effectiveness of the measures in place concerning illegal internet casinos that have their mind and management in the Netherlands. ● Increase effectiveness in the monitoring of precious metals dealers, lawyers and accountants. **With respect to Recommendation 25:** ● The FIU should provide DNFBPs with a more specific feedback on reported transactions.
4.4 Other designated non-financial businesses and professions (R.20)	There are no recommendations with regard to this Recommendation.
5. Legal Persons and Arrangements & Nonprofit Organizations	
5.1 Legal Persons–Access to beneficial ownership and control information (R.33)	● Information on ultimate beneficial owners of Dutch legal persons should be accessible and up-to-date in all cases. ● The dematerialization process should be completed as soon as possible to ensure that bearer shares issued by Dutch NVs are not abused for ML or TF purposes.
5.2 Legal Arrangements–Access to beneficial ownership and control information (R.34)	● The definition of the "beneficial owners" as contained in the WWFT should extend to "the natural person(s) who ultimately owns or controls a legal arrangement." ● For trusts not administered by a Dutch FI or DNFBP, put in place additional measures to ensure that timely, accurate, and complete beneficial ownership information is available in all cases.
5.3 Nonprofit organizations (SR.VIII)	● For NPOs outside of the CBF's seal mechanism undertake outreach initiatives to enhance NPO's awareness about the risks of terrorist abuse and the mechanism available to mitigate such risks, and to promote transparency, accountability, integrity and public confidence in the NPO sector. ● For CBF approved NPOs, ensure that all information available is used by the Dutch authorities to review the activities, size, and other features of the NPO sector and to formulate appropriate preventive measures. ● Develop coordination and information exchange mechanisms that involve the CBF to facilitate the effectiveness of the supervisory framework and to warrant the application of preventive and investigative action in all cases where a particular NPO may be abused for ML or TF purposes.
6. National and International Cooperation	
6.1 National cooperation and coordination (R.31)	● Make greater use of existing coordination bodies and, if appropriate, combine some of the bodies so as to focus the resources of the participating parties; ● Encourage the supervisors and the FIU to make greater use of the information on reporting patterns and to consider benchmarking

Table 2. Recommended Action Plan to Improve the AML/CFT System	
	the Dutch experience against that of other countries so as to establish a risk-based awareness program to tackle those sectors where reporting is minimal; • Make greater use of the private sector's desire for greater feedback from the FIU so as to maximize the value of the reporting process.
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	• Implement fully the Vienna and Palermo Conventions. • Implement fully the CFT Convention, in particular by addressing the shortcomings identified in SR II. • Address the shortcomings identified in relation to the implementation of UNSCRs 1267 and 1373.
6.3 Mutual Legal Assistance (R.36, 37, 38 & SR.V)	• Amend the dual criminality as applied by Article 552o (3) of the CPC to ensure that the Netherlands can assist any foreign country in searching and seizing of evidence in relation to any ML case. • Address all shortcomings identified under Special Recommendation II to ensure that the dual criminality requirements as applied under the ECJTA and the CPC do not limit the Netherlands' ability to provide MLA. • Ensure that access to information held by notaries, lawyers and accountants can be granted in all cases, including in the context of MLA. • To establish the effective application of the existing framework, maintain statistics on (1) the timeframes within which MLA requests are implemented to establish that the Netherlands provide MLA in a timely, constructive, and efficient manner and (2) the number of requests received and granted in relation to the seizing and confiscation of assets and the total number of assets seized and confiscated based on foreign request. • Consider putting in place measures to ensure that all forms of assistance may also be granted in the absence of a treaty basis, for example based on reciprocity.
6.4 Extradition (R. 39, 37 & SR.V)	• In relation to non-Council of Europe members and countries with which the Netherlands have not signed a multilateral or bilateral extradition treaty, ML should be an extraditable offense in all cases, including drug related cases. • The shortcomings identified under Special Recommendation II should be remedied so as to allow for extradition in all cases relating to the TF, and the financing of individual terrorists become an extraditable offense. • Amend the law to set out a legal obligation by Dutch authorities to prosecute a suspect domestically in cases where an extradition request is denied purely on the basis of nationality. • Maintain more detailed statistics on the number of extradition request received in ML and TF cases and the numbers of cases rejected and granted as well as the time required to complete extradition proceedings to ensure that extradition proceedings in the Netherlands are dealt with efficiently and in a timely manner.
6.5 Other Forms of Cooperation (R. 40 & SR.V)	• The authorities should review the scope of professional secrecy obligations and consider amending the CPP to make sure that it does not subject exchange of information to unduly restrictive conditions. • The authorities should maintain statistics on international cooperation by law enforcement agencies.
7. Other Issues	
7.1 Resources and statistics (R. 30 & 32)	• Staff training should be required on an annual basis and sufficient data on the nature of training received by supervisory staff should be kept.

Table 2. Recommended Action Plan to Improve the AML/CFT System	
	• Attention should be paid to the level of training of some police officers and their ability to deal with complex cases. • Accurate and complete statistics should be maintained on: (1) the number and types of predicate offenses committed in the Netherlands; (2) the number of investigations conducted for ML and FT, including information on how these cases where initiated and the types of crime these cases relate to, the number of investigations terminated and the reasons for the termination, and the number of cases pending; (3) the types of predicate offenses involved in ML prosecutions and convictions; (4) the number of ML and TF investigations in which assets were seized and the amounts seized in each case; (5) the total amounts requested to be seized and eventually realized in each case should be maintained; (6) the number of MLA requests received and granted in ML and TF cases in relation to the seizing and confiscation of assets and the total number of assets seized and confiscated based on foreign request; (7) the number of extradition request received in ML and TF cases and the numbers of cases rejected and granted as well as the time required to complete extradition proceedings.
7.2 Other relevant AML/CFT measures or issues	
7.3 General framework – structural issues	