DIRECTORATE GENERAL
HUMAN RIGHTS AND RULE OF LAW

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Final

Assessment Report

ASSESSMENT OF THE CONCRETE IMPLEMENTATION AND EFFECTIVE APPLICATION OF THE 4TH ANTI-MONEY LAUNDERING DIRECTIVE IN THE NETHERLANDS

JUST/2018/MARK/PR/CRIM/0166

CONTENTS

GLOSSARY OF ACRONYMS

AFM	Authority for the Financial Markets
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
BFT	Financial Supervision Office
BO	Beneficial Owner
BTWwft	Tax and Customs Administration AML/CFT Supervision Office
CDD	Customer Due Diligence
CFT	Countering Financing of Terrorism
CI	Credit institution
COM	European Commission
CTR	Cash Transaction Reports
DNB	De Nederlandsche Bank
DNFBP	Designated non-financial businesses and professions
DTA	Legal Profession Supervision Unit within the Netherlands Bar
EDD	Enhanced Due Diligence
EMI	Electronic Money Institutions
EWRA	Enterprise-wide Risk Assessment
FATF	Financial Action Task Force
FDI	Foreign Direct Investment
FI	Financial institution
FIU	Financial Intelligence Unit
FTA	Legal Profession Financial Supervision Unit within the Netherlands Bar
FUR	Follow-up Report
iCOV	Information Exchange on Criminal and Unexplained Wealth
KNB	Royal Dutch Association of Civil-Law Notaries
KYC	Know your customer
LEAs	Law Enforcement Agencies
MER	Mutual Evaluation Report
MoU	Memorandum of Understanding
MSB	Money Services Business
MVTS	Money Value Transfer Services
NBA	Royal Netherlands Institute of Chartered Accountants
NOB	Dutch Association of Tax Advisers

NOvA	Netherlands Bar
NRA	National risk assessment
OEs	Obliged entities
PEP	Politically Exposed Person
PSP	Payment Service Providers
RB	Dutch Register of Tax Advisers
RBA	Risk-Based Approach
RCA	Relative or Close Associate
SAR	Suspicious Activity Report
SI	Significant Institutions (bank subject to direct ECB supervision)
SRB	Self-Regulating Body
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Providers
TFS	Targeted Financial Sanctions
UBO	Ultimate Beneficial Owner
UNODC	United Nations Office on Drugs and Crime
Wtt	Trust and Company Service Provider Supervision Act 2018
Wwft	The Money Laundering and Terrorist Financing [Prevention] Act

EXECUTIVE SUMMARY

This report provides a summary of the main findings and the main challenges of the practical operation of AML/CFT rules as transposed by the Netherlands.

Main Findings

1. There is uneven implementation of the requirement for carrying out comprehensive risk assessments and guidelines issued by the competent supervisory authorities for risk assessment (as well as for the use of new technologies for onboarding of customers) are not sufficiently detailed combined with limited feedback on unusual transaction reports (UTRs).
2. Privacy provisions hinder the sharing of information of critical data between firms belonging to a group (particularly when the parent or branches/subsidiaries are in third countries).
3. There is limited application by tax advisors, real estate agents, and some investment sector obliged entities (OEs) of the customer due diligence (CDD) requirements and concerns about the application by payment service providers of some requirements for conducting CDD, and about the application by the investment firms of enhanced CDD.
4. The identification of beneficial owners of complex structures as well as CDD for existing customers are negatively impacted by the lack of guidance and insufficient oversight in some cases.
5. The effectiveness of implementation of the requirements for identifying politically exposed persons (PEPs) is impacted by the lack of verification of the PEPs screening lists as well as the limited guidance and monitoring of implementation of the requirement to determine whether existing customers required re-classification as a PEP.
6. The reliability of the beneficial ownership register and availability of accurate beneficial ownership information for legal persons are affected by the ongoing process of implementation of the register, concerns about the accuracy and availability of the data held in the central register for legal persons, and the lack of requirements in place concerning the beneficial ownership registration for trusts.
7. OEs do not have full access for AML/CFT purposes to the information held in the beneficial ownership register.
8. The analysis of suspicious transaction reports performed by another authority, in addition to the FIU, (combined with the lack of proper feedback to the FIU by law enforcement) as well as the lack of powers of the FIU to request information, when it is not directly accessible, affect the effective implementation of the FIU's core functions.
9. It is not fully demonstrated that the unusual transaction reporting (UTR) system and the FIU analysis contribute systematically to the prevention and repression of ML and particularly of FT.
10. There are issues of effectiveness of the objective UTR reporting system, as well as issues of quality of reported UTRs combined with underreporting by certain types of non-financial professions.
11. The effectiveness of supervision is impacted by the absence of clear methodology of the assessment of risks related to channels of delivery and technology.
12. The application of uniform risk assessment methodology by the De Nederlandsche Bank across all OEs results in an incomplete understanding of the risks associated with particular OEs and the number and scope of onsite visits undertaken appears to be inadequate in view of the National Risk Assessment conclusions and findings from previous examinations.

13. Reliance on professional bodies by the Financial Supervision Office (BFT) for assessing the risks associated with the obliged entities within their remit result in ineffective risk rating considerations for those obliged entities, while on-site inspections of law firms are performed on a very limited time scale and therefore to a limited extent.
14. All supervisors lack methodology to assess the effectiveness of the approach taken in supervising OEs.
15. Deficiencies were observed with regard to the verification of the fit and proper information of tax advisors, administration offices, domicile providers, real estate offices and accountants.
16. De Nederlandsche Bank and Authority for the Financial Markets do not make use of the full range of sanctions at their disposal and concerns remain about the dissuasiveness and proportionality of the predominantly informal measures imposed. There are concerns about the effectiveness of sanctions imposed on administration offices and lawyers, and, more generally, about the lack of comprehensive assessment of the proportionality and dissuasiveness of sanctions.
17. Issues of data ownership, having affected the sharing of information (for the purpose of the NRA, FIU access to information), have repercussions on the understanding of risks and developing of a response to ML/FT risks at policy level.
18. The effectiveness of the FIU international cooperation is limited by the modalities of access to certain sources of information and the mechanisms applied to postpone operations.
19. The international cooperation between supervisors is impacted by some specific data sharing arrangements and cooperation with regard to sanctions in cross-border cases was not demonstrated except by De Nederlandsche Bank.

Overall Level of Practical Application of the Requirements of the 4th AML Directive

Risk assessment, internal control and group policies (Articles 8, 45, 46)

Supervisory authorities have issued sectoral guidelines concerning the implementation of the AML/CFT law, including for the requirement to carry out and document an enterprise-wide risk assessment (EWRA). Although these sectoral guidelines require risk assessment for customers, product, service transactions, channels of deliveries and geographic risk, they are, with very few exceptions, quite high-level and do not provide sufficient operational details for the OEs. Among the shortcomings of the guidelines, the most significant is the one concerning the near absence of risk scenarios for FT, given the FT risk posed by the Netherlands. OEs that fall under the purview of the DNB are required to undertake a "systemic integrity risk analysis" (SIRA), which is an analysis of "integrity risk", rather than specifically of the ML/FT risk, which is included in the assessment as one of the risk components (together with corruption, fraud, circumvention of sanctions, etc).

Supervisors check systematically, to varying degrees, that OEs undertake risk assessments which consider customers, countries/geographic areas, products, services and transactions, which may include a review of the quality of the EWRA performed by the OEs under their purview. As regards OEs that fall under the purview of the DNB, it was observed that the quality of the SIRA has overall improved, although there remain gaps in conducting SIRAs and challenges for banks to identify and address emerging risks (such as VASPs). FIs exhibited a better understanding of their ML and FT risks, compared to some DNFBP types that were interviewed. There was however insufficient identification of FT risk particularly by FIs.

Oversight on the operation of group policy varies significantly. Foreign banks that have a subsidiary or branch office in the Netherlands often rely heavily on the policies and procedures of their parent. Where this concerns a parent from outside the EU, investigations by the supervisor often show that they are not sufficiently adapted to the AML/CFT law. Examples of relevant remedial action taken by DNB was demonstrated. Privacy provisions hinder the sharing of information of critical data between firms belonging to a group (particularly when the parent or branches/subsidiaries are in third countries).

In the period under review Dutch authorities, including through public-private partnerships, have made significant efforts to provide guidance and training on ML/FT typologies and red flags to improve the quality of the UTRs, including by engaging the most material types of OEs on a regular basis by the FIU to discuss the quality of the UTRs. Nevertheless, some concerns about the lack of feedback on UTRs in some cases and the timeliness of feedback remain.

Customer Due Diligence (Articles 13.1, 14, 18 (1-3), 20, 21, 22, 23, 25, 26, 27, 28, 29)

Obliged entities interviewed by the assessment team demonstrated good knowledge and understanding of the requirements and application of Article 3 of the AML/CFT Law (Wwft). Following frequent interventions by the DNB, several of the Netherlands' major banks have rolled out large-scale and long-term CDD remediation and improvement programmes in recent years. Some OEs continue to find establishment of complex ownership structures challenging, while the investment, real estate and tax advisor sectors, evidence continued challenges in meeting the requirements of Article 3 of the Wwft, along with some domiciles providers and vehicle dealers. Supervisors have taken a variety of measures to address violations and improve compliance levels.

The use of automated onboarding technology supported by use of non-face-to-face identification verification technology and/or supplemented by artificial intelligence to undertake CDD is used or is being assessed for use by some OEs. Current supervisory tools used to collect information about these do not allow the collection of sufficient information so as to assess whether those systems are operated in compliance with CDD provisions. Currently, there is no published guidance from supervisors about the use of such systems in fulfilment of the Wwft obligations.

Some OEs continue to have difficulties in implementing existing CDD reviews, either by establishing time periods for reviews which are not sustainable relative to resource and capacity or longer review periods which have prevented the timely detection of changes to a customer's existing CDD information or risk profile. No guidance is provided to clarify how obliged entities should approach the review of existing CDD information beyond the requirements outlined in the Wwft. The large-scale AML cases in the Netherlands banking sector, such as ABN AMRO, have highlighted how the effectiveness of existing customer CDD reviews can be compromised.

Most obliged entities interviewed demonstrate an adequate understanding of the instances wherein enhanced CDD measures should be applied to customers with elevated risk characteristics. OEs report having both domestic foreign PEP customers, the extent to which was determined based on the scope of the entity's product offering. Guidance across the different supervisors was not always seen by OEs as helpful in clarifying how these requirements should be fulfilled. Some OEs noted continuing challenges with aligning transaction monitoring alerts and PEPs within their customer base. Where OEs rely upon PEP lists, their verification as to its accuracy was not always subject to regular monitoring and testing. No specific supervisory guidance or industry-wide feedback has been provided on the selection and oversight over the use of PEP lists.

There is limited guidance for OEs which clarifies what circumstances may give rise to extending a PEP customer or owner's risk classification beyond the 12-month period after they have ceased to

hold the relevant position. Less focus appears to be placed by supervisors on understanding how OEs link transactional behaviour with PEP customers or owners and how these results inform the reclassification of low risk rated customers. The challenges identified by some DNFBPs in determining the ownership for complex structures also affect their ability to accurately identify and classify PEP family members and close associates.

Transparency of beneficial ownership information and beneficial ownership registration (Articles 30-31)

Data provided by LEAs show that in the majority of cases entities misused for ML/FT purposes have legal personality, although the data does not show a (relative) prevalence of certain legal persons when it comes to ML/FT, the foundation being the exception. The NRA includes an analysis of the ML risk posed by legal persons incorporated in the Netherlands, focusing also on legal entities that act as directors in companies.

As the deadlines provided for by the law for submitting information on the BO to the register had not yet elapsed at the time of the evaluation, it is not possible to provide firm conclusions on its effective implementation, as it is not clear what was the share of the legal entities (incorporated prior to the entry into force of the requirement) that, at the time of the evaluation, had complied with the requirement

It is unclear whether there have been instances in which ascertained violations of the requirements to provide information to the Register have resulted in criminal investigations, even though there have been several cases that have led to the identification (including through reports of OEs) of incorrect data entered in the BO register.

The BO data is accessible publicly for a very small fee. but accessible data for OEs is only limited to the name, month and year of birth, state of residence and nationality, as well as the nature of the economic interest held by the ultimate beneficial owner and the extent of that interest, albeit only indicated in "bandwidths". OEs do not have access to identifiers such as the date of birth, the place of birth, the country of birth and the address of residence, which are accessible, in a timely manner, to the FIU and other competent authorities, without having to alert the persons concerned.

As regards transparency of legal arrangements, Article 31 has not been transposed yet. A legislative proposal that envisages the creation of a register for BO information related to trusts is currently before Parliament. Dutch law does not provide for the establishment of legal arrangements such as express trusts or Treuhand. However, certain express trusts established under the laws of another country are recognised as the Netherlands has signed and ratified the Hague Convention on the Law Applicable to Trusts and on their Recognition of 28 September 1995.

Functioning of FIU (Article 32)

The institutional arrangement concerning the FIU-NL presents a certain decree of convolution and has a number of issues that could potentially affect the operational independence of the FIU-NL. The independence of the FIU is not enshrined in a law, but only in a decree, and referred to the head of the FIU and not the institution. There are no rules establishing under what circumstances the head of the FIU can be removed. Third, the operational independence of the FIU is actually implemented only indirectly through a sub-mandate, which can be revoked at any time.

The FIU's responsibility of receiving, analysing, and disseminating financial intelligence to combat ML and FT activities are overall in accordance with the 4th AMLD. However, the additional reporting requirement (to the Police) affects the receipts and, possibly, the analysis functions of the FIU.

Moreover, it should be noted that, in addition to the FIU's analysis of UTRs, the Anti-Money Laundering Centre (AMLC), established within the FIOD, also performs analyses of STRs, which it receives from the FIU with a weekly and a quarterly export with GoAML (the system used by the FIU to receive and store UTRs), as well as strategic analysis for the identification of ML trends and typologies. Thus, there appear to be two institutions in charge of performing analysis of ML-related information.

The FIU has direct access to a number of other authorities' databases and there are additional arrangements for accessing relevant information by other means(e.g., Police data or fiscal information within iCOV, where a specific covenant exist that allows the exchange of information among participating institutions), although some limitations to obtaining other types of information that it may need to properly undertake its functions remain.

The evaluation team is not in a position to firmly conclude to what extent the outputs of the operational analysis of the FIU-NL contributes to the repression of ML/FT activities. The FIU was not able to provide statistics to demonstrate what is the share of these STRs that actually have contributed either to the starting of a new or to supporting an existing criminal investigation of ML or other types of predicate offences, nor was it able to indicate data on seizure of assets by the prosecutor (the FIU has not the power to suspend the execution of transaction) resulting from a request of the FIU, or by disseminated UTRs. The FIU does not maintain statistics differentiating ML and FT UTR analysis. Some examples were provided that show that investigators use the financial intelligence provided by the FIU; however, the evaluation team has strong concerns about the lack of feedback (enshrined in the AML/CFT law) from law enforcement authorities and the public prosecution office on the follow-up of disseminated UTRs.

Suspicious transaction reporting (Articles 33, 34, 35, 36, 46.2)

The scope of the reporting requirement in the Netherlands refers to unusual (and not suspicious) transactions. OEs are required by the AML/CFT law to disclose to the FIU unusual transaction reports (UTRs) on the basis of objective indicator (i.e., a match with the indicator requires an automatic reporting of the transaction) as well as subjective, (i.e., the transaction is reported when the OE has reason to suspect that the transaction may be related to ML or FT).

In general, the assessment team has strong reservations about the UTR system and the automatic reporting of transactions based on objective indicators and without an actual assessment of the suspiciousness of the transaction, particularly given the poor results in terms of these transactions' generating actual STRs in the analysis of the FIU and, ultimately, triggering criminal investigations.

All supervisors check in their inspections that OEs comply with their requirement to identify and report UTRs. The DNB has observed that banks are generally aware of the obligation to report unusual transactions to the FIU-NL, although the quality of the reporting processes and procedures as well as the necessary knowledge varies from one institution to another, and that the scope of the reporting – unusual, rather than suspicious "leads to confusion, especially for foreign banks with an independent establishment or branch in the Netherlands, because they often rely on the policies and procedures of the (foreign) parent." Another observation made by DNB is that a number of banks are not always acutely aware that not only transactions should be reported, but also intended transactions.

In general, OEs interviewed by the assessment team had a good understanding of the STRs requirements and were aware of how to report to the FIU. The banks and large FIs that were interviewed appear to have good knowledge of the policies and procedures to prevent, detect and report suspicious transactions, including through risk assessment and customer acceptance policies,

complemented by transaction monitoring systems (with both rule-based and scenario based systems to identify suspicious transactions, and a combination of real time and post event monitoring), with procedures for internal escalation and analysis of suspicious transactions prior to their reporting. However, some banks reported that FT risks indicators and scenarios are not very specific and difficult to embed in their transaction monitoring systems.

In view of the legal privilege, lawyers interviewed by the assessment team exhibited a more mixed understanding of the requirement to provide additional information to the FIU-NL upon request.

The FIU-NL provides feedback to the OE when a UTR is transformed into an STR. As noted by the DNB in their engagements with the banks, they indicate that only a fraction of the reports is deemed to be suspicious by the FIU, while no feedback at all is received concerning the reports not deemed to be suspicious. The interviews with OEs confirmed that feedback, when provided, concerns only the case of a UTR transformed into an STR. No further feedback is provided concerning the opening of criminal investigations (of which also the FIU is unaware).

Practical arrangements in terms of data protection and record-retention (Article 40 with AML relevance caveat)

Most OEs interviewed had not received guidance from their supervisors on how this obligation should be undertaken when conducting customer due diligence. Existing guidance was not found to be assistive in the practical implementation of these requirements, in fulfilling the Wwft's requirements. Some OEs, particularly those from the professional sectors, expressed difficulties in resolving the conflict that was apparent between minimum retention requirements under Article 33 of the Wwft, destruction requirements under Article 34a(3) of the Wwft and specific rules of their profession which required the retention of certain documents for a longer period.

Supervision of financial institutions and designated non-financial businesses and professions (Articles 47-48)

Supervisors demonstrate a strong knowledge of the risks identified in the NRA and, for most OEs, the risks specific to the sector in which they operate. A risk-based approach towards supervision is applied. All supervisory body have adopted their own methodology for assessment and scoring, except for the BFT and Local Bar Presidents, which do not risk assess the OEs they supervise. Some gaps were identified in relation to the risk factors assessed, in particular, on the use of technology and delivery channel risks. In some instances, it was unclear how data requested of OEs was incorporated into the risk assessment process, based on the models used. The methodology applied in the assessment of banks forms the basis of the assessment conducted by the DNB of the other entities it supervises.

There appears to be a misalignment between the risk rating of licensed payment service providers by the DNB the risk rating assigned in the NRA. It is unclear what data contributed to the downgrading of risk related to licensed payment service providers in the NRA, and equally the raising of the risk level associated with payment services providers not required to obtain licence (high). The DNB, however, has rated payment service providers low to medium risk. The assessment team was unable to clarify the reason for the inconsistency between approaches.

Resourcing is a significant factor that impacts upon the effectiveness of supervisory activities and the regulatory responses across all sectors. Resourcing is very different across the different supervisors and does not always reflect the nature, size and complexity of their OEs supervised or the risks related to them. Resourcing also requires scaling to incorporate the necessary technical knowledge to effectively test and assess technologies used or likely to be used by OEs to comply with Wwft

obligations. Reliance on professional bodies, as in the case of the BFT, has been necessary to fulfil its oversight function, in light of the number of OEs it supervises. Supervisors have adopted different approaches towards addressing violations of the Wwft, which are influenced, to varying degrees, by available resourcing. The number and scope of onsite visits undertaken by DNB appears to be inadequate in view of the risks identified in the NRA and the findings from previous examinations.

None of the supervisors work to a methodology for assessing the effectiveness of their supervisory activities and whether they achieve the desired outcome (i.e., deter non-compliance behaviour / achieve greater compliance with the Wwft requirements etc.). Metrics are maintained in relation to number of visits, questionnaires received, days spent on examination etc. but limited or no metrics are maintained to measure whether supervisory measures employed are effective.

Sanctions for non-compliance (Articles 58-59)

The Wwft provides for a wide range of enforcement measures at the disposal of all AML/CFT supervisors. Supervisors have imposed a variety of sanctions (referred to as enforcement measures), which it classifies as either formal or informal, the latter which can be undertaken without have recourse to a formalised enforcement policy or process. In practice and based on the data provided to the assessment team, the DNB and AFM do not make use of the full range of sanctions at their disposal. The DNB and AFM use informal enforcement measures as the most common response to Wwft violations. Supervisors based their decision on which measures to apply in line with formalised enforcement policies. National coordinating bodies or meetings held to decide how to proceed with a particular case were perceived as not being effective and responsive, requiring that supervisors adopt informal measures in order to progress cases as needed.

Tax advisors, and in particular, administration offices, appear to consistently be found to have violations in relation to KYC and CDD requirements and suspicious transactions. A variety of sanctions have been imposed in response, which have included substantial fines. While the level of supervision undertaken has increased and is partly attributable to the increased detection of violations, the findings indicate there continue to be challenges with OEs in these sectors applying the Wwft requirements.

The Enforcement Policy applied by the legal profession outlines a process which, in practice, restricts the Local Bar President's ability to exercise their discretion as to the type of sanction which to impose in response to violations of the Wwft, thus creating the risk that more proportionate sanctions are not imposed in practice. The assessment team was advised that steps are being taken to improve this process.

Overall, neither data is collected by any of the supervisors, nor an analysis is undertaken to determine whether the sanctions imposed are effective in achieving the desired deterrent effect and level of Wwft compliance.

National cooperation and coordination (Article 49 - excluding Law Enforcement agencies)

There is a robust framework for domestic cooperation and coordination, with various platforms among competent authorities as well as private public partnerships (e.g., the FINTEL alliance) which are a strength of the Dutch system. In spite of the extensive cooperation framework, there are a number of issues that could affect both the level of policy-making and the more operational ones. The most significant are related to issues of data ownership and sharing and to the limited role of stakeholders in assessing risk (top-down approach instead of bottom-up, resulting in risks of lack of ownership of findings of risks assessments).

International cooperation between FIUs and supervisors (Articles 45.4, 48.4, 48.5 and 52-57)

FIU-NL cooperates with foreign FIUs regardless of their organizational status and has provided several examples of good cooperation with different types of FIUs (including of administrative nature). The FIU exchanges information with foreign counterparts spontaneously or upon request. The FIU-NL can provide information related to ML even if the exact predicate offence has not been identified at the time of the request for assistance by another FIU.

The issues in the legal framework which could affect the ability of the FIU-NL to use the same powers which it would normally use domestically for obtaining and analysing information pursuant to a foreign FIU's request of assistance, are partly compensated in the practice of the FIU-NL.

There is evidence of active engagement of the Netherlands supervisors in international cooperation. The Netherlands prioritises international cooperation and has mechanisms in place. The DNB works closely and cooperates with the European Central Bank and supervisors of Member States both on an informal level and in the exchange of supervisory information related to AML/CFT compliance about OEs. AML/CFT-related information is exchanged with other Member States and the Netherlands concerning passporting entities.

Nevertheless, risks were noted in relation to the completeness of the information exchanged. Steps have been taken through the introduction of AML/CFT colleges in 2021 to mitigate these risks from occurring. There are limited instances where national cooperation arrangements could impact the effectiveness of international cooperation. The effectiveness of cooperation with regard to ensuring the effect of sanctions and administrative measures in cross-border cases was only demonstrated by the DNB.

ASSESSMENT REPORT

Preface

The present Report outlines the findings on the level of effectiveness of implementation of the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (4th AML Directive) by The Netherlands. It was produced by the Council of Europe pursuant to the Service Contract with the European Commission on Assessment of the Concrete Implementation and Effective Application of the 4th Anti-Money Laundering Directive in the EU Member States (JUST/2018/MARK/PR/CRIM/0166). The process aims to provide the European Commission with analysis on the adequacy of the implementation of the AML/CFT rules in the Member States, excluding the overseas countries and territories of the Member States.

The country assessment was conducted pursuant to a methodology developed by the Council of Europe for this specific purpose, which looks at ways in which Member States implement selected provisions of the 4AML Directive, namely:

i. Risk assessment, internal control and group policies (Articles 8, 45, 46);

ii. Customer Due Diligence (Articles 13.1, 14, 18 (1-3), 20, 21, 22, 23, 25, 26, 27, 28, 29);

iii. Transparency of beneficial ownership information and beneficial ownership registration (Articles 30-31);

iv. Functioning of the FIU (Article 32);

v. Suspicious transaction reporting (Articles 33, 34, 35, 36, 46.2);

vi. Practical arrangements in terms of data protection and record-retention (Article 40 with AML relevance caveat);

vii. Supervision of financial institutions and designated non-financial businesses and professions (Articles 47-48) and sanctions for non-compliance (Articles 58-59);

viii. National cooperation and coordination (Article 49 - without covering the Law Enforcement agencies);

ix. International cooperation between FIUs and supervisors (Articles 45.4, 48.4, 48.5, 52-57, 58.5).

The assessment of Netherlands was carried out concurrently with the European Banking Authority (EBA) in line with the modalities agreed between the Council of Europe and the European Banking Authority.

The assessment team of the Council of Europe was composed of:

1. Mr Giuseppe Lombardo, Council of Europe expert;
2. Ms Samantha J Sheen, Council of Europe expert;
3. Mr Evgeni Evgeniev, Council of Europe Secretariat; and
4. Ms Teresa Armengol de la Hoz, Council of Europe Secretariat.

The on-site visit of the assessment of the Netherlands was replaced with a series of on-line meetings due to the Covid-19 restrictions in place. The duration and scope of the on-line interviews were fully in line with the initially planned on-site visit and followed the principles and procedures applied in previous EU Member State assessments.

Institutions, entities and individuals met during the on-site visit (via videoconference) include (full agenda attached in Annex 2):

1. Dutch Financial Intelligence Unit;
2. Netherlands Authority for the Financial Markets;
3. Dutch Ministry of Finance
4. Dutch Ministry of Justice and Security;
5. The Central Bank of the Netherlands;
6. Tax and Customs Administration of the Netherlands;
7. Netherlands Chamber of Commerce;
8. Dutch Police;
9. The Netherlands Bar (including Legal Profession Financial Supervision Unit (unit FTA) and the Legal Profession Supervision Unit (unit DTA));
10. Royal Notary Association;
11. The Dutch Association of Tax Advisers;
12. Financial Supervision Office (BFT);
13. Sample of banks;
14. Sample of Trust Offices and Domicile Providers;
15. Sample of payment service providers;
16. Sample of lawyers, notaries and legal advisors;
17. Sample of accountants and tax advisors;
18. Sample of asset management and investment firms.

The Report findings are based on: a) 4th AML Directive transposition assessment (Compliance Study of the 4th AMLD and the Funds Transfer Regulation – Country Summary Report and Transposition Table1); b) data provided authorities pursuant to a Council of Europe dedicated questionnaire and statistical table; c) information gathered during an on-site visit and meetings with sample reporting entities and competent authorities (20 - 23 September 2021) and provided following the on-site visit.

Feedback on the relevant parts of this assessment report concerning the practical application of the 4th AMLD requirements with regard to the banking sector was provided by the European Banking Authority.

[1] Please note that the assessment of technical compliance falls outside the scope of the current review.

The Report presents the analysis on the effectiveness of implementation and practical application of the select provisions of the 4th AMLD divided into four main themes (pillars) as follows:

a. **Status of Transposition:** Includes an overview of the remaining deficiencies related to the transposition (incompleteness or non-conformity). Where relevant, the relation to the scoping of issues for further analysis is noted.

b. **Analysis of Application in Practice:** Assessment of the issues affecting the effectiveness of implementation and practical application for each Article of the 4th AMLD under the respective theme.

c. **Compensatory Measures and Detrimental Factors Section:** Presents any underlying reasons for the deficiencies in the practical application of the 4th AMLD of a systemic nature, related to contextual factors, as well as any additional legal requirements, practices and procedures that impact the practical application. Alternative measures that contribute to the effectiveness even in the case of gaps in transposition or application are also identified.

d. **Conclusions:** Conclusions on the level of practical application are presented in a standard, uniform manner ensuring consistency between the themes and with other reports. The overall effect on the AML/CFT objective of the Member State and the application of other provisions of the 4th AMLD is also assessed, where relevant. Finally, the analysis focuses on the impact of the observed deficiencies on the effective application of the directive.

Findings presented in this Report reflect the situation in the Netherlands at the time of the on-site visit (from 20 - 23 September 2021). Any subsequent changes to legislation, policies, and operational practices are not reflected in this Report.

This report follows the approach in reviewing the effectiveness of implementation of the 4th AMLD developed and applied by the Council of Europe to all EU Member States assessments. The analysis focuses on the deficiencies and any factors detrimental to the effective application of the respective themes (provisions of the 4th AMLD within the scope of the assessment). When analysing the practical application of the 4th AMLD provisions the following general factors when considered to be of a systemic nature could be taken into account (examples):

- Any conflicting provisions of the Member State legislation or regulatory framework that are contrary to or create significant obstacles for the application of requirements of the 4th AMLD;
- Any established practices that are contrary or create significant obstacles for the application of requirements of the 4th AMLD;
- Any deficiencies arising from the implementation of requirements or procedures that are considered by the Member State authorities to provide an alternative to the 4th AMLD requirements to achieve the same result;
- Failure to ensure the allocation of proper resources for the application of the 4th AMLD requirements;
- Deficient action by national authorities to enforce the application of the 4th AMLD;
- Lack of cooperation in the field of AML/CFT with the obliged entities, member states authorities, EU institutions;

- Failure to ensure proper application of sanctions and other remedial measures.

Authorities' comments

The draft report was submitted to the authorities for comments on 10 December 2021. The feedback and input from the authorities was received on 21 December 2021.

The assessment team adopted a range of substantive amendments based on the additional information provided by the authorities. In strict application of the methodology and after careful consideration of the consistency with the information obtained by the assessment team as well as with the scope of the 4th AMLD process, some amendments suggested by the authorities were not accepted. The views expressed during the interviews were also duly taken into account by the assessment team.

CHAPTER 1. Overall Risk Focus of the Assessment

Contextual Factors, Risks and Issues of Focus for the Assessment

1. The Netherlands has a highly developed financial system2 with a number of systemically important institutions globally and at European level. Despite the general resilience of the financial sector some vulnerabilities associated with the interconnectedness of the Dutch financial system and the (AML/CFT) supervision of the financial sector, were taken into account for the assessment of the practical application of the 4th AMLD. The events related to failures in AML/CFT compliance of a number of banks in the European Union (among which ING) had significant repercussions as reflected in a 2019 report3 of the European Commission on the assessment of recent alleged money laundering cases involving EU credit institutions.

2. The substantial level of inward and outward FDI of the Netherlands is also noted4. The significant trade linkages of the Netherlands, economic competitiveness and export orientation are important contextual factors with regard to the ML and FT risks5. The Netherlands is also considered very important transit country in terms of trade6. While measures have been undertaken by the Netherlands to mitigate risks associated with aggressive tax planning7, the effectiveness of some measures remains to be demonstrated.

3. Moving funds through special purpose entities, letterbox or shell companies with no real economic activity in the Netherlands has been widely observed8. The development of particular associated activities and sectors of the economy (setting up companies, tax advice, associated financial services etc.) and the general attractiveness of Dutch financial markets9 required particular attention to the effectiveness of application of AML/CFT measures to target potential misuse of legal entities and arrangements and the financial sector, ensuring strict compliance by company service providers, tax advisors, and several other DNFBPs and increasing transparency of beneficial ownership. Financial secrecy, the complexity of business ownership and the high share of foreign shareholders10 are factors which the team took into account for the assessment.

---

[2] Assets close to 800% of GDP, with the banking sector accounting for half of the assets in the financial sector. Please see p. 6 of the IMF Financial System Stability Assessment 2017, IMF Country Report No. 17/79, accessed July 2021. Please see also p. 13 and further for vulnerabilities.

[3] Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institutions, Brussels, 24/7/2019, COM(2019) 373 final.

[4] Please see 2020 European Semester: Country Report the Netherlands 2020, accessed July 2021.

[5] See e.g. Dutch National Risk Assessment on Money Laundering 2019, H.C.J. van der Veen, L.F. Heuts, with the cooperation of E.C. Leertouwer.

[6] Ernesto U. Savona and Michele Riccardi (eds), 2018, Mapping the risk of Serious and Organised Crime infiltration in European Businesses – Final report of the MORE Project. Milano: Transcrime – Università Cattolica del Sacro Cuore.

[7] Please see e.g. p. 7 and p. 28 of the 2020 European Semester: Country Report the Netherlands 2020, accessed July 2021.

[8] Please see e.g. An overview of shell companies in the European Union, EPRS | European Parliamentary Research Service, Ivana Kiendl Krišto and Elodie Thirion, Ex-Post Evaluation Unit and European Added Value Unit, PE 627.129 – October 2018; as well as 2020 European Semester: Country Report the Netherlands 2020, p. 32.

[9] 2020 European Semester: Country Report the Netherlands 2020, p. 32.

[10] Ernesto U. Savona and Michele Riccardi (eds), 2018.

4. The Dutch National Risk Assessment on Money Laundering 2019 identifies 15 major ML risks of significant residual potential impact, the highest including ML via crypto currencies, trade-based constructions involving services, underground banking, including unlicensed payment service providers, use of offshore companies and dealers of high value services/goods. Money laundering via trade-based constructions involving goods, via legal entities and the use of intermediaries, physical movement of cash, structures by trust offices, fictitious company turnover, investment institutions/companies and bank wire transfers are identified as areas of lower impact.

5. The ML NRA does not provide substantial detail with regard to the ML predicate offences, although it refers to another extensive study where fraud and drug crimes were estimated to be the most important offences. In view of the aforementioned contextual factors the assessment team attempted to obtain a more granular understanding of the authorities and obliged entities of the important types of predicate crime and the application of relevant mitigating measures. Although various relevant statistical data has been taken into account to identify risks, the NRA acknowledges issues concerning quantitative data to perform an overall analysis. Moreover, it notes that they could not get the data they wanted because of issues in obtaining consent from (public) stakeholders that had the data.

6. Some studies11 point out the gambling and betting activities as particularly attractive for investment by organised crime groups. Despite action indicated by the authorities to target illegal gambling, the assessment team considered important to focus further on the issue of providers of gambling services (online) that may be offering their services to Dutch residents without being licensed, and what steps are authorities taking to tackle this phenomenon.

7. The FT risks of highest residual potential impact include financing via foundations or other legal entities (charitable, religious, educational) and acquisition of and/or financing with legally obtained personal funds12. In addition, the FT NRA refers to funds obtained via 'charities' without a legal form, financing with crypto currencies, use of fictitious or non-fictitious flow of goods, physical movement of cash, loans or gifts from private persons, funds obtained via fraud, use of online platforms/payment service providers, underground banking, and unlicensed payment service providers. The assessment team saw merit in assessing the level of understanding of the authorities and private sector of the patterns of FT risk identified in detail by the NRA.

8. The EU Supra National Risk Assessment of 2019 found that the use of new technologies by such regulated entities as FinTech, can enable speedy and anonymous transactions with increasingly non-face-to-face business relationships, while bringing considerable benefits, but may pose a higher financial crime risk. The increased reliance upon technology-enabled services the last 18 months has had a commensurate increase in the FC risk exposure associated with them.

9. The Netherlands has operated a residence-by-investment scheme aiming to attract wealthy foreign nationals since 201313. There has been no information made available to the

[11] Please see e.g., p. 194 in Ernesto U. Savona and Michele Riccardi (eds), 2018, Mapping the risk of Serious and Organised Crime infiltration in European Businesses – Final report of the MORE Project. Milano: Transcrime – Università Cattolica del Sacro Cuore.

[12] Dutch National Risk Assessment on Terrorist Financing 2019, H.C.J. van der Veen, L.F. Heuts, with the cooperation of E.C. Leertouwer

[13] European Getaway. Inside the Murky World of Golden Visas. Transparency International 2018.

assessment team (prior to the on-site meetings) on any mitigating measures particularly targeting associated risks although some information about the scheme's criteria is publicly available14.

10. **Risk assessment, internal control and group policies (Articles 8, 45, 46).** The team assessed the private sector (both FIs and DNFBPs) awareness and understanding of the ML/FT risks present on country level as noted above and the risks to their business/sector, the implementation of risk assessment requirements by categories of OEs, particularly the financial sector (banks, asset management and investment firms), payment service providers and DNFBPs, particularly the variety of entities providing company services. Emphasis was put on OE policies, controls and procedures for effective mitigation and management of ML/FT risks and training programmes for employees to mitigate the identified risk. The team also considered the level of available guidance regarding up-to-date information on the ML/FT practices provided by the authorities and the provision of feedback on filed unusual transaction reports.

11. **Customer Due Diligence (Articles 13(1), 14, 18 (1-3), 20, 21, 22, 23, 25, 26, 27, 28, 29).** In addition to ascertaining the application of CDD measures commensurate with major ML/FT risks, the team explored how the FC risks associated with new technologies were taken into account within the obliged entities' CDD activities including whether appropriate guidance on the risks associated with such technologies is available and used, including typologies and case studies shared by supervisors and enforcement with regulated entities to support such detection efforts. It is interesting to understand how PSPs satisfy both record retention and data protection provision required transposed under the 4th AMLD.

12. The assessment team took into account the limited information provided as part of the assessment and the seemingly limited efforts of the authorities to target the risks associated with possible misuse of investment-related insurance policies (particularly in relation to the risk of tax evasion). Omission of these products from the CDD process is unclear, in light of the ways in which they have been misused by customers both in relation to ML and tax evasion. The information provided by the authorities indicates that familiarity with AML/C FT requirements within the insurance sector still lags somewhat behind that of other sectors supervised by DNB and life insurers mainly regard the requirements from the Wwft as an administrative burden and believe that primarily the banks should perform a gatekeeper role. The team assessed whether steps have been taken by the DNB to both raise awareness of banks to the FC risks associated with investment-related insurance products and measures taken, in order to verify whether those efforts have impacted the application of the AML requirements.

13. With regard to the application of CDD measures to existing customers, the basis upon which reviews are initiated can impact upon the timely detection of material changes to a customer's understood risk profile and assigned risk rating. The operationalisation ensuring that reviews are resourced and undertaken to effectively detect such changes was an area explored by the team. While work was undertaken to raise the PSP sector' SIRA quality and the taking of enforcement action where non-compliance was observed, the size and nature of the population of payment institutions has changed considerably, along with their payment volumes, over the last 2 years. The current Dutch population of payment institutions is very diverse, not only in size and transaction volume, but also in services, channels and geographical activity, requiring CDD measures of varying degrees of complexity. The team reviewed the customer due diligence processes applied by regulated payment service businesses to both new and existing

[14] See: https://ind.nl/en/Pages/Investing-in-the-Netherlands.aspx

customers and the examination method applied by supervisors in evaluating both their technical compliance regulatory requirements and effectiveness of those controls.

14. **Transparency of beneficial ownership information and beneficial ownership registration (articles 30 and 31).** The mission focused on the effective implementation of articles 30 and 31 on beneficial owner transparency. At the time of the COM assessment, these two provisions were in the process of being transposed by a legislative proposal due to be submitted to the House of Representatives of the States General. Taking into account the risks and challenges related to misuse of company structures, the assessment team focused on the availability of adequate up-to-date BO information and records held with legal entities and trustees along with measures taken by the authorities to ensure accuracy of the BO information as well as any particular strategies applied in order to mitigate the risks associated with the use of special purpose entities, letterbox or shell companies and cooperation among the competent authorities to that end.

15. **Functioning of the FIU (Article 32).** The mission also focused on the powers of the FIU to obtain all the information it needed to properly undertake its functions, particularly information from obliged entities that have not submitted a UTR, whether in the context of financial analysis or at the request of a foreign FIU. The analysis of COM notes that article 32.4 of the Directive is not explicitly transposed and that it is not sure that the FIU can have access to data concerning financial, administrative and enforcement information that it requires to fulfil its tasks.

16. **Suspicious transaction reporting (Articles 33, 34, 35, 36, 46.2).** The assessment team focused on the level of reporting by certain categories of OEs, such as inter alia non-bank FIs, legal professionals (e.g., lawyers and accountants) along with the various entities providing company services and mechanisms for reporting). The mission aimed to also ascertain whether legal privilege (for lawyers) was a hindrance to the effective implementation of this article and, more in general, to the implementation of the UTR requirements.

17. **Data protection and record-retention (Article 40 with AML relevance caveat).** The team reviewed the extent to which regulated entities understood and have operationalised controls to ensure that record retention requirements, limits on its use and the destruction of those records, are complied with. The team also explored guidance and feedback provided by supervisors to regulated entities on their compliance with these requirements within the context of their overall AML/CFT compliance programmes.

18. **Supervision of financial institutions and designated non-financial businesses and professions (Articles 47-48) and sanctions for non-compliance (Articles 58-59).** In view of the market entry requirements falling mainly under the remit of a number of industry associations, the assessment team focused on the assessment of the application of measures and relevant cooperation to prevent criminals convicted in relevant areas or their associates from holding a management function in or being the beneficial owners of those obliged entities. In view of the incidents involving financial institutions from the Netherlands and in view of certain vulnerabilities previously noted in supervision by DNB and others in the financial sector the team aimed to assess any changes in the effectiveness of supervision. The team assessed whether supervision was carried out in line with the important ML/FT risks. The team explored the approach taken by supervisors, during their examination of regulated entities, in relation to their use of new technology. The availability of sufficient guidance (on CDD related to new technologies, application of measures related to existing customers, etc.) was explored. The ability of supervisors to impose appropriate and proportionate sanctions is

a critical element of the Netherlands AML regulatory framework. While the technical requirements of the 4th AMLD have been mostly transposed in relation to sanctions, there was limited information provided to the team with regard to the approach taken by supervisors to decide which sanctions should be imposed in a given case. The team reviewed the process followed by the supervisor when assessing cases involving AML deficiencies and how they determined which sanctions, if any, should be imposed. The team also reviewed how supervisors evaluate the effectiveness of those sanctions, in terms of their intended use and influence of the obliged entity involved.

19. **National Cooperation (Article 49).** The NRA also notes that data sharing between competent authorities could be improved (one of their lessons learned). Therefore, the team focused on these important aspects both in terms of strategic planning as well as operational exchange.

20. **International cooperation (Articles 52-57, 45.4, 48.4, 48.5 and 58.5).** In view of the international nature of some financial institutions in the Netherlands and their customers, international cooperation is essential for the timely detection, disruption and prevent of financial crime, notably in relation to innovative businesses such as FinTechs and the misuse of new products and services. Noted in the 2019 NRA, that of the 15 greatest money laundering threats these include ML via offshore companies. The timeliness in which information can be exchanged and actioned, it is a critical element that the team looked into, in terms of the additional resources for the responsible bodies that are available to them. The team also assessed the extent to which the availability of those resources contributes towards effective cooperation.

CHAPTER 2. Application of risk assessment, internal control and group policies (Articles 8, 45 and 46)

Status of Transposition

21. The analysis of COM does not note any issue of transposition or conformity with regard to these articles.

Analysis of Application in Practice

Article 8

22. Supervisory authorities have issued sectoral guidelines concerning the implementation of the AML/CFT law, including for the requirement to carry out and document an enterprise-wide risk assessment (EWRA). Although these sectoral guidelines require risk assessment for customers, product, service transactions, channels of deliveries and geographic risk, they (particularly those for DNFBPs, except those under the purview of the BTWwft, e.g., real estate agents) do not provide sufficient operational details for the OEs. As regards OEs that fall under the purview of the DNB, they are required to undertake a "systemic integrity risk analysis" (SIRA), which is an analysis of "integrity risk", rather than specifically of the ML/FT risk, which is included in the assessment as one of the risk components (together with corruption, fraud, circumvention of sanctions, etc) and should be performed at least annually. The SIRA is integrated with an assessment of the integrity risk appetite of the firm and informs the firm's AML/CFT policies. The DNB has issued an "Integrity Risk Analysis" good practice paper for OE's to assist them in performing the assessment of their integrity risks, including AML/CFT risks and the control environment for such risks, as well as good practices on Integrity Risk Appetite.

Specifically concerning the AML/CFT component, a Chapter in DNB's a Guidance on the implementation of the AML/CFT law focuses on AML/CFT risk assessment.

23. While the conceptual approach underlying sectoral guidance for the risk assessment is sound (being based on the identification of the inherent risk, an analysis of the effectiveness of the control measures and of the impact of the unmitigated risk) and entails all the elements envisaged by the Directive, it is too high-level and not sufficiently detailed (for example it does not explain in particular the analysis of the control measures, and the risk scenarios are quite basic and refer only to ML and not to FT). The DNB Guidance is not sufficiently tied to the findings of the NRA and does not differentiate between the different types of OEs that fall under the purview of the DNB. Of these shortcomings, the most significant is the one concerning the near absence of risk scenarios for FT, given the FT risk posed by the Netherlands, which was also confirmed by the banks interviewed during the evaluation and which has resulted in an insufficient assessment of the FT risk, as also confirmed by a thematic review on FT conducted by the DNB in 2018.

24. Supervisors check systematically, to varying degrees, that OEs undertake risk assessments which consider customers, countries/geographic areas, products, services and transactions, which may include a review of the quality of the EWRA performed by the OEs under their purview (for FIs, for DNFBPs the focus is more on whether CDD is carried consistently with the risks identified, rather than a focus on the EWRA per se, which, in most cases, is justified by the small size of the DNFBPs). Since the introduction of the requirement to undertake risk assessment in 2015, the DNB has been very proactive in ensuring that OEs implement this requirement, particularly by conducting a thematic review in 2015 which showed that several firms had not yet complied with the requirement. The DNB took several remediation measures and conducted also a follow-up review in 2016, which showed significant improvement in the compliance with this requirement. Although according to the DNB the quality of the SIRA has overall improved, there remain challenges for banks to identify and address emerging risks (such as VASPs). In 2019, according to the DNB, 14% of the banks did not undertake a SIRA, and a thematic review conducted in 2019 on 6 banks revealed shortcomings related to the quality of the SIRA. Issues were also observed with incorrect classification of customers based on their ML/FT risk (with customers being classified as low risk by default). From the analysis of the questionnaire that the DNB receives annually from its OEs, the DNB found that 83% of the banks have formulated an integrity risk appetite, but only for 5% of the banks there is a risk appetite statement with verifiable indicators and/or limit values; and that there is often no identifiable link between the SIRA and the risk appetite.

25. As regards DNFBPs, contradictory information was provided by the BTWwft with regard to the compliance of the real estate agents with this requirement, while one of the findings of the inspections undertaken by BFT is that OEs that fall under their purview, depending on their size, do have an understanding of their AML risks. However, their ML risk is not always correctly and consistently applied to their customer base and do not always take into account all relevant risk factors. Additionally, they do not always record a separate risk profile for each individual customer. One of the main findings from AML inspections performed by the KNB (Royal Dutch Association of Civil-law Notaries) in 2019/2020 was that notaries have insufficient sound business practices with respect to AML risk policies. All of these supervisors have taken steps to remedy these deficiencies.

26. Banks and FIs interviewed undertake the EWRA regularly. In general, the types of OEs interviewed demonstrated varying degrees of awareness of the findings of the NRA and particularly of their requirements to undertake an enterprise-wide risk assessment (EWRA): a

common shortcoming observed across types of OEs (including few banks) is the confusion between the EWRA and the risk classification of the customers. FIs and some DNFBP types (e.g., accountants and tax advisors) exhibited a better understanding of their risks and corresponding mitigating measures adopted, while some DNFBPs (e.g., lawyers) had a less satisfactory understanding of their risks in few instances. However, the understanding of the FT risk by the OEs interviewed was not commensurate to the risk of FT in the Netherlands, as it was very generic. Only some banks were able to articulate sufficiently on FT risks and specific measures to mitigate it, albeit only in the context of foundations and foreign terrorist fighters, acknowledging that the SIRA does not allow for FT-specific risk scenarios that can be effectively embedded in transaction monitoring.

27. In general, the OEs interviewed demonstrated that they have policies for customer due diligence (CDD), reporting, record-keeping, internal control, employee screening and compliance arrangements.

28. On-site visits to inspect the functioning of the compliance function of banks has been carried out since 2014, showing that the quality of the compliance function needs to be improved. This applies both to the number and quality of FTEs of the compliance function and the adequate fleshing-out of the countervailing power. The reporting by compliance to senior management is sometimes considered to be inadequate (this was confirmed also by the interview of certain banks, where the AML/CFT compliance function did not have a direct reporting line with management and was embedded in other departments of the bank). These issues are also observed by DNB in its AML/CFT investigations. With regard to the audit function, the findings of the DNB show that this is adequate in most large and mid-sized banks, whereby the quality of the audit function is lacking in small-sized banks. The audit function is often IIA-certified and turns out to be a good countervailing power for the business. Some banks do not have their own audit function or only a very limited one; they use external parties to carry out this work. In those cases, there are sometimes doubts about the independence and/or quality of the audit work carried out. In the annual integrity risk questionnaire, several questions are asked regarding the compliance and audit functions.

29. Larger law firms (and other independent professionals) have a dedicated AML/CFT function, although some concerns were expressed, in at least one case, on who should bear the responsibility of filing the UTR in case of a disagreement between the professional that has identified the transaction as suspicious (and how personally bears responsibility for not reporting it) and the compliance officer.

Article 45

30. In the Netherlands, the most material institutions belonging to a group are banks and payment service providers (PSPs) (out of those the assessment focused on). Oversight on the operation of group policy varies from one institution to another. Foreign banks that have a subsidiary or branch office in the Netherlands often rely heavily on the policies and procedures of their parent. Where this concerns a parent from outside the EU, investigations by the supervisor often show that they are not sufficiently adapted to the AML/CFT law. DNB will then call the relevant institutions to account for this. Banks must inform DNB if they operate in countries where they cannot comply with the requirements of the AML/CFT due to other legislation and regulations. If such a situation arises, a bank should implement alternative measures to comply with the legal requirements or when this is impossible the bank should cease the activity in question or move it to another jurisdiction. DNB has not been informed of any such situations. Following a number of incidents at foreign branches of Dutch institutions, DNB carried out

investigations to establish compliance with the AML/CFT obligations at subsidiaries and branches of Dutch institutions. Reference was provided to an important case in which the DNB imposed a group-wide remediation to a bank.

31. Several firms (both FIs and DNFBPs) expressed concerns arising from partial alignment between the AML/CFT Directive and the data protection directive which has also cascaded at national level, posing challenges to the sharing of specific information among the group (e.g., the client name, in the case in which the client has been reported in a UTR). The DNB is in discussion with some institutions about sharing suspicious transaction information within the group where they encounter conflicting local legislation in other Member States.

32. OEs belonging to groups (including international groups) were (with very few exceptions) generally aware of risk assessment undertaken at group level and of relevant risk-mitigating policies, although in some cases the risk assessment appeared to have been conducted at the level of the single institution, rather than at group level.

33. In line with the Directive, the prohibition of tipping off does not apply to the exchange of information intra-group (including where branch or subsidiaries of the group are in third countries), unless the FIU prohibits to disclosure of the relevant information. In the period under review there were no cases in which the FIU has instructed OEs to refrain from sharing information within the group.

Article 46

34. Training plans and programs and their implementation by OEs are generally checked during inspections carried out by supervisors, particularly the DNB and AFM. DNB investigations have shown that close to all institutions regularly give AML/CFT training courses. All the banks investigated by DNB offer (mandatory) training to their employees in the field of compliance and the statutory AML/CFT requirements. The frequency and depth of training varies greatly from bank to bank. Where necessary, DNB provides feedback to investigated institutions on what the regulator notices with regard to training. From the investigations conducted by DNB, it became evident that not all employees of exchange institutions take training courses on a sufficiently regular basis and were insufficiently familiar with AML/CFT legislation and regulations.

35. As regards other types of FIs that fall under the purview of the AFM, the answers to the risk questionnaire in 2018 by 289 investment firms show that only half of the firms provide training so that employees and policy-makers are familiar with the provisions of the AML/CFT law. By 2019, this percentage had grown to more than 60%, thanks to the AFM's attention to this subject in its Guideline, investigations outreach initiatives. In 2020, 78% of the investment firms did provide AML/CFT training. The percentage of investment firms that provide AML/CFT training has therefore steadily been increasing since 2018.

36. In the period under review Dutch authorities, including through public-private partnerships, have made significant efforts to provide guidance and training on ML/FT typologies and red flags to improve the quality of the UTRs, including by engaging the most material types of OEs on a regular basis by the FIU to discuss the quality of the UTRs. The Fintell Alliance, which includes 4 major banks and key stakeholders, is a very effective avenue for conveying critical information to the banks. Although feedback on specific STRs (i.e. when a UTR becomes an STR after the FIU's analysis) may not always be provided, in line with the Directive's approach which requires feedback "where practicable", several types of OEs complained about the lack

of feedback (calling into question the effectiveness of the UTR regime) and some OEs have also remarked that in some instances where they have not received feedback this has created some challenges as the customer that is the subject of an UTR is placed under enhanced scrutiny by the OE. The FIU stated that after a report has been declared suspicious the obliged entity receives a notification about the declaration, and that FIU representatives (so-called 'relationship managers´) maintain close contacts with OEs, their branches and association of obliged entities to inform them on relevant developments with regard to the reporting of UTRs, to raise awareness as well as to share cases, best practices and to discuss ways forward.

Compensatory Measures and Detrimental Factors

37. Not applicable.

Conclusions (risk assessment, internal control and group policies)

38. The assessment team has identified **major deficiencies** in the practical application of the risk assessment, internal control and group policies measures with **major impact** on the effectiveness across all sectors of OEs, as follows:

    a. Uneven implementation by OEs of the requirement for carrying out comprehensive risk assessments.

    b. Insufficient identification of FT risk, particularly by FIs.

    c. With a few exceptions, guidelines for risk assessment are not sufficiently detailed.

    d. Compliance functions' reporting lines are not always appropriate to the size of the business.

    e. Privacy provisions hinder the sharing of information of critical data between firms belonging to a group (particularly when the parent or branches/subsidiaries are in third countries).

    f. Concerns about the lack of feedback on UTRs in some cases and the timeliness of feedback (please see below).

CHAPTER 3. Application of customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3, 20-23, 25-29)

Status of Transposition

39. In terms of completeness, the transposition analysis of COM[15] does not note any issue.

40. In terms of conformity with the Directive's provisions, the transposition analysis of COM notes issues concerning: i) Article 20(b)(ii) of the Directive on taking adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with politically exposed persons and on ii) Article 21 of the Directive on requiring obliged entities to take reasonable measures to determine whether the beneficiaries of a life or other investment-related insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons.

Analysis of Application in Practice

Sub-theme (a): General CDD

Article 13.1

41. Obliged entities interviewed by the assessment team demonstrate good knowledge and understanding of CDD elements contained in Article 3 of the Wwft. Identity is determined and verified on the basis of valid official documents for natural persons and comprehensive corporate identity documentation for legal persons and arrangements. Obliged entities interviewed report they have procedures in place for the determination and verification of UBO of corporate entities in line with the requirements of the 4th AMLD up to the natural person(s) who ultimately owns or controls the customer, or on whose behalf a transaction or activity is carried out. Entities demonstrated good knowledge of the ways in which control can be exercised over legal entities and through the use of complex structures.

42. Some entities reported a familiarity with the risks associated with "golden visas", and undertake due diligence, on a risk basis, to verify whether a customer or owner holds more than one form of citizenship. Obliged entities demonstrate their use of procedures for CDD commensurate with the different product and services they offered. Trust and corporate services providers and trust offices have a strong awareness of the risks associated with nominee arrangements and efforts to conceal ownership and control.

43. Establishing the purpose and intended nature of business relationships is also understood by most obliged entities to be an essential element of CDD. Published guidance for payment service providers about compliance with Article 3 has not yet been generated, particularly in relation in relation to platforms and other partnership arrangements entered into and relied upon by the payment service provider. The DNB has advised the assessment team steps are being taken to produce published guidance on this subject in the near future.

[15] Please note that the Status of Transposition sections are entirely based on the 2019 COM analysis. The review of technical compliance falls outside the scope of the assessment. Therefore, the team notes but cannot take a position on the statement of the authorities that there are no remaining transposition issues related to completeness and conformity.

44. Guidance is published by all supervisory bodies, providing examples of best practices, typologies and examples of how to calculate beneficial ownership both in relation to legal entities and arrangements. Most obliged entities considered this Guidance to be useful and relevant. Guidance has been updated or published on tax integrity risks and the importance of CDD in its detection and prevention. In limited instances the guidance published has not been refreshed to reflect more recent observations and best practises (See, for example, see post transaction analysis guidance for payment service providers dated 2017, and risk indicators document published by the BFT dated 2014).

45. Following frequent interventions by DNB, several of the Netherlands' major banks have rolled out large-scale and long-term CDD remediation and improvement programmes in recent years, investing in new IT support for CDD. The DNB has taken steps to build upon the deterrent effect of these programmes to ensure that other banks initiate measures to improve the effectiveness of their AML/CFT compliance programmes and reduce the risk of similar cases transpiring in the future.

46. Some obliged entities find implementation of the senior managing official as UBO requirement to be challenging. Guidance has been issued on this obligation, but some OEs experience difficulty in interpreting circumstances where this measure is appropriate.

47. Some trust offices and trust and corporate service providers note challenges in establishing full ownership structures where they are not administering all entities that form a part of that structure. DNB has noted that some trust offices have exited client relationships, following an investigation by the supervisor, where it has been unable to establish a clear understanding of the client ownership structure. This has occurred despite the fact the client has been accepted, contrary to the requirements of Wtt 2018 which requires that that trust offices have full understanding of the entire structure.

48. Supervisory data indicates that certain sectors continue to show weakness in their implementation of Article 3's requirements in two industry sectors – real estate and tax advice, in particular administration offices. Real estate agents constitute a high-risk group, which is mentioned in the NRA a number of times as a risk "the purchase/construction of real estate and/or renovation using undeclared or untraceable funds".

49. The supervisors for real estate agents have undertaken several supervisory measures to raise awareness in the sector about the fulfilment of their AML/CFT obligations. This has included presentations at real estate agent member meetings and periodic consultations with the three largest estate agents', FIU-NL and the Ministry of Finance. .

50. Tax advisors were found to not comply with CDD requirements in consistent proportions across a five-year period (2015 – 2020), inclusive of the time period within the scope of this assessment. The BFT reports this is primarily, although not exclusively, in relation to administration offices. The figures suggest an ongoing challenge with non-compliance with Article 3. These failings also occur in conjunction with other AML/CFT compliance failings.

51. Domiciles and vehicle dealers were also reported to have a disproportionate number of compliance deficiencies related to their implementation of the CDD requirements. Additional resources have been allocated to provide additional supervision to these sectors. Sanctions and other measures have been imposed to reduce the risk of reoccurrence and deter non-

compliance within these sectors.16In relation to both the tax advice sector, and, in particular administration offices, the BFT has analysed the possible causes for the of non-compliance with the Wwft requirements. These relate to the relative size of the businesses compared to the other OEs, the absence of a professional body for administration offices conducting professional oversight, the limited size of individual organisations i.e., a lot of organisations with only one staff/owner and the (lack of) professional qualifications required for the operation of administration offices. Efforts have therefore been made to undertake enhanced supervision of this subsector.

52. The assessment team identified evidence to suggest that some obliged entities in the investment sector also fail to effectively implement the CDD requirements. These included deficient information about the intended use of products (anticipated transaction activity), failure to identify all beneficial owners of a customer, and failures to complete CDD in full prior to onboarding of a customer. These occurred in conjunction with other system implementation failings at the same obliged entity. It is unclear based on the evidence provided to the assessment team, what further steps have been taken by the supervisor to determine whether these failings are more broadly systemic across the sector.

53. Several of obliged entities interviewed are currently using or planning to use automated onboarding processes, supported by use of non-face-to-face identification verification technology and/or supplemented by artificial intelligence to undertake CDD. Most annual questionnaires do not request information from obliged entities about their actual or planned onboarding processes. Those which do ask for information are limited to asking for a general description of the onboarding process used and the number of customers onboarded in this manner. Information is not requested concerning how CDD measures are applied to comply with Article 3 using this method of non-face-to-face onboarding. Obliged entities reported having never received any formal guidance from supervisors about the use of eKYC or online onboarding of customers. Some entities rely upon guidance issued by other jurisdictions. Other entities reported having taken the initiative to brief supervisors about their online onboarding initiatives but receiving very little by way of guidance or feedback as to whether those plans were considered aligned to the Wwft's CDD requirements.

Article 14

54. None of the FIs and DNFBPs interviewed referred to practices to verify the identity of the customer and the beneficial owner during or after the establishment of a business relationship or the conduction of a transaction. Accordingly, the gaps related to the transposition (i.e. non-conformity in terms of completing procedures as soon as practicable after initial contact, and of opening of accounts under adequate safeguards) do not appear to have a measurable impact on effective implementation.

55. Some payment service providers employ the use of simplified due diligence as permitted under Article 6 of the Wwft to onboard new merchants, deferring certain CDD measures to be completed following the establishment of the business relationship. One model used by payment service providers provides for pay-in or receipt of funds into a merchant's account, with pay-out or settlement to the merchant from those funds only permissible once all required

[16] The regulated nature for AML/CFT purposes of these two sectors creates additional challenges for its supervisor, which includes measures to identify domiciles operating but otherwise not complying with the Wwft requirements.

CDD is completed. It is unclear whether measures are in place to ensure that the CDD requirements of the Wwft are completed, where CDD measures are deferred.

56. There is evidence that obliged entities in the investment sector have onboarded customers without having first completed CDD. Deficiencies have not been detected due to corresponding CDD review requirements which were assessed by the supervisor as being set according to time intervals too long relative to the risk rating assigned to the customer (e.g., review periods of once every three years).

57. As to the application of CDD to existing customers under Article 3(11) of the Wwft, obliged entities refer to the practice of reviewing CDD information in customer files on a regular (e.g., semi-annually or annually) or ad-hoc (e.g., in case of unusual/ suspicious activities) basis. However, there are deficiencies in the effective implementation of this requirement. Some obliged entities have established time periods for CDD reviews which are not sustainable, relative to available resourcing and capacity. In other cases, obliged entities have attempted to establish, on a risk basis, longer review intervals (sometimes up to 5 years), which prevent the timely detection of changes to a customer's existing CDD information or risk profile.

58. Some obliged entities experience difficulties implementing a CDD review process for existing customer that combines both periodic reviews (based on a specified period) and trigger-events (transaction alerts or adverse media monitoring). Procedures to undertake reviews in response to trigger events are not clearly described in operational procedures. Some supervisors place emphasis on the time and efficient processing of transaction monitoring alerts but fail to determine whether such measures comprise the effectiveness of timely detection of changes to customer CDD information. No guidance is provided to clarify how obliged entities should approach the review of existing CDD information beyond the requirements outlined in the Wwft.

59. The large-scale AML cases in the Netherlands banking sector highlighted how the effectiveness of existing customer CDD reviews can be compromised. Examples in these cases included backlog of adverse media reviews, late detection of customer risk profile changes and escalation of suspicious activity. These factors do not appear to have been understood by some obliged entities or used to inform supervisory assessment of effective practices in the fulfilment of this requirement. The failure to conduct timely and effective CDD reviews can expose obliged entities to unmitigated financial crime risks associated with business relationships. It can also prevent entities for detecting previous non-compliance with CDD requirements and allow for the timely adjustment of monitoring measures where the risk profile of a customer has changed. These prevent obliged entities from ensuring they have a clear view of their overall financial crime risk exposure and whether this exceeds their established risk appetite.

Articles 18.1-18.3

60. Most obliged entities interviewed demonstrate an adequate understanding of the instances wherein enhanced CDD measures should be applied to mitigate higher risks associated with cross-border and PEP relationships, as well as with shell banks. Higher risk scenarios are interpreted and applied in a way that take into account the factors set out in Annex III of the 4th AMLD, with reference to customer risk, product risk and geographical risk. Background and purpose checks seem to be part of routine business for all transactions, including complex or large ones or those lacking apparent economic or lawful purpose.

61. Detailed guidance is provided on the undertaking of enhanced CDD, including typologies. Annual questionnaires request detailed information from obliged entities about customers, transactions and links to high risk jurisdictions, products and payment methods.

62. As to the scope and nature of enhanced CDD measures, banks, trust and corporate service providers and most professional entities are able to clearly define the measurable difference – between standard and enhanced measures in terms of additional information obtained and increased number/ timing of controls applied in higher risk situations.

63. Payment services providers and other DNFBPs met have a rudimentary understanding of enhanced CDD measures. Investment firms met demonstrate a similar level of understanding and have been identified as having several shortcomings in their implementation of CDD and other AML/CFT requirements, as noted in the sections above.

Sub-theme (b): CDD for PEPs

Article 20

64. Risk management systems that obliged entities are required to implement under Article 8(5) of the Wwft for determining PEP status of customers and beneficial owners are anchored on commercial screening databases and supplemented by customer self-statements during the onboarding process. Obtaining senior management approval, establishing the source of wealth and source of funds, and conducting enhanced ongoing monitoring are reported to be requisite elements of customer due diligence in dealing with both domestic and foreign PEPs. Supplementary guidance is provided by supervisors with varying degrees of detail concerning the practical implementation of these requirements.

65. Larger FIs have higher risk exposure to PEPs given their size and international operations, and utilise commercial lists to screen for PEPs both at the on-boarding stage as well as periodically on existing customers. Some notaries are using automated screening tools depending on their nature size and complexity and smaller firms may use batch screening practises to check whether customers could be PEPs. Some real estate sector participants rely upon outsourced support to undertake PEP screening. Smaller OEs that do not have automated screening programmes are nevertheless aware of requirements and undertake enhanced measures.

66. Across the regulated sectors, OEs report having both domestic foreign PEP customers, the extent to which was determined based on the scope of the entity's product offering (e.g., those entities with an international business base reported having both domestic and foreign PEPs).

67. Trust and corporate service providers, banks and trust offices demonstrate a strong awareness of the risks associated with PEPs and the misuse of complex corporate structures and arrangements to launder the proceeds of bribery and corruption.

68. Obliged entities dealing with high net-worth customers and private banking lines of business report continuing challenges when trying to obtain information concerning a PEP's source of wealth. Others report difficulties in establishing source of wealth for PEPs involved with the operation of state-owned entities. Guidance across the different supervisors was not always seen by OEs as helpful in clarifying how these requirements should be fulfilled.

69. Some of the banks interviewed noted continuing challenges with aligning transaction monitoring alerts and PEPs within their customer base. Banks are asked in the Annual Questionnaire to confirm their use of an alert for PEPs in transaction monitoring rules. Guidance also states that obliged entities should check periodically and in the event of alerts or changes whether an existing customer has subsequently become a PEP.

70. Implementation of Article 8(5)'s requirements with regard to PEPs is inconsistent across obliged entity sectors. Compliance is reviewed only to a limited extent by supervisors, outside of planned on-site examinations. Annual questionnaires generally request figures concerning the number of domestic and foreign PEPs within an obliged entity's customer base, their jurisdictional links and, in some cases, the proportion of product or assets associated with those business relationships. Some deficiencies related to PEP procedures were reported in both the investment sector and payment service providers. These ranged from lack of screening procedures, inaccurate classification of customers (e.g., customers or owners who should have been classified as PEPs, but were not), lack of application of risk-based measures to PEPs, not obtaining senior management approval for establishing relations and not obtaining senior management approval for continuing relations.

71. Where OEs rely upon PEP lists, their verification also to the accuracy of those lists was not subject to regular monitoring and testing. In the banking sector, it was reported that instances have occurred where the PEP list used by a bank was not correct. Some supervisor's guidance reinforces the need to rely upon multiple information sources to identify PEPs. Other guidance makes specific reference to a list maintained on the website of the Tax Office. No specific supervisory guidance or industry-wide feedback has been provided on the selection and oversight over the use of PEP lists.

72. Guidance for some sectors, such as banking, advises OEs that reliance should not be based on lists, alone, to identify PEPs. It advises that the OE should have regard to the customer or owner's political influence and whether it is genuinely comparable to that of similar national positions. In such instances, OEs are expected to consider designating such persons as high-risk. This approach is not reflected across other sectors' guidance on PEPs.

73. As a location which attracts international customers and international business, for business tax reasons, the Netherlands is likely to encounter PEPs on a more frequent basis. This exposes it to the risk that fund flows emanating from bribery or corruption may be layered through the products and services offered by OEs.

Article 21

74. Article 8(6) of the Wwft outlines the requirements in relation to the PEPs who are the beneficiary or one of the beneficiaries of a life insurance policy. It requires that appropriate measures be taken to determine whether a beneficiary is a PEP no later than at the time the insurance policy is paid out or is transferred in part of in full. A senior member of management must be informed of payment and the entire business relationship with the policy holder must be subject to increased monitoring.

75. Supervisors stated that life insurance companies comply with the respective provisions of the Wwft Article 8(6). Where non-compliance has been identified, action has been taken to ensure that this is remediated. The DNB, for example, conducted two AML/CFT investigations at two life insurance companies in 2019 . Both obliged entities were found to not fully comply the requirements of Article 8(6) and were required to undertake remediation to resolve this.

Article 22

76. Article 8(7) of the Wwft requires that if the customer or the beneficial owner no longer serves in a prominent public function, obliged entities must perform appropriate risk-based measures for as long as is necessary, but at least for a period of 12 months, until the increased risk associated with politically exposed persons no longer applies to the PEP. If, during the business relationship, the customer or the beneficial owner becomes or appears to be a politically exposed person, the institution shall comply with the provisions of Articles (5),(6) (7) and (8) immediately upon this becoming known.

77. Limited data was provided to the assessment team about the ways in which obliged entities undertake the monitoring of PEPs to identify when they cease to hold the relevant position. There is limited guidance issued by the DNB, AFM, BFT or NoVA, clarifying what circumstances may give rise to extending a customer or owner's risk classification beyond the 12-month period. Some of the existing guidance provides indicia of possible risks posed by a former PEP. Annual questionnaires provided to the assessment team to not requests data regarding the number of PEPs reclassified as per Article 8(7) or the process followed in arriving at this decision. Overall focus of supervisory activity appears to be on the initial identification and classification of PEPs, and the enhanced due diligence undertaken. Less focus appears to be placed is placed on understanding how obliged entities link transactional behaviour with PEP customers or owners and how these results inform the reclassification of low risk rated customers.

Article 23

78. Article 8(8) of the Wwft stipulates measures to be applied to "non-core" PEPs, i.e., family members or persons known to be close associates of PEPs, identical to those required for relationships with "core" PEPs. All obliged entities interviewed demonstrated a clear understanding of the requirements related to family members and known close associates.

79. The challenges noted by banks in relation to linking transactions to PEPs also apply with respect to the transactions linked to close associates. The challenges identified by some DNFBPs in determining the ownership for complex structures also affect their ability to accurately identify and classify PEP family members and close associates.

Sub-theme (c): CDD related to performance by third parties

Article 25

80. National provisions allow third party reliance in conformity with the requirements of the 4th AMLD, particularly establishing the ultimate responsibility of obliged entities for meeting CDD requirements whenever they exercise such reliance. Article 10 of the Wwft permits reliance upon third parties by an obliged entity without prejudice to its obligation to comply with the provisions of subsections 3.2(a), (b), (c), (e) and (f). Further clarification is provided in section 5.6 of the General Guidance issued by the Ministry of Finance and Ministry of Justice and Security (last updated July 2020). These also make clear the obligation to have measures in place to ensure the OE has access to and the introducer retains the customer due diligence information upon which reliance is based.

81. The scope of parties on which reliance can be placed are restricted in several ways. For example, reliance can only be placed on OEs either regulated and operating in the Netherlands or another Member State.

82. Most sectors prefer to obtain the KYC directly than replace reliance on an external party.17 Among DNFBPs, both lawyers and notaries confirm some practice of customer acceptance through referrals by reputable EU law firms; however, this is not reported to amount to automatic acceptance of the CDD outcomes from such third parties (i.e., they do their own CDD before client onboarding). Other DNFBPs do not report third party reliance practices, preferring to obtain and retain customer due diligence directly from the customer.

83. Most OEs appear to have elected to forego third party reliance for operational reasons, finding it easier to require the production of customer due diligence information by the customer directly.

Article 26

84. Banks confirm to have strict rules prohibiting reliance on third parties from higher risk countries or offshore jurisdictions, where the only exception is for subsidiaries within the same group applying group-wide policies and procedures. This is supplemented by the DNB Wwft and Sw Guideline which covers both the situation in which third parties are also themselves obliged entities for AML/CFT purposes (cf. Article 5 Wwft), and the situation in which third parties are not themselves obliged entities (cf. Article 10 Wwft). For participants in other sectors, this reliance is not observed, due in large part to a preference to obtain and retain customer due diligence directly. The assessment team did not identify any deficiencies in the practical application of these requirements.

Article 27

85. National provisions outline the requirements for third party reliance related to the obtaining of required customer due diligence information under Article 3 of the Wwft programme. These are supplemented by section 5.6 of the General Guidance issued by the Ministry of Finance and Ministry of Justice and Security (last updated July 2020). The assessment team did not identify any deficiencies in the practical application of these requirements.

Article 28

86. National provisions outline the requirements for third party reliance related to a Group programme. These reflect the requirements stipulated in Article 28. Number of banks and payment service processors will rely on branches, subsidiaries or in the case of PSPs, regional KYC teams to undertake the required KYC and enter it on the system.

87. The model used by payment service providers to conduct customer due diligence, suggests a form of internal group reliance that is likely to appear more frequently as the use of automated onboarding and eKYC technology is used by obliged entities. This model involves the use of a single eKYC process, applied across different jurisdictions, with regional KYC teams completing

[17] It was reported in the Questionnaire submitted to the assessment team that third party reliance requirements do not apply to most obliged entities falling within the supervisory scope of the BTWwft, save for those OEs where outsourcing arrangements are in place.

customer due diligence. This model is used to accommodate specific AML/CFT regulations that apply in the jurisdiction from which a customer is established or operates.

88. The degree to which these arrangements constitute reliance versus outsourcing has not yet been reviewed by the DNB but may warrant further examination to accurately understand the potential AML/CFT risks involved with such arrangements.

Article 29

89. Separate guidance is provided to obliged entities concerning the outsourcing arrangements for completing customer due diligence. The guidance clearly distinguished from third party reliance arrangements. Separate obligations including conducting a risk assessment of the expertise and practical approach of the third party and its compliance with the relevant customer due diligence requirements in the Wwft. This also includes stipulation in writing that the third party will comply with the regulator and where necessary the institutions policy rules and that the firm will periodically verify and ascertain this and if required received reports on it from the outsourcing partner.

Compensatory Measures and Detrimental Factors

90. Amongst the compensatory factors that contribute to effectiveness, the assessment team notes that the Netherlands has a well-established AML/CFT regulatory framework which has included PEP requirements for some time. OEs in the banking and TCSP sector demonstrate a mature understanding of the financial crime risks associated with PEPs. They also have invested time and resources into the development of onboarding processes which facilitate the detection of new customers and owners who may be PEPs. OEs in these sectors report positive interaction with the supervisor and receiving guidance on these topics. Equally, members of the professional sectors also demonstrated a strong awareness of the importance of identifying PEPs at onboarding and undertaking the required due diligence measures in Article 8(5).

Conclusions (customer due diligence)

General CDD

91. The assessment team has identified **major deficiencies** which have a **major impact** on effective implementation of CDD measures, as follows:

    a. Lack of guidance for all OEs who use or seek to use online onboarding processes and other EKYC technology to fulfil customer due diligence requirements under the Wwft.

    b. Limited application by tax advisors, real estate agents, and some investment sector OEs and concerns about the application by payment service providers[18], of the requirement for conducting CDD, particularly regarding the nature and purpose of transactions and expected transactional activity.

92. The assessment team has identified **limited deficiencies** which have **limited impact** on effective implementation, as follows:

[18] In view of the gaps identified in the analysis under this chapter and the limited supervisory engagement with the sector.

a. Need for additional guidance for OEs concerning the conducting of CDD for the identification of beneficial owners involving complex structures.

b. Gaps in implementation guidance affecting all categories of OEs on conducting CDD reviews for existing customer CDD and the required approach for combining time-based and trigger-based reviews.

c. Concerns about the compliance of all payment service providers with existing customer CDD requirements and the application of CDD under simplified due diligence onboarding processes in view of the limited oversight by supervisors.

d. Deficiencies of compliance by the investment sector with enhanced due diligence requirements.

CDD for PEPs

93. The assessment team has identified **limited deficiencies** with **major impact** affecting all categories of obliged entities:

a. Lack of guidance and monitoring of implementation of the requirement to determine whether existing customers required re-classification as a PEP and the linking of alerts or other signals to the existing risk profile of a customer.

b. Lack of guidance on the application of PEP declassification requirement and the limited extent to which obliged entities effectively apply the stated criteria.

94. The assessment team has identified **limited deficiencies** with limited impact as follows:

a. OEs not verifying the accuracy of the lists for the identification and screening of PEPs.

CDD related to performance by third parties

95. The assessment team has identified **limited deficiencies** which have **limited impact** on effective implementation as follows:

a. The application of third-party reliance requirements to payment service providers in light of their onboarding processes and potential risks associated with models used to address regional disparities between the Netherlands and other jurisdictional AML/CFT regulatory requirements requires further review by the competent authority to ascertain any relevant risks.

CHAPTER 4. Application of transparency of beneficial ownership and registration for legal persons (Article 30) and for legal arrangements (Article 31)

Status of Transposition

96. At the time of the analysis of COM, this provision had not yet been implemented; there was a legislative proposal which was before the House of Representatives of the States General. The UBO registration became finally effective on September 27th of 2020. Legal persons founded in the Netherlands and other legal entities need to register information about the UBO within a period of 18 months. Therefore, at the time of the evaluation, the term for submitting the BO information had not yet elapsed.

Analysis of Application in Practice

Sub-theme (a): Transparency of beneficial ownership and registration of legal persons

Article 30

97. Data from LEAs show that in the majority of cases legal entities misused for ML/FT purposes have legal personality, although the data does not show a (relative) prevalence of certain legal persons when it comes to ML/FT, the foundation being the exception. The NRA includes an analysis of the ML risk posed by legal persons incorporated in the Netherlands, focusing also on legal entities that act as directors in companies. The NRA notes that, as regards legal entities incorporated in 2017, out of 39169 legal entities that appear as directors in the incorporation of a legal entity, many held the position of director for less than 30 days; 185 were acting as directors for more than 50 legal entities, and of these only 17 were incorporated in the Netherlands; and in the case of 168 foreign legal entities (acting as directors for legal entities incorporated in the Netherlands) the country of incorporation was unknown19. Authorities were not able to explain the reasons for not knowing countries of incorporation in these cases, but indicated that, in their opinion, they indicate an increased risk of ML. The NRA also notes that complex structures by trust offices can be used to disguise the origin of illegally gained funds.

98. As the deadline for submitting information on the BO to the register had not yet elapsed at the time of the evaluation, it is not possible to provide firm conclusions on its effective implementation, as authorities were not able to indicate what was the share of the legal entities that, at the time of the evaluation, had complied with the requirement, i.e., those legal entities that existed prior to the date of entry of the requirement (September 27, 2020). Legal entities established after that date are required to provide BO information as part of the registration process. The authorities explained that the information submitted is checked for completeness (e.g., the person entering the information the identity of the BO and the required appendixes), and if there appear inconsistencies, the matter is followed-up with a request to the concerned legal entity. In the case of lack of response, additional investigation is undertaken, including by the Economic Enforcement Bureau which can consider imposing an administrative fine (which cannot exceed € 21,750). During the period February-July 2021 there were 275 files opened for investigation; with 106 requests to the concerned legal entities. In 51 cases the investigation concluded that the information provided/entered was correct; however, although in the other 54 cases the investigation concluded that the data provided was incorrect, there were no procedures initiated for issuing fines. In these cases, authorities stated that the data in the register was amended accordingly.

99. It is unclear whether there have been instances in which ascertained violations of the requirements to provide information to the Register have resulted in criminal investigations. The Netherlands has a sophisticated system for performing risks analysis of the data concerning legal persons (including their BOs), named "TRACK" which, by automatically scanning several closed and public sources on a daily basis, looks for any relevant financial or criminal records of directors, and the legal or natural persons in their immediate surroundings. Analysis is both performed upon registration of a new legal entity, as well as on a permanent basis during the life span of legal entity . If TRACK determines there is indeed an enhanced risk, a risk report is issued to an investigative or supervisory body. While there has been a case

[19] See NRA, page 62, box 16.

where through TRACK an investigation into a potential hit of a company link with a UN designated persons was initiated, authorities stated that they were not aware of other criminal investigations triggered through TRACK.

100. Users of the BO register (including the register for legal persons), and particularly OEs and competent authorities, are one of the primary sources of information for identifying inconsistencies with the registered data. Although no exact figures could be provided, authorities stated that (for data concerning the legal persons) thousands of reports of inconsistencies are received every year. Authorities stated that in many cases these inconsistencies are proven to be unfounded, and that the data is actually correct. However, OEs interviewed stated that in their experience the information on the register is not always accurate or current, and that they had reported such inconsistencies to the Register. While these inconsistencies refer primarily to data on legal persons (which is out of the scope of the present chapter) and not on the BO, since the register is still being populated, this could raise some concerns about the accuracy of the data being held on legal entities.

101. The beneficial owner data is accessible publicly for a fee of EUR 2,50. The accessible data to OEs is only limited to the name, month and year of birth, state of residence and nationality, as well as the nature of the economic interest held by the ultimate beneficial owner and the extent of that interest, albeit only indicated in "bandwidths". This means that OEs do not have access to identifiers such as the date of birth, the place of birth, the country of birth and the address of residence. The FIU and other competent authorities have unrestricted access to all BO information held in the Register, without having to alert the persons concerned. There are no issues with the timeliness of access to the information by competent authorities or the FIU.

102. OEs interviewed by the assessment team stated that they use the basic and BO information in the ER for performing their due diligence requirements, but they were aware that they should not rely exclusively on the BO information for fulfilling their requirements, also considering the issues noted in regard to accuracy of the data and inconsistencies.

Sub-theme (b): Transparency of beneficial ownership and registration of legal arrangements

Article 31

103. Article 31 has not been transposed yet. A legislative proposal that envisages the creation of a register for BO information related to trusts is currently before Parliament.

104. By way of background Dutch law does not provide for the establishment of legal arrangements such as express trusts or Treuhand. However, certain express trusts established under the laws of another country are recognised as the Netherlands has signed and ratified the Hague Convention on the Law Applicable to Trusts and on their Recognition of 28 September 1995. According to the authorities (and confirmed by the OES interviewed) there are however no indications that a substantial number of express trusts are active in the Netherlands.

105. There is one Dutch legal arrangement that shares some similarities with a trust, in the sense that it is a freeform contractual arrangement often used for some form of asset management, with the important distinction that it has transferable participant certificates. This is the mutual fund ('Fonds voor Gemene Rekening'). The mutual fund has two variants: the open fund and the closed fund. There are around 2,800 open mutual funds in the Netherlands.

Compensatory Measures and Detrimental Factors

106. Several detrimental factors impact the beneficial ownership transparency. The beneficial owner data is accessible publicly for a fee, but this is only limited to the name, month and year of birth, state of residence and nationality, as well as the nature of the economic interest held by the ultimate beneficial owner and the extent of that interest, albeit only indicated in "bandwidths" (detrimental factor). Contrary to the 4th AMLD, OEs do not have full access to the BO information held in the register. There is not yet a central register on beneficial ownership information regarding trusts (detrimental factor).

Conclusions (transparency of beneficial ownership)

107. The assessment team has identified **major deficiencies** in the practical application of the transparency of beneficial ownership having a **major impact** by affecting the reliability of the register and availability of accurate beneficial ownership information for legal persons as follows:

    a. The implementation of the BO Register is still ongoing.

    b. Some concerns about the accuracy of the data held in the central register for legal persons and limitations in the scope of information available to the OEs impact the effectiveness of the implementation.

108. The assessment team has identified **major deficiencies** having a **limited impact** concerning the effective implementation of the Directive's provisions on the transparency of beneficial ownership concerning legal arrangements, as follows:

    a. No requirements in place concerning the BO register for trusts.

CHAPTER 5. Functioning of the FIU (Article 32)

Status of Transposition

109. The transposition analysis of COM notes conformity issues regarding access rights of the FIU to information (Article 32 (4)), as there is no provision in the domestic legislation, among those that establish the powers of the FIU, which creates the power of the FIU to request information from other public authorities. Further transposition issues are noted in relation to Article 32 (5), as the circumstances that relieve the FIU from the requirement to provide information in the cases stipulated by Article 32 (4) are not reflected in the national provision – which summarises them as "important interest". As regards the power of the FIU to take urgent action where there is a suspicion that a transaction is related to money laundering or terrorist financing, to suspend or withhold consent to a transaction that is proceeding, in order to analyse the transaction, confirm the suspicion and disseminate the results of the analysis to the competent authorities (Article 32 (7): this article is not considered transposed as this power cannot be used in the case of information/request received from a financial intelligence unit of another Member State. More in general on the power of the FIU to suspend a transaction, the analysis of COM notes that this can only be achieved through a request (by the FIU) to the public prosecutor. However, the Directive does not contemplate an "indirect" attribution of this power. Moreover, the answer provided by the Dutch authorities on the implementation of this provision makes reference to Articles 94 and 94a of the code of criminal procedure, which empower the public prosecutor to seize assets, and to the requirement of OEs to report directly

to the Police (and not to the FIU) when they have suspicions or knowledge of ML or FT. Considering that the power to seize is not the same as the power to suspend a transaction, and that this power should be vested directly in the FIU (and not in another competent authority), it is doubtful that this provision of the Directive can be actually considered transposed. It should be noted that the Council of Europe thematic monitoring review on Art. 14 – postponement of suspicious transactions – concluded that the legislative system in itself is in order20. Currently the Netherlands is working on draft legislation which will provide the FIU-NL with the power to postpone suspicious transactions directly.21

110. Although the conformity issues noted above do not appear to have a very significant impact in the implementation (see Section on compensatory measures and detrimental factors), it should be noted that the existence of a requirement to report suspicions of ML/FT to the Police, and the performance of the analysis of STR also by the Anti-Money Laundering Centre (AMLC), established within the FIOD seriously affects the conformity of this Article's provision requiring that the FIU be a "central national unit" for receiving and analysing STRs.

Analysis of Application in Practice

Article 32

111. The FIU of the Netherlands (hereinafter: FIU-NL) is placed in the Dutch Police. The Minister of Justice and Security is politically responsible for the overall management, organisation and administration of the FIU-NL. In addition, the Minister of Justice and Security and the Minister of Finance share a policy-management responsibility, as they set the budget for the FIU-NL.

112. The FIU-NL is established by the AML/CFT law, which sets its powers. Additional institutional and operational provisions are established in a 2013 FIU Institutional Decree. This decree establishes the independence of the FIU head (not of the institution), with regard to: i) declaration of unusual transactions to be suspicious; ii) phrasing and implementing policy and its innovation; iii) issuing binding instructions to obliged entities with respect to the unusual transactions reported; iv) deciding on participation in relevant national and international meetings relating to the FIU-the Netherlands; v) negotiating on and concluding MoUs and agreements with foreign FIUs or other relevant partners; vi) directly advising and informing the Ministries involved in the FIU-the Netherlands. The decree also states that the head of the FIU-NL shall independently decide on the use of the financial resources granted to the FIU.

113. For other operational aspects, the FIU operates under a mandate given to the head of the FIU by the Minister of Justice and Security to the Head of FIU-NL, whereas managerial and organisational decisions are delegated by the Minister of Justice and Security to the Chief Constable of the Netherlands Police with a mandate (that can be revoked at all times) and subsequently delegated to the Head of FIU-NL with a sub-mandate, for the daily management of the FIU-NL.

114. The AML/CFT law (Article 21) establishes also a Committee on the duty to report unusual transactions, tasked to hold periodic consultations with the Minister of Justice and the Minister of Finance in respect of (proposed) legislation and policy plans that relate to the organisation and performance of the obligation to report UTRs and the objective indicators for establishing whether a transaction is unusual. Members of the Committee also discuss AML/CFT issues

[20] https://rm.coe.int/c198-cop-2019-1rev-hr-ii-art14-en/1680a12458

[21] It is noted that the section on the status of transposition of the 4th AMLD is entirely based on the 2019 COM analysis.

more broadly and the obliged entities can point out where they face issues implementing policy and how to overcome them. In their written submissions, the authorities stated that the Committee "has a kind of overview or is a mechanism that has an indirect influence on the functioning of FIU-NL".

115. This institutional arrangement concerning the FIU-NL presents a certain degree of convolution and has a number of issues that could potentially affect the operational independence of the FIU-NL. First, the independence of the FIU is not enshrined in a law, but only in a decree, and referred to the head of the FIU and not the institution. Second, there are no rules establishing under what circumstances the head of the FIU can be removed. Third, the operational independence of the FIU is actually implemented only indirectly through a sub-mandate, which can be revoked at any time (as can the mandate), without any indication of the circumstances that could entitle the Minister or the Chief of Police to revoke the mandate/sub-mandate.

116. The evaluation team has no concrete evidence to conclude firmly that these potential issues affect in practice the operational independence of the FIU-NL. However, the opportunity of positioning of the FIU and related implication for its operational independence have been publicly debated in the Netherlands22, as has the risk arising from the fact that staff assigned to the FIU combine the responsibilities of both FIU and Police staff (the majority of staff of the FIU is seconded from the Police, being seconded at 75% to the FIU), particularly regarding the processing of Police data by personnel of the FIU-NL with regard to the (lack of) clarity for which purpose and on which legal grounds Police data could be processed by personnel of the FIU-NL. This issue was addressed in 2019 with the adoption of a series of "in control measures", aimed at distinguishing the roles between requesting and providing Police information for the execution of FIU tasks. This was followed by an audit commissioned by the Minister of Justice and Securities, which has assessed these measures and made further recommendations for improvement, as well as by a study and consultation with other stakeholders on the positioning of the FIU, which concludes that the current positioning of the FIU-NL within the Police is the best option.

117. In the period under review the FIU staff has steadily increased, reaching the current organigram of 90 staff (actual number of staff: 85). In April 2021 an external high-performance data-team has been contracted to support FIU the Netherlands on the roadmap to a more data-driven organization. Together with FIU-analysts and FIU-investigators, this high- performance data-team is expected to create products and reports that will be disseminated to law enforcement and other relevant stakeholders.

118. The FIU's responsibility of receiving, analysing, and disseminating financial intelligence to combat ML and FT activities are overall in accordance with the 4th AMLD. Nevertheless, it should be noted that, in addition to the FIU's analysis of UTRs, the Anti-Money Laundering Centre (AMLC), established within the FIOD, also performs analyses of STRs, which it receives from the FIU with a weekly and a quarterly export with GoAML (the system used by the FIU to receive and store UTRs), as well as strategic analysis for the identification of ML trends and typologies. Thus, there appear to be two institutions in charge of performing analysis of ML-related information.

119. UTRs are received electronically and processed through GoAML, which has very limited functionality for automatic screening and automatic prioritization of the incoming information,

[22] Letter of the Minister of Justice and Security to Parliament of March 23, 2021: Capaciteit en uitkomsten verkenning positionering Financial Intelligence Unit-Nederland | Tweede Kamer der Staten-Generaal

which is not ideal in an environment characterized by a very large number of incoming information (more than 700.000 UTRs in 2020, doubled from 2015). However, the FIU-NL has developed an in-house, manual, prioritization system for operational analysis based on themes and queries of its database and other databases it has access to. The prioritization is based on the highest risks with a residual potential impact, as identified by the NRA (e.g., corruption, human trafficking, drug trafficking, cryptocurrency, trade-based ML etc) and on the priorities of the prosecution and investigative services.

120. The main goal of the operational analysis is to declare UTRs "suspicious". This is done according to four baselines. The first baseline is that the UTRs are matched with the database of the investigative services and the Central Judicial Collection Agency (CJIB). The second baseline entails the analysis based on priority themes, described above. The third baseline to declare transactions as suspicious is by targeted information requests from the investigative services via an LOvJ-request. These requests may be submitted for the purpose of criminal investigations or confiscation of unlawfully acquired assets. In the case of a LOvJ-request, the FIU-NL conducts a detailed investigation in its database. The fourth baseline to declare transactions suspicious is by exchanging information with foreign FIUs.

121. Although the legal framework governing the responsibilities of the FIU does not distinguish between operational and strategic analysis, since the end of 2019 the FIU-NL enlists a team of five strategic analysts and a data scientist who are responsible for the execution of strategic, cross-file analyses, focusing on identifying phenomena and trends, thematic research, analysis, refinement but also restructuring large amounts of data. Although authorities indicated in their written submissions examples of such analyses (e.g. COVID-19 fraud conduct by FIU-NL strategic analysts) and stated that strategic analysis supports operational analysis through the themes described above as well as the exchange of information through various platforms (see analysis under article 49), they seemed more ML-related than FT; and during the interview the FIU was not able to articulate more comprehensively on the strategic analysis "outputs" it has produced.

122. As noted by the analysis of COM, the FIU-NL is not given by the AML/CFT law the power to request information from other public authorities. While this is a significant issue of consistency with the Directive, its relevance in practice is reduced by the fact that the FIU has direct access to other authorities' databases (e.g., land registry and company registry data, including data on BO) by other cases in which the information can be accessed otherwise (e.g., Police data or fiscal information within iCOV, where a specific covenant exist that allows the exchange of information among participating institutions). However, in the absence of an enabling provision, and considering how strict are privacy laws in the Netherlands, there could be some instances where the FIU may not have access to other types of information (e.g., specific tax records, or the register of bank accounts) that it may need to properly undertake its functions, including strategic analysis. For example, Article 25 of the Wwft refers only to access of the FIU to facts that may indicate money laundering or terrorist financing discovered by the respective supervisory authority (and no other information generally maintained and monitored by the supervisors, etc.). The DNB confirmed that it does not have the legal basis to provide information at the request of the FIU (although the FIU provides information on a quarterly basis on reporting trends of OEs falling under the purview of the various supervisory authorities). It is also unclear if and how the FIU has access to and whether it is processing for AML/CFT purposes information related to cross-border declarations of cash (no case concerning this information has ever been transformed into a STR, according to the information provided by the FIU).

123. The FIU has the power to request further information from OEs to perform its analysis function, regardless as to whether they have submitted an UTR, which was confirmed during the interviews with OEs. However, the lawyers interviewed by the evaluation team expressed different views on whether the AML/CFT law can indeed prevail over their confidentiality requirements. The FIU ensures that all data it generates or receives from obliged entities and foreign FIU is kept confidential and secured through its own IT system.

124. Once an UTR has been declared an STR, the information is uploaded into a data warehouse of law enforcement, which is directly accessible by law enforcement and can be used on an "as needed" basis. The authorities stated that the goal for 2021 is to improve the quantity and quality of the disseminated suspicious transactions by adding extra contextual information to it (attachments, type of criminality, etcetera). This will help law enforcement in a better understanding of the financial intelligence that is produced by FIU-NL.

125. The evaluation team is not in a position to firmly conclude to what extent the outputs of the operational analysis of the FIU-NL contributes to the repression of ML/FT activities. The FIU was not able to provide statistics to demonstrate what is the share of these STRs that actually have contributed either to the starting of a new or to supporting an existing criminal investigation of ML or other types of predicate offences, nor was it able to indicate data on seizure of assets by the prosecutor (the FIU has not the power to suspend the execution of transaction) resulting from a request of the FIU, or by disseminated UTRs. The FIU does not maintain statistics differentiating ML and FT UTR analysis. In response to a question asked by a Parliamentarian the Minister of Finance explained that "it is not possible to indicate how often a report of an unusual transaction that is declared suspicious by FIU-the Netherlands ultimately leads to a specific investigation or conviction. However, the investigative services are becoming increasingly adept at indicating, by means of analyses of their data, how suspicious transactions are used in criminal investigations. Based on a recent analysis by the Anti Money Laundering Centre (AMLC) has shown that over the past five years an average of 60% of FIOD investigations have been linked to suspicious transactions. A recent random sample from the Public Prosecution Service also shows that of all the signals submitted to the Money Laundering Signals Consultation - a national consultative body in which signals are consultation in which signals are weighed up for the purpose of detection - in a period of three months in 2021, 57% of these signals concerned suspicious transactions by FIU-the Netherlands"23 Examples of cases were provided that show that investigators use the financial intelligence provided by the FIU; however, the evaluation team has strong concerns about the lack of feedback (enshrined in the AML/CFT law) from law enforcement authorities and the public prosecution office on the follow-up of disseminated UTRs, which seriously calls into question also the effective implementation of paragraph 6 of Article 32 of the Directive.

126. In recent years, the absence of its own postponement authority with regard to requests from a foreign FIU has been overcome by requesting permission to forward the information to the police and judicial authorities. In accordance with agreements already made with the investigation services and the Public Prosecution Service, a Dutch investigation into fraud / money laundering was opened in cases of a foreign FIU request, after which a classic seizure

[23] Detail 2021D47223 | Tweede Kamer der Staten-Generaal (answer to question 3).

took place. A condition of this method was that there had to be sufficient suspicion to be able to open an investigation and carry out the seizure.

Compensatory Measures and Detrimental Factors

127. Issues of conformity of transposition regarding the power of the FIU to access information are only in part compensated by the fact that the FIU-NL has online and direct access to a number of databases, although not all the information that the FIU-NL may need to properly perform its analytical functions may be available in the absence of a legal provision enabling the FIU to request that information. Issues of conformity related to the lack of the power of the FIU to take urgent action where there is a suspicion that a transaction is related to ML or FT, to suspend or withhold consent to a transaction that is proceeding, are only in part compensated by the practice to request the Public Prosecution to seize the assets, although a seizure is not the same as a suspension, as it requires a higher prima facie evidence.

128. On the other hand, the existence of a requirement to report STRs to the Police (and not to the FIU, which is only informed) and the fact that also another institution performs both operational and strategic analysis of ML-related information seriously affects the implementation of the Directive's requirement that the FIU shall be a "central national unit" for receiving and analysing STRs (detrimental factor); there is also no systematic feedback by law enforcement to the FIU on the information disseminated by the FIU (detrimental factor).

Conclusions (functioning of the FIU)

129. The assessment team has identified **major deficiencies** in the implementation of the respective theme with **limited impact** on overall effectiveness as follows:

    a. The existence of a requirement to report suspicious transactions to the Police under certain circumstances, and the fact that also another authority, in addition to the FIU, performs analysis of STRs (combined as well with the lack of proper feedback to the FIU by LEAs) affect the effective implementation of the FIUs core functions.

    b. Issues that can potentially affect the operational independence of the FIU.

    c. It is not fully demonstrated that the UTR system and the FIU analysis contribute systematically to the prevention and repression of ML and particularly of FT.

    d. The FIU has no power to request additional information to other competent authorities when such information is not directly accessible to the FIU (which is still subject to certain limitations).

    e. Systematic lack of feedback by law enforcement authorities on STRs disseminated by the FIU.

CHAPTER 6. Suspicious transaction reporting (Articles 33-36 and 46.2)

Status of Transposition

130. The analysis of COM does not note any issues of transposition or conformity with regard to these articles.

Analysis of Application in Practice

Articles 33 - 35

131. The scope of the reporting requirement in the Netherlands refers to unusual (and not suspicious) transactions. OEs are required by the AML/CFT law to report to the FIU unusual transaction reports (UTRs) on the basis of indicators established by an "order in council" (the annex to the implementing decree of the AML/CFT law). These indicators are objective (i.e., a match with the indicator requires an automatic reporting of the transaction) as well as subjective, (i.e., the transaction is reported when the OE has reason to suspect that the transaction may be related to ML or FT). It should also be noted that both the AMLD conformity analysis and the 2011 MER refer to an additional and autonomous reporting requirement, envisaged by articles the Criminal Procedure Code (CPC), according to which if an institution knows or suspects that a transaction relates to ML or FT it must report the matter to the police (it must also inform the Dutch FIU that the matter has been reported to the police). Authorities explained that this is a general requirement to report a crime, although the provision they quoted to support this (art. 161 of the CPC) makes no reference to the requirement to inform the FIU in such cases.

132. The indicators are tailor-made to the different types of OEs and the objective ones include also the reporting of transactions where certain thresholds are met. This could explain the very high number of UTRs sent by certain types of OEs: e.g., the one terrestrial casino reported 4629 and 5268 in 2018 and 2019, respectively, which seem excessively high for one institution, even considering that that casino has 14 establishments; however, they could also be an indication of ineffective/defensive reporting (see statistics further down). There are no indicators specifically focusing on FT, which is of concern given the FT risk of the Netherlands. As the FIU-NL does not maintain statistics broken down per ML/FT, it is not possible to assess whether the number of FT-related UTRs is consistent with the country's risk profile. The FIU-NL could not also indicate the number of ML (or FT) criminal investigations triggered by UTRs that have been confirmed into STRs, which makes it quite difficult to determine to what extent analysed UTRs contribute to new or existing criminal investigations.

133. When it comes to ML, the scope of the subjective indicator is narrower than the scope of the reporting obligation as envisaged by the Directive, which is suspicion or knowledge that the funds are "the proceeds of a criminal activity". This narrower scope could (partially) explain the reason why, according to the statistics provided by the authorities the number of subjective UTRs is much lower, across all types of OEs, than the number of objective UTRs. For example, in 2019 the number of UTRs filed by the banking sector on the basis of subjective indicator was about 50.000, against about 250.000 reports filed on objective indicators, although sectoral guidelines (e.g., the DNB) stress that the emphasis in the detection of transactions should be more on subjective indicators. The ratio is much higher for other types of FIs, e.g., PSPs.

134. In the period under review the UTRs that are reported on a "subjective" basis decreased when compared to UTRs reported on an "objective basis" (although certain objective reasons for the very strong decrease of the subjective reporting in 2018-2019 are noted):

Reported Unusual Transactions (UTRs) per type of indicator per year the transactions were registered at the FIU-NL (2015-2020), excluding BES-reports **Year registered**

Type indicator	2015	2016	2017	2018[13]	2019[14]	2020	Total
Objective	22%	20%	32%	87%	70%	43%	46%
Subjective	78%	80%	68%	13%	30%	57%	54%

Total	100%	100%	100%	100%	100%	100%	100%

135. If compared with the share of UTRs that are declared suspicious by the FIU, the majority of those are related to UTRs reported on a subjective basis, which could call into question the effectiveness of the objective-based UTRs:

Suspicious Transactions (STRs) per type of indicator per year the transactions were declared suspicious (2015-2020), excluding BES-reports **Reporting year**

Type indicator	2015	2016	2017	2018	2019	2020	Total
Objective	17%	14%	13%	10%	15%	9%	13%
Subjective	83%	86%	87%	90%	85%	91%	87%
Total	100%	100%	100%	100%	100%	100%	100%

136. Finally, when comparing the number of UTRs received per year with those that are "declared" STRs the number of transactions declared suspicious appear rather low. This could call into question the effectiveness of the UTR system in general; this concern was also shared by some of the OEs interviewed and during the inspections by the DNB of the banking sector (see further down – observation of the DNB on the quality of reporting, awareness of the procedure and confusion, especially for foreign banks).

Number of unusual transaction reports received by FIU-NL (2015-2020) **Year**	**2015**	**2016**	**2017**	**2018***	**2019***	**2020**
UTRs	312,160	417,067	361,015	394,743	541,236	722,247

UTRs declared STRs	2018		2019		2020	
	STRs	Files	STRs	Files	STRs	Files
Total	*57,950*	*8,514*	*39,544*	*5,302*	*103,947*	*19,114*

137. The assessment team has strong reservations about the UTR system and the automatic reporting of transactions based on objective indicators and without an actual assessment of the suspiciousness of the transaction, particularly given the poor results in terms of these transactions' generating actual STRs in the analysis of the FIU.

138. The banking sector accounts for the majority of the UTRs filed, although according to information provided the majority of the reports are made by a limited number of banks. The large banks account for the largest number of reports, which can be explained by their position in the Dutch market. As regards other types of FIs statistics provided by the AFM show an increasing steady trend in the reporting of UTRs (including those subjective based), while the UTRs sent by the insurance sector (DNB) is rather low, which may be consistent with the lower AML/CFT risk of the insurance sector. Among DNFBPs the highest numbers of UTRs (in addition to the terrestrial casino noted earlier) are filed by i) other persons trading in goods; ii), auditors, external accountants and tax advisors and iii) notaries, with TCSPs and, particularly, lawyers, on the lower end, which may not be consistent with these sectors' risk profile (36and 68 UTRs reported in 2018 and 2019 respectively).

139. All supervisors check in their inspections that OEs comply with their requirement to identify and report UTRs. However, the statistics provided by the BTWwft show that sanctions applied to the OEs under their purview may not be proportionate or dissuasive: e.g., for real estate agents, an average of 7500 EUR and 15.000 EUR for 2018 and 2019 respectively for notaries, accountants and tax advisors between 2015 and 2020 the BFT has issued fines in the average between 4290 EUR (lowest) and 14235 EUR (highest). In all these cases the fines were issued for AML/CFT violations that included also the reporting requirement (in addition to other violations); authorities explained that in determining the fine they need to take into consideration the turnover of the OE, which could explain why in certain cases the sanctions could appear low.

140. The DNB has observed that banks are generally aware of the obligation to report unusual transactions to the FIU-NL, although the quality of the reporting processes and procedures as well as the necessary knowledge varies from one institution to another, and that the scope of the reporting – unusual, rather than suspicious "leads to confusion, especially for foreign banks with an independent establishment or branch in the Netherlands, because they often rely on the policies and procedures of the (foreign) parent." Another observation made by DNB is that a number of banks are not always acutely aware that not only transactions should be reported, but also intended transactions. According to the statistics provided by the FIU, the total number of UTRs related to attempted transactions filed by all OEs is 21644, 23949 and 17530 for 2018, 2019 and 2020 respectively. It was not possible to obtain statistics on the number of STRs arising from the inability of the OE to conduct CDD; the FIU explained that OEs use a free-text field while reporting a transaction, and that they do not report and describe this in a uniform way. The inspections of the DNB have also shown that (in the past) there was still room for improvement in the quality of the transaction monitoring systems and the assessment of the alerts (especially when having to apply the subjective indicator) generated by these systems, which underpin the FIU-NL reports, and has followed up with the concerned banks, including

by providing specific guidance, which has resulted in the banks' improvement of their (post) transaction monitoring systems and processes.

141. According to the DNB, based on signals from the banking sector, the quality of FIU-NL reports could be further improved by ensuring more systematic feedback on transactions reported to FIU-NL (both those that are identified as suspicious and those that are not). Banks have informed DNB that they find there is little effect visible from the reports made to the FIU, linking this to their transaction monitoring efforts. Issues of quality of UTRs were also noted by the AFM as the result of their 2019 thematic inspection of TM and Mandatory Reporting 2019, which showed that the quality of the reported unusual transactions can be improved and that, in particular, it is not always clear why the reporter believes the transaction or transaction pattern to be unusual.

142. In general, OEs interviewed by the assessment team had a good understanding of the STRs requirements and were aware of how to report to the FIU. Some DNFBPs observed, however, that the system used for reporting is not user-friendly and can be very time consuming. Authorities have explained that the FIU has modified the reporting tools to make them more user-friendly and less time consuming.

143. The banks and large FIs that were interviewed appear to have good knowledge of the policies and procedures to prevent, detect and report suspicious transactions, including through risk assessment and customer acceptance policies, complemented by transaction monitoring systems (with both rule-based and scenario based systems to identify suspicious transactions, and a combination of real time and post event monitoring), with procedures for internal escalation and analysis of suspicious transactions prior to their reporting. However, some banks reported that FT risks indicators and scenarios are not very specific and difficult to embed in their transaction monitoring systems.

144. Lawyers have legal professional privilege and confidentiality on the information communicated by a client. Compared to other types of OEs, which had no issues in providing additional information to the FIU-NL upon their requests, lawyers interviewed by the assessment team exhibited a more mixed understanding of this requirement. They were in general aware of the power of the FIU to request additional information and of their obligation to provide it, although they did not express the same views as to whether the AML/CFT law would indeed prevail over legal privilege in the case of a request of the FIU related to a UTR that was not filed by a lawyer. They stated that in these cases they would seek the opinion of the dean, which could amount to potential tipping off.

Article 36

145. Most STRs from supervisors are received from DNFBP supervisors. As regards banks there was one case in 2019 and 3 cases concerning PSPs between 2018-2020. Information and materials provided by the authorities demonstrate that supervisors check in their inspections if OES are complying with the STR requirements. However, when a transaction is deemed to be unusual and subject to reporting supervisors, the DNB requires the FI itself to report the transactions, if applicable through informal or formal measures. This seems also the practice of other supervisors (e.g., the supervisor of lawyers).

Article 46.2

146. The supervisory authorities (through guidelines and direct engagement with the firms) and the FIU (by way of bilateral meetings with more material and riskier banks) made considerable efforts to improve the quality of STRs, although it is not possible to conclude that the system is more effective (based on the analysis of data).

147. The FIU-NL provides feedback to the OE when a UTR is transformed into an STRs. As noted by the DNB in their engagements with the banks, they indicate that only a fraction of the reports is deemed to be suspicious by the FIU, while no feedback at all is received concerning the reports not deemed to be suspicious. The interviews with OEs confirmed that feedback, when provided, concerns only the case of a UTR transformed into an STR. No further feedback is provided concerning the opening of investigations (of which the FIU is unaware).

Compensatory Measures and Detrimental Factors

148. The existence of an additional reporting requirement (apart from the FIU) ; the narrower scope of the subjective indicators and, in the case of lawyers, potential issues related to attorney/client privilege may hamper the effectiveness of the reporting obligation (detrimental factor).

Conclusions (suspicious transaction reporting)

149. The assessment team has identified **major deficiencies** with regard to the reporting of STRs with **major impact** on overall effectiveness:

    a. Narrower scope of the subjective indicators and near absence of FT specific indicators.

    b. Issues of effectiveness of the objective UTR reporting system, as well as issues of quality of reported UTRs (decreasing trend for subjective STRs, low ratio between UTRs submitted and those declared STRs).

    c. Limited reporting by some types of DNFBPs (notaries, TCSPs and lawyers).

    d. Limited feedback provided by the FIU and concerns about the timeliness of feedback.

CHAPTER 7. Application of arrangements in terms of data protection and record-retention (Article 40 with AML/CFT relevance)

Status of transposition

150. In terms of completeness, the transposition analysis of COM does not note any issue.

151. The COM assessment indicates a conformity issue concerning Article 40(1)(b) of the Directive on retaining documents and information related to the obligation to keep the data only for the required period relative to the filing of the transaction to the FIU, unlike the Directive which imposes the obligation relative to the end of the relationship or the date of the occasional transaction.

Analysis of Application in Practice

152. Some DNFBPs, particularly those from the professional sectors, expressed difficulties in resolving the conflict that was apparent between minimum retention requirements under

Article 33 of the Wwft, destruction requirements under Article 34a(3) and specific rules of their profession which required the retention of certain documents for a longer period (e.g. tax advisors need to retain certain documents for a period of 10 years; notaries may require to retain certain records for a longer period). There was therefore uncertainty around the content of the notice required to be given to customers about the use of their personal data under 34a(2) of Wwft.

153. Most obliged entities expressed the view that little or no guidance had been provided by their supervisors on how to fulfil the requirements of Article 34a of Wwft. Guidance currently available comprises mainly of a summary of the Article's requirements, the data to be retained pursuant to Article 33 of Wwft and confirmation that obliged entities can retain a copy of an individual's identification document. No further information is provided as to how obliged entities are to determine, for example, whether the scope of customer due diligence collected, meets the requirements of Article 34a(1) of Wwft and the measures expected to ensure its requirements are complied with. Some obliged entities are currently using or planning to use automated onboarding processes, artificial intelligence data lakes and cloud storage and other forms of technology which may involve the processing of personal information. No guidance has been provided, either during examinations or published on supervisor websites, on how these technologies should be configured to ensure compliance with Article 34a.

154. Some guidance is provided in the General Guidance on the Money Laundering and Terrorist Financing [Prevention] Act Wwft published by the Ministry of Finance and Ministry of Justice and Security (updated as a 21 July 2020). It explains that the principle of data minimisation means that data not mentioned under article 33(2) or in section 5.2.6 of this guidance may, in principle, not be processed. If an obliged entity wishes to record more data, it must be able to justify why it is necessary to carry out proper and complete customer due diligence. However, almost none of the obliged entities identified this guidance as assistive in understanding how they are expected to comply with the requirements of Article 34a. None of the questionnaires sent by supervisors to obliged entities request information to understand the scope of their compliance with Article 34a.

Article 40

Compensatory Measures and Detrimental Factors

155. Among the compensatory measures that contribute to effectiveness, the assessment team notes the appropriate practices by obliged entities to ensure that policies and procedures are in place for data retention in compliance with Article 33, and that there is a general awareness that personal information collected should only be used for the purpose of preventing money laundering and terrorist financing. Some obliged entities have pro-actively engaged with the Netherlands data protection office to better understand their obligations related to the scope of information they may process and how customers should be notified of their processing activities. The Ministry of Finance and Ministry of Justice and Security endeavours to clarify that Article 34a(1) Wwft is not to be treated as a blanket exemption for all data collected.

156. Obliged entities may be collecting or continuing to retain data under the misguided belief that, in needing to perform customer due diligence or ongoing monitoring, all personal data collected falls within Article 34a(1) of the Wwft and that no further measures are required. This risk of non-compliance is potentially compounded by the increasing use by obliged entities of technology that may lead to the processing of personal information beyond the parameters of Article 34a(1) of the Wwft.

Conclusions (data protection and record-retention)

157. The assessment team has identified **limited deficiencies** affecting all categories of obliged entities in relation to the requirements under Article 34a which have a **limited impact** on effective implementation, as follows:

    a. Uncertainty about the notification to be provided to the customers regarding the use and storage of personal data.

    b. Insufficient guidance to ensure the scope and adequacy of the information collected and retained/destroyed under the CDD process, including in the case of newly introduced methods of CDD by certain institutions.

CHAPTER 8. Application of measures for supervision of financial institutions and designated non-financial businesses and professions (Articles 47 and 48) and sanctions (Articles 58 and 59)

Status of Transposition

158. The transposition analysis of COM notes that the following provisions have not been transposed into domestic legislation: i) Article 48(2) of the Directive, on the obligation to ensure that the competent authorities have adequate powers (as there is no specific provision on the technical means and financial provisions transposed); ii) Article 59(1)(c) of the Directive, on Member States' obligation to ensure that the administrative sanctions and measures under Article 59 apply with respect to record-keeping and iii) Article 59(2)(b) and (e) of the Directive, on administrative sanctions and measures including an order requiring the natural or legal person to cease the conduct and to desist from repetition of that conduct and maximum administrative pecuniary sanctions of at least twice the amount of the benefit derived from the breach where that benefit can be determined, or at least EUR 1 000 000.

Analysis of Application in Practice

Sub-theme (a): Supervision of financial institutions and designated non-financial businesses and professions

Article 47

159. New market entrants who are banks, (re)insurers, clearing institutions, general pension funds, premium pension institutions, trust offices, payment service providers (including money transfer offices, MTOs), currency exchange offices and EMIs in the Netherlands may only start performing activities from the moment a licence is granted by DNB or the ECB, unless a legal exemption to the licence requirement applies. Fit and proper requirements exist for Directors and for persons who take up key positions which must be satisfied as part of market entry. In the case of banks, credit unions and insurers, individuals who hold a management position directly below the level of the policymakers and whose work activities can substantially affect the institutions' risk profile ("key function holders") are also subject to a propriety and fitness assessment. Any natural person or legal entity that acquires, holds, or expands a qualified holding in an OE must apply for a declaration of no-objection (DNO) from the DNB (or, in case of banks, the ECB) prior to obtaining a qualified holding. A qualified holding is the equivalent of BO or equivalent control, directly or indirectly, amounting to 10% or more in an OE. In the

case of banks, credit unions and insurers, individuals who hold a management position directly below the level of the policymakers and whose work activities can substantially affect the institutions' risk profile ("key function holders") are also subject to a propriety and fitness assessment. A license is not issued until the necessary DNOs have been issued. Where changes take place in the persons or legal entities with a qualified holdings during the licensed status of the OE, a DNO must first be obtained from the DNB. The DNB applies a rigorous and comprehensive process to the market entry process, in general, and the fitness and propriety requirements (which include criminal record checks), in particular. DNB also maintains a public register of OEs it has authorised.

160. The DNB maintains statistics on a cross-sectoral basis of the number of DNOs granted on an annual basis. In 2020, the largest number of DNOs were granted to investment firms followed by payment institutions. The DNO also maintains a public register of OEs it has authorised.

161. The assessment of an individual's fitness and propriety involves consideration of Five categories of records: (i) criminal records, including convictions, out-of-court settlements, (conditional) dismissals, or acquittals or discharge of prosecution, (ii) financial records, including major personal or corporate financial problems and bankruptcies, (iii) supervisory records, including providing incorrect or incomplete information to a supervisor, rejected licence applications, or formal or informal measures imposed, (iv) tax-law records, including personal or corporate negligence penalties imposed by the Tax and Customs Administration, (v) other records, including disciplinary measures or industrial conflicts. In the case of a conviction for insider dealing or forgery of documents, this will automatically result in a negative opinion on an individuals' propriety. The DNB can also take account of other sources of information, on a discretionary basis.

162. Where findings indicate that an individual will not meet the fit and proper criteria, the DNB will inform the applicant of how this impacts the applicant's licence approval. The applicants often decide to withdraw or replace the individual who will not meet the fit and proper criteria prior to receiving a formal negative fit and proper decision from DNB. Changes that occur after a license had been granted to any individuals in positions subject to fit and proper assessment must be notified to the DNB as a condition of the OE's licence or authorisation.

163. The licensing process also involves a thorough consideration of the applicant's understanding of its AML/CFT risks, which includes a detailed assessment of its SIRA, various components of its AML/CFT compliance programme including client acceptance, reporting of transactions, transaction monitoring measures and the applicant's risk appetite. The DNB also assesses the design of the control framework, including the degree to which integrity risks are being addressed in developed internal policies, procedures and measures. The requirement to conduct a SIRA also applies to Dutch branch offices of banks and insurers who have their headquarters elsewhere in the EU.

164. The DNB reports that in nearly 100% of licence applications where the approval process was delayed or rejected for payment service providers, this was due to the lack of quality of the SIRA initially submitted by the applicant. However, most applicants were able to make the required adjustments to their SIRA, leading to them before being granted a licence.

165. The DNB also monitors and receives notifications about new entrants to the jurisdiction through its branch office where its parent or main operations are in another Member State.

166. After receipt of the complete notification package, DNB has two months to prepare its integrity supervision of the branch office in question. A receipt of the complete notification means that DNB has received all information it requires to form an adequate opinion of the new branch office's risk profile. Contrary to cross-border service provision, the activities of a branch office may not start until two months after DNB has confirmed receipt of the full notification, or after it has informed the entity, through its home supervisor, of any additional conditions to be observed in the public interest

167. The DNB supervises MTO payment services agents. It conducts a "landscape scan" twice a year to obtain a view of the number of active MTO payment service agents in the Netherlands. This scan is one of several means employed by the DNB to identify illegal market entrants. The DNB also supervises smaller payment institutions which may be exempt from licensing requirements but must still comply with Wwft requirements. Small payment institutions that only provide payment services in the Netherlands and small EMIs may be exempted from the obligation to be licensed if they meet certain characteristics and conditions. One of the conditions is that the institution's policymakers have no criminal record relating to ML/FT, offences against property or instances of non-compliance with financial supervision legislation that constitute criminal offences. There is therefore no "de facto" exemption applied to these institutions. Institutions that qualify for an exemption are registered with the DNB and may not provide services until registration has taken place. Payment institutions and EMIs issued an exemption must still comply with all the Wwft's requirements, including the completion of a SIRA.

168. The DNB monitors for illegal market activity (i.e. participants operating without the required license or registration). It does this by relying on signals from a variety of sources including OEs, other national supervisors, the Netherlands Police, and the FIU. Additional signals are received during various national cooperation initiatives and meetings. The DNB has also undertaken thematic investigations into illegal operations that have involved crypto service providers and trust offices in 2020-21. The DNB has also undertaken monitors of trust offices, more specifically the clients of the trust offices, after trust offices no longer have a licence. The DNB performed a thematic review in which it identified trust offices who had continued to offer services, despite no longer being authorised to do so. No information on further remediation action was made available to the team.

169. The BFT is responsible for supervising compliance with the Wwft by the civil law notarial profession, accountants, tax advisors, auditors and all persons conducting similar activities in a professional or commercial capacity (e.g. administration offices), as well as legal advisers performing professional activities like those of civil-law notaries or lawyers. The BFT is not directly involved in the market entry of OEs nor undertakes fitness and propriety assessments of individuals involved in the direction, control or ownership of OEs. The BFT relies upon certain professional bodies (see below) to supervise market entry and determine the fitness and propriety of some OEs. This is also due to the fact that relative to the resource is available to the BFT for supervisory purposes, the approximately 48,000 OEs for which it is responsible, cannot be sufficiently supervised by the BFT, alone.

170. Market entry by civil-law notaries is overseen by the Royal Dutch Association of Civil-law Notaries (KNB). All notaries must be a member of the KNB to practice in the profession. The KNB's Admissions Committee is responsible for assessing integrity aspects of an applicant. Criminal background checks are undertaken for the KNB through the Ministry of Justice. An applicant must receive a positive advice by the Committee to become a member of the KNB.

171. The BFT monitors the register of notaries maintained by the KNB and decisions issued by its disciplinary judge in order to identify individuals who may be practicing without being admitted by the KNB. The KNB has implemented a policy which prohibits registered notaries from employing or in another way cooperate with a notary removed from the register in the last 10 years. Notaries discharged from the office by the disciplinary judge are removed from the register. The BFT is not made aware of candidates being considered for admission by the KNB or the results of assessments undertaken, where concerns relevant for AML/CFT purposes were identified. The KNB does not assess, in its review of an applicant notary's business plan, its proposed AML/CFT compliance programme or its level of understanding about the possible financial crime risks to which it could be exposed. However, as part of the admissions process, the Ministry of Justice will contact the BFT and enquire whether it has grounds to object to a proposed notary's appointment. Grounds can include where a candidate may have an adverse history in relation to their compliance with the Wwft. Practicing as a civil-law notary without the requisite approval from the KNB can result in civil or criminal prosecution initiated by the KNB in consultation with the Ministry of Justice.

172. Accountants are required by law to be registered with the Royal Netherlands Institute of Chartered Accountants (NBA), upon successful completion of their study and work placement programmes. The accountant profession is subject to statutory disciplinary law through the Disciplinary Court for Accountants. NBA applicants must provide a certificate of conduct to be eligible for membership. This involves the screening of criminal records related of real estate their directors, and other persons and associated companies. This document is issued by Judicial Agency for Testing, Integrity and Screening (Dienst Justis) under the Judicial Data and Criminal Records Act. In each decision on whether or not to issue a certificate of conduct consideration is given to an individual's previous criminal record. There was no evidence provided to the assessment team whether the NBA undertakes industry monitoring to identify individuals providing accountancy services without first being registered. Individuals who, after being registered, are found out to have a criminal record not voluntarily disclosed at the time of registration, can be removed from the register. This requires that the NBA initiate disciplinary proceedings. The NBA can also refer its members to the Accountancy Division of the Trade and Industry Appeals Tribunal.

173. Tax advisors and administration offices are in general, not subject to a specific registration or licensing requirement. Tax advisors can elect to become a member of the RB (Dutch Register of Tax Advisors). Membership criteria requires that the applicant evidence their good character by ways of a self-declaration. The RB does not undertake independent checks to verify the fitness and propriety of applicants. Tax advisors can also elect to become a member of the NOB (Association of Tax Advisors), which operates in a similar manner to the RB. The NOB is the professional association in the Netherlands for tax advisors with an academic degree. Both Associations reported to the assessment team that they do not pro-actively monitor the fitness and propriety of their members. If an Association receives a signal suggesting such concerns, they are limited to reviewing what is available in open-source information about the member or what they are permitted to obtain under their Association's disciplinary procedures. The NOB can, in the case where a member's fitness and propriety is of concern, elect to end the individual's membership or file a complaint with its disciplinary board. Pursuant to Article 32 C of the Wwft, the BFT may disqualify an offender from holding policy making positions where the nature of the noncompliance is punishable by a fine. The disqualification may be for a duration for a maximum of one year and renewed for one additional year.

174. The BFT undertakes separate enquiries to identify OEs who are not required to be registered with a professional body but who are required to comply with the Wwft. In 2019, the BFT developed a database comprising of all OEs falling within its supervisory remit. The database is subject to regular review and update. It also includes information concerning past investigations undertaken in relation to particular OEs and UTRs reported by OEs. The BFT also regularly reviews the Chamber of Commerce registry to identify legal entities who may appear to be offering these services. The assessment team did not receive information to indicate whether the BFT reviews the fitness and propriety of individuals and entities falling within this group of OEs.

175. The NOvA (The Netherlands Bar) is the professional organisation of the legal profession. Lawyers are required to be members of the NOvA to practice in the Netherlands. Legal candidates are subject to strict admissions criteria which includes the issuing of a Certificate of Good Standing from the Ministry of Justice and Security. This includes an examination of the individual's criminal record. The BOs of every law firm must be lawyers themselves and therefore must satisfy the same eligibility criteria. Lawyers' conduct is subject to extensive rules and requirements, non-compliance with which can result in disciplinary action, ranging from including disbarment from the roll, suspension, and reprimands. When lawyers move to a different judicial district, the Local Bar President must be notified, and their previous disciplinary record is provided to them. The NOvA maintains a list of individuals who are qualified to practice law.

176. Monitoring is undertaken to identify individuals who may be practicing law without having qualified and registered with the NOvA. Complaints appear to be one of the main mechanisms through which the NOvA or Local bar President may become aware of an illegal practicing lawyer or the conduct of a lawyer which calls into question their fitness and propriety.

177. The BTWwft is responsible for supervising a wide range of DNFBPs including high value dealers, domicile providers, real estate sector professionals and art market participants. No specific registration or licensing obligations exist for the DNFBPs within the BTWwft's remit. The BTWwft is not responsible for supervising market entry of the OEs which it supervises. It is also not entrusted within the requirements of the Wwft for formally screening the fitness and propriety of directors and associated persons. Market entry is not contingent upon a review by the BTWwft of their AML/CFT compliance programmes or production of a completed SIRA. As part of its ongoing supervision, the BTW wft monitors open source information and other signals which may call into question the integrity of companies and those responsible for their direction and ownership. These matters may be followed up on as part of broader Wwft-related investigation.

178. The scope of DNFBPs supervised by the BTWwft includes the real estate sector and domicile providers. Neither sector have a professional association, like that of the KNB or the NOvA. The real estate sector has three different organisations in which OEs can become a member. Membership is not mandatory. Applicants must provide a certificate of conduct to be eligible for membership. This involves the screening of criminal records related to real estate directors, and other persons and associated companies. This document is issued by Judicial Agency for Testing, Integrity and Screening (Dienst Justis) under the Judicial Data and Criminal Records Act. In each decision on whether or not to issue a certificate of conduct, consideration is given to an individual's previous criminal record. Attention is devoted to the frequency, timing and severity of offences. Where the conduct concerns a legal person, the Minister can include consideration of criminal offences committed by any of its directors, partners, associated or administrators. The responsible Minister can refuse to issue a certificate in certain

circumstances, in view of the risk to society and the other circumstances of the case. Domicile providers are not required to participate or obtain membership in an Association as a prerequisite to working in the sector (which could assess their fitness and propriety as a condition of membership).

179. The BTWwft undertakes monitoring to identify instances where market participants may be operating without complying with Wwft requirements. This includes monitoring the size and population of DNFBPs using open-source information, signals from the FIU and other stakeholders and review of the Chamber of Commerce Company data. The BTWwft also performs ad-hoc searches on high value dealers, largely following signals from market players and other authorities. The BTWwft estimates that the number of domicile providers is rising.

Article 48 (except for 48.4 and 48.5)

180. The DNB demonstrates strong knowledge of the risks identified in the NRA and, for most OEs, the risks specific to the sector in which they operate. This involves an analysis of data from a variety of sources. The DNB prepares a risk assessment of the OEs it supervises based on several information sources, including the use of a detailed annual questionnaire. The findings of on-site and other supervisory investigations and information obtained from supervisory interaction provide additional input for the risk scoring of an OE. A scoring model is used and a score assigned to each OE. The model contains two scoring sheets: one for inherent integrity risks including ML and FT, and one for the control measures taken by the OE to mitigate the identified inherent integrity risks. The scoring methodology is applied in the same manner across all supervised OEs. The methodology is designed so that OEs receive a final score ranging between 1(low risk) and 4 (High). Based on this scoring, the DNB prepares a risk profile of the different OE sectors and sets out its supervisory plan for the following year. The DNB has assessed that large bank pose the largest risk (score of 4). The DNB reviews the risk profiles of OEs once a year. Scores can be adjusted for an OE where incidents or signals indicate a higher level of risk.

181. Although the DNB asks for information about OE's distribution channels, this is not adequately included as a risk factor that is assessed in determining the risk profile of an OE. Similarly, although the questionnaire completed by payment service providers requests detailed information about certain types of payment methods, the payment methods are not systematically or comprehensively covered as a risk factor to be assessed in determining their risk profile. It was also noted that questionnaires given to most OEs request information concerning the outsourcing of certain AML/CFT compliance functions. Several OEs interviewed have or are planning to rely on different forms of technology to onboard new customers, provide customers with online access to products and services and support AML/CFT compliance controls. This is not included as a risk factor that is assessed in determining the risk profile of an OE.

182. The DNB's current risk methodology is applied across all OEs it supervises. It is unclear how the methodology informs the supervisory process applied by the DNB and, in particular, the specific areas of risk evaluated as being greater in relation to a particular obliged entity (i.e. specific lines of business, geographic reach etc.). Overall, the methodology does not clearly identify the key risk drivers associated with an obliged entity. Moreover, this methodology may not be relevant or may omit material risk factors pertinent to other OE sectors. The questionnaires prepared for the different OE sectors, for example, request information concerning specific aspects of the OE's business, which are most relevant to the sector. However, the risk methodology and assessment criteria are not designed with sufficient

flexibility to accommodate this information. The assessment of payment service providers is one such example.

183. The questionnaire provided to payment service providers, for example, requests a breakdown of 7-8 types of payment types that are processed, from the 150 different types of payment methods that can be supported by at least one licensed service provider. Several licensed payment service providers relying upon online onboarding of customers have rated the majority of their customers as low risk. In the case of one large payment service provider, KYC activities are highly automated with reliance often placed on staff located in different jurisdictions to provide necessary enhanced due diligence support. The volume of UTRs submitted, according to the assessment team interviews, are in the "tens of thousands". The payment services sector has seen a notable growth in the Netherlands, with 64 providers currently licensed and some banking institutions might be predominantly focusing on such faster payment services diverging from the traditional practices of banks, as discussed during the interviews. The DNB has advised the assessment team it is alive to some of these risks, which are considered as part of the licensing process. The DNB confirmed in materials provided that the methodology applied to determine the level of risk-based supervision for payment service providers is the same methodology applied to the banking sectors. The DNB prepares an analysis of the transactional activity and merchant base of the payment service providers, to gain an understanding of these risks on a sectoral basis.

184. The risk rating of payment service providers by the DNB does not appear to be in line with the risk rating assigned in the NRA. It is unclear what data contributed to the downgrading of risk related to licensed payment service providers in the NRA, and equally the raising of the risk level associated with unlicensed payment services providers (high). The DNB, however, has rated payment services providers low to medium risk. The assessment team was unable to clarify the reason for the inconsistency between approaches.

185. The AFM adopts a similar methodology as the DNB in the risk assessment of OEs. The AFM relies primarily on the data provided by OEs in the annual questionnaires for certain OEs. This is because while the supervisors consider other source of data including information received from investigations, supervisory interaction with FIs (e.g. through account management), signals from consumers, the sector and/or LEAs (FIOD and police), information deriving from cooperative partnerships with the public and/or private sectors, like FEC, AFM-OM-FIOD (Steering Team), Wwft Supervisors Consultation and Financial Intelligence Unit (FIU), data collected from these sources may be limited. the AFM applies a two pronged risk scoring methodology whereby each supervised sector is a signed a risk score and each obliged entity its own score. Unlike the DNB, the AFM includes in the risk factors to be assessed OE's distribution channels. The AFM employs a slightly different scoring system as compared to the DNB, which ranges from 1 (low risk) to 3.5 (high). Based on its assessment, investment firms and managers of investment institutions are rated medium risk while life insurance intermediaries are rated low risk. The risk assessment results reflect the AFM's consideration of the risk factors identified in the NRA and other external sources of information. Factors considered by the AFM to contribute to financial crime risks in the investment sector were the involvement with the wealth management or private banking customers in support of asset management and investment advice, considered to pose a higher risk from customers who wish to hide the source of their funds or evade taxes in their own jurisdiction. Another factor potentially increasing the risk related to these OEs is the use of complex (foreign, including offshore) company structures by customers, such as foreign express trusts and partnerships

that do not have measures in place to distance beneficial owners from their funds or assets and the relatively greater likelihood of wealthy PEPs being customers.

186. The BFT does not employ the equivalent formalised assessment as compared to the DNB and AFM. The BFT relies upon signals received from parties such as the Netherlands Police, the FIOD, the Tax and Customs Administration, the OM, the AMLC and the FIU-NL, an annual questionnaire and other data to determine the risk profile of OEs. The BFT assesses OEs' risk based, partly, on considering whether an OE has a membership in a large professional organisation and whether it holds a WTA license. It considers those affiliated with a professional organisation to have a higher level of awareness about Wwft requirements and are, as a result, treated as posing a lower risk. The BFT also relies upon the KNB in the case of civil-law notaries and the NBA in the case of accounts to provide it with accurate figures on the number of OEs under AML supervision and on the findings of examinations they may have conducted of their members. The BFT is reliant upon the NBA to provide it with an overview of accountancy firms. The BFT maintains a database based on data provided by professional bodies and other information sources. It is unclear whether the BFT has formally documented the methodology it applies, whether OEs are assigned a risk rating on an individual or sector-wide basis or how risk factors identified in the NRA and specific to the OE sectors are assessed in understanding their risk profile.

187. The BTWwft conducts a data-driven risk assessment on a per-sector basis for the different OE it supervises. It further assesses target groups within sectors, and the risks associated with their products and services. This is undertaken through the use of 8 risk matrices designed to assess the specific risk factors for certain sub sectors (auction houses, PMG (precious metals and gems), art and antiques, pawn shops, vessels, vehicles, REBV (real estate brokers and valuers), and the residential furnishings sector (including kitchens, bathrooms, and furniture sectors). The methodology takes account of the NRA risk factors and those which the BTWwft has identified based on a variety of data sources. The output from these assessments is used to prepare risk summaries of each sector and subsector for use by staff when performing supervisory inspections, and for supervisory planning.

188. TheLocal Bar Presidents does not conduct a formalised risk assessment of the OEs it supervises, either on an individual or sector-wide basis. This is the responsibility of the local deans of the 11 different districts in the Netherlands. The deans base their assessment on whether an OE performs services falling within the scope of the Wwft. The deans also rely on signals received from parties including the Wwft Supervisors Meeting, OM, FIU-NL, BFT, AFM and BTWwft, along with regular meetings between the local bar presidents. It is unclear whether the local deans follow a documented methodology for their assessment of risk across the OEs they supervise and how its results are applied to its supervisory approach and planning.

189. The objective of the risk rating process is to inform the manner in which the supervisors will undertake, on a risk basis, oversight of OEs, and the tools they will for this purpose. In general, all supervisors rely on the following supervisory tools: on-site and off-site examinations, thematic and signals-based investigations, annual and thematic questionnaires, industry engagement and communications (either directly with OEs or via professional associations). The length and depth of information requested in questionnaires varies between supervisors and the sectors they supervise. To varying degrees, supervisors issue guidance to assist OEs to comply with the Wwft. The extent and way supervisors followed-up with OEs found to have deficiencies in their AML/CFT compliance programmes also varies.

190. Unusual transaction reports are not analysed by some supervisors as part of their supervisory tasks. The focus is primarily on whether the reports are made, and not on how obliged entities use the data from these reports to better understand the FC risks to which they are exposed. This focus has the effect of OEs focusing more on the need to report as opposed to how the information should be used to better detect and prevent financial crime. In this respect, the reports at present are of limited value from a supervisory perspective.

191. Resourcing is a significant factor that impacts upon the effectiveness of supervisory activities and the regulatory responses across all sectors. Resourcing is very different across the different supervisors and does not always reflect the nature, size and complexity of their OEs supervised or the risks related to them.

192. The DNB disposes of a comprehensive set of supervisory tools. The combination of tools used are determined based on previous planned events (i.e., scheduled onsite examinations) and responsive needs (unanticipated incidents or events). The DNB has recently adopted a new supervisory approach called the ATM. The goal of this new methodology is to assist the DNB in determining, given its limited capacity, the most effective way in which to deploy its resources and apply its various supervisory tools as effectively and efficiently as possible. Supervision activities will be divided into two main categories: (i) scheduled supervision activities (both a basic and a risk-based programme), and (ii) unscheduled supervision activities (supervision requests and unforeseen supervision activities). The ATM is still in its early stages of implementation (full implementation started in the second half of 2020). It is therefore not possible for the assessment team to evaluate its overall effectiveness. Nevertheless, some concerns remain with regard to the application of the methodology in view of the observations on on-site inspections, the shortcomings in taking into account appropriately the risk posed by particular obliged entities and the complicated process of selecting a supervisory response.

193. The DNB relies upon the data provided in annual questionnaires to conduct desk-based monitoring and analysis of OEs. The questionnaires request comprehensive information to allow the DNB to understand the nature, size and complexity of the risks to which the OE is exposed and reflect the risks identified in the NRA. The DNB also exercises its powers to request additional information from OEs.

194. In general terms in the framework of examination, the DNB will take account of prior deficiencies and interventions, a willingness on the part of the OE to resolve any identified deficiencies and whether further re-examination or additional assurance measures (e.g., the review by an external auditor to confirm completion of remediation work) is required. In most circumstances, the DNB will reach agreement with an OE on the required remediation work needed and accept assurance from its senior management as to the completion of what work. In the event the work is not completed to an assurance is inaccurate, the DNB has escalated cases in which further supervisory measures, including further sanctions have been imposed.

195. Currently, onsite visits which focus specifically on an OE are estimated to require 3-4 days and between 2-4 DNB staff, depending on whether it is conducted on or off-site, which is extremely limited. This does not include post-visit analysis, draft report preparation and post-visit follow-up with the OE. Planned thematic investigations are estimated to take up to one year to complete and can require between 1 and 4 staff members, again depending on whether it is undertaken onsite or offsite. Thematic investigations initiated based on an incident or other signals require between 6-8 weeks of time to undertake and involve 2 to 3 staff members. Thematic examinations will involve a sample of OEs in a sector or can involve OEs from different sectors.

196. In practice, the whole examination process is influenced by the nature, size and complexity of an OE, and can take up considerable time and resources. The inspection of 4 exchange houses began in the Autumn of 2015. Findings from the visit were sent to the one OE in Q2 2016, whereas the process for the remaining 3 institutions had not yet concluded at the time of this assessment. This suggests that despite the knowledge and expertise of the DNB staff, it is insufficiently resourced to conduct examinations in a timely manner. This also suggests that the processes applied to conduct examinations may not be as efficient as they could be.

197. The number of onsite visits undertaken relative to the number and profile of OEs supervised by the DNB, appears to be inadequate, relative to the risks identified in the NRA and the findings from previous examinations of Wwft compliance. The DNB currently supervises 84 credit institutions, 14 MTO and 1028 MOT agents and 73 payment service providers, in addition to approximately 600 other OEs in various sectors. Approximately 15 onsite visits of banks, 5 of payment institutions, 3 of MTOs were undertaken over a 4-year period from 2015 to 2018, with a noticeable drop to 7 visits for banks, 2 for payment institutions in 2019. Offsite examinations, both thematic and regular, were varied across the sector. While the thematic examination of banks in 2018 showed a total of 88 banks being reviewed, this dropped to 2 banks in 2019, with an increase to 13 in 2020. Thematic reviews of payment institutions in 2018 involved a total of 32 being reviewed, with a drop to 2 OEs in 2019 and 4 in 2020. MTOs offsite examinations showed a similar trend. The examinations undertaken have been described by the DNB as intensive. The DNB also undertakes enhanced supervision of trust offices for which it performed, on average, 16 onsite examinations in 2018 – 2019, 32 offsites in 2018 and 12 in 2019.

198. The data provided suggests that both resourcing and time taken to complete examinations has resulted in a reduction in the number of onsite visits and quality of checks as well as greater reliance on desk-based analysis, largely driven by the data provided in the questionnaires. The reduction in examinations does not appear consistent with the risk ratings assigned to the different OE sectors. This reduces the DNB's ability to test the effectiveness of controls used by OEs and their application of procedures put in place to mitigate financial crime risks. In the absence of sufficient examinations being undertaken, the DNB is left with limited supervisory tools with which to evaluate the effectiveness of OE compliance programmes in detecting and preventing financial crime.

199. The DNB invests considerable time in educating and raising the awareness of OEs about their obligations under the Wwft. This involves one on one discussions with OEs, periodic meetings and community outreach in the form of roundtables and group discussions. It has published several guidance documents to assist OEs to understand their Wwft obligations, detect financial crime risks and incorporate controls to effectively mitigate those risks.

200. The DNB does not currently work to a methodology with which to assess the effectiveness of its supervisory activities and whether they achieve the desired outcome. While the DNB has received additional resources to support its supervisory work, it would be of benefit for the supervisor to evaluate its past activities against the results produced, to determine if there are more effective and efficient ways in which to supervise OEs. For example, in November 2019, the DNB held a roundtable with unlicensed payment service providers that fall below thresholds requiring a license. The session was organised to raise the OE's awareness of their Wwft obligations. In 2020, the DNB conducted a thematic review of 44 unlicensed payment services providers on the same subject. Approximately 41% of those were found to have shortcomings in their compliance with the Wwft. It is unclear from the supervisory approach taken whether the effectiveness of those roundtables was evaluated to determine whether it

achieved better compliance by OEs with the Wwft's requirements. The DNB has invested considerable time in the supervision of large banks. The recent cases of ING and ABN AMRO may suggest a need for a review of the way in which supervision of large banks is undertaken to ensure that systemic issues of non-compliance are responded to in a timely and effective manner and achieve the desired results from the bank that can be achieved in a resource-efficient manner. The discrepancy with the very limited number of days dedicated to the on-site inspections on average (see above) which will not allow full-scale checks is also noted.

201. DNB resourcing also requires scaling to incorporate the necessary technical knowledge to effectively test and assess technologies used by OEs to comply with Wwft obligations. Some OEs interviewed reported they perceived the DNB does not have a good understanding of technology adopted to support their AML/CFT activities.

202. The AFM follows a similar approach to the DNB in its supervision. Supervisory activities are divided between risk-based sectoral investigations and thematic investigations. The AFM relies on the data in its annual questionnaires to conduct thematic reviews. The AFM also conducted signal-based or incident investigations, follow-up investigations and regular investigations. As a rule, the investigations focus on OEs in a particular sector. The AFM has not provided statistics on the time taken to complete examinations. The target for completion of an investigation is to arrive at a result in at least 75% of cases within a year.

203. The number of onsite visits undertaken relative to the number of OEs supervised by the AFM, appears to be inadequate, relative to the risks identified in the NRA and the findings from previous examinations of Wwft compliance. The AFM currently supervises over 7860 OEs of which 899 are registered or licensed investment firms. The number of investigations in 2018 and 2019 both on and off-site have remained consistent (23 onsite and 29 offsite in 2018 and 25 onsite and 28 off-site in 2019). Investigations in 2019 resulted in 21 violations of Wwft being identified. The number of visits appear insufficient relative to the previously identified cases of non-compliance by the investment sector with the Wwft and limited scope of other supervisory measures undertaken to assess the effectiveness of OE's compliance controls.

204. The supervisory approach for these examinations appears primarily driven from the answers received in the annual questionnaires and less based on risk identified in the NRA or signals obtained from other bodies. OEs will receive written instructions where answers concerning Wwft compliance to the questionnaire are considered by the AFM to be inadequate or suggest concerns regarding their compliance controls. A sampling of the OEs who complete the questionnaire is undertaken in the form of a focused or thematic investigation. This approach has been consistently applied for at least 4 years.

205. The questionnaires have recently been expanded to incorporate data relevant to the NRA risks identified as relevant to the investment sector: involvement with the wealth management or private banking customers in support of asset management and investment advice, use of complex (foreign, including offshore) company structures by customers, such as foreign express trusts and partnerships that do not have measures in place to distance beneficial owners from their funds or assets and PEPs.

206. Statistics on the answers given in the questionnaire to Wwft matters suggests a high level of compliance with Wwft requirements. For example, over a 3-year period from 2018 to 2020, approximately 91% of investment firms said they completed a SIRA, and in 2020, 90% reported it was updated. Approximately 82% reported completing CDD prior to the acceptance of a customer and 80% reported have a transaction monitoring system in place. However, these

statistics only confirm the technical requirement of the Wwft and not whether these controls are applied effectively to mitigate risks.

207. Evidence suggests that the AFM's supervisory approach is not resulting in improved compliance by some OEs and take considerable time to complete. In 2018, the AFM analysed 289 questionnaires received from investment firms (including branches in the Netherlands of foreign firms). From this group, the five most high-risk OEs were selected for on-site investigations. The investigations covered compliance with the entire Wwft. Infringements were found in all five investigations. Three investigations were completed in 2019. Of the three OEs examined, two received a letter of findings requesting a plan of action. One OE received a warning letter. In 2020, another of the OEs received a warning letter and the fifth OE was transferred to a foreign supervisor. In 2019, a risk-based sectoral investigation into investment managers. Onsite investigations were conducted on two licensed managers and three registered managers. One investigation was completed in 2019. Three investigations were completed in 2020. One investigation was completed in 2021. Wwft infringements were found in all investigations; In 2020, five new risk-based investigations of investment firms were conducted and concluded. Infringements of the WWft were found in four of the five investigations.

208. The examples provided illustrate that the conduct of onsite inspections does not appear to encourage investment managers to improve their WWft compliance even if the introduction of new AML/CFT requirements is taken into account. On each occasion where examinations where undertaken, more violations were identified. The time taken to complete the examinations potentially leaves financial crime risks unmitigated for a long period of time. The AFM's response to these examination results appears to favour voluntary compliance or informal warning letters, even in cases of serious systemic failings. Over a four year period from 2017 to 2020, 4 warning letters have been issued, 19 compliance briefings held, 21 instruction letters issued on compliance with the Wwft and 30 information letters on compliance with the Wwft. Sanctions have been imposed in limited instances (see section on sanctions below).

209. An example of an instruction and a warning letter were provided to the assessment team that were sent to of investment firms following an examination conducted in 2020. The reason for conducting the thematic investigation TM and Mandatory Reporting in 2019 was the number of reports of unusual transactions to FIU-NL, which, according to the AFM, had been low for years. The risk survey undertaken in 2018 also disclosed that 27% of investment firms, 16% of licensed (managers of) investment institutions and 35% of registered (managers of) investment institutions had no automated or manual system at all to monitor transactions. In response to these findings, further thematic investigations were undertaken in 2020. The findings from those examinations disclosed failings in addition to transaction monitoring that disclosed possible systemic non-compliance concerns across the OEs' compliance controls and evidence a lack of understanding and/or application of the Wwft requirements such as PEP's, conducting enhanced due diligence, conducting KYC practices inconsistent with set policies and weakness in risk assessments. These same areas were identified as risk areas identified in the NRA which contribute to the medium risk rating assigned to investment managers. The AFM applied different supervisory responses to the results of these further thematic revues, determined based on several factors. For example, where one OE had started the necessary remediation to resolve the deficiencies as at the time of the examination, a warning letter was deemed to be a suitable response accompanied by the submission of a detailed action plan within an expedited time period and a deadline by which to be completed. Monitoring was

undertaken to ensure that deadline set were satisfied. To verify completion of those measures, and external third party review of the remediation undertaken was completed.

210. The data above suggests that there is an over-reliance on questionnaires as the main supervisory tool. This reliance is intended to improve the efficiency of the AFM's supervisory activities. However, these questionnaires disclose continuing non-compliance by OEs with the Wwft requirements, despite efforts by the AFM to engage and educate them to comply with these requirements. Sample investigations reinforce findings of non-compliance, but no further steps are taken to assess whether the scope of non-compliance extends more widely across the OE sector. The number of instances in which non-compliance has been observed over the 4-year period, suggests that non-compliance may be more widespread. The supervisory responses observed non-compliance involving feedback correspondence, discussions, warnings and individualised instruction letters fail to provide the broader OE sector with feedback through published guidance, which would reach a wider audience, be more resource efficient and possibly be a more effective deterrent.

211. The AFM does not currently work to a methodology with which to assess the effectiveness of its supervisory activities and whether they achieve the desired outcome. The AFM fails to assess its resourcing needs relative to the risk profile of the OEs it supervises and the types of supervisory measures it undertakes. The AFM's examinations are extremely time-consuming and fail to result in timely findings. It would be of benefit for the supervisor to evaluate its past activities against the results produced, to determine if there are more effective and efficient ways in which to supervise OEs and achieve the desired level of compliance.

212. As of 2020, the BFT supervises approximately 48,000 OEs, which included 773 civil law notary firms, 3,374 individual civil law notaries and as of 2019, almost 8,900 external accountants and auditors. Most entities supervised are accounts and auditors (8.899) and civil-law notaries (3,312) (figures as at 2019). The BFT is aware of the specific risks in the NRA, relevant to accountants/tax advisors: ML using loan-back scheme, entity stacking, offshore schemes, investment schemes;-Trade-Based ML (TBML) including -misuse of entities through straw men and foundations. It is unclear how these risks are reviewed by either the SRA, RB, or by the BFT outside of its thematic risk-based reviews. The BFT's supervisory approach now largely relies upon the other professional associations to support its supervisory activities and employs more off-site supervisory tools.

213. The Dutch Register of Tax Advisers (RB) and the Association of Registered Accountants (SRA) are responsible for performing examinations (referred to as reviews) of their members compliance with the Wwft. The supervision arrangements are considered a form of horizontal supervision (e.g., audits by the sector organisations themselves). These reviews are in addition to the supervision exercised by the BFT. Wwft requirements are assessed during these visits which also examine other unrelated compliance matters. Both the SRA and the RB perform approximately 40 reviews on a yearly basis. The selection of OEs chosen for reviews is not based upon their risk profile, however, the reviews themselves are undertaken by applying a risk-based approach. The reviewers of both the RB and the SRA who conduct these examinations are trained by the BFT. The RB and the SRA inform the BFT on the outcomes of their reviews in their annual reports, but do not provide a detailed examination report of their findings. It is reported by the BFT that in general, most of the reviews result in a compliant or largely compliant results. There is no evidence that the BFT conducts periodic checking of these reviews to confirm the accuracy of their examination findings. The BFT has provided input on the review methodology and contributed to case study examples for the benefit of the professional organisation reviewers.

214. Cases of non-compliance are only escalated to the BFT when members are not willing to cooperate with the audit. Such cases are subsequently handled by BFT. No similar audits are conducted by the RB of tax advisors who are not its members.

215. The BFT undertakes a limited number of risk-based thematic risk-based reviews focusing on specific sector of OEs (TCSPs) or client groups (i.e.health care service providers) . These risk-based inspections have almost doubled over a 5-year period from approximately 20 to just below 50 inspections. The BFT is reliant upon professional organisations to provide regular engagement with their members on Wwft compliance. While BFT published guidance on compliance with the wwft, the most recent materials were published in 2018, and those concerning financial crime risk indicators last published in 2014.The BFT has acknowledged it is more difficult to engage in supervisory activity with those OEs who are not members of these organisations. The BFT is supported by a Special Investigations Support Team set up within the BFT in 2013.

216. The supervisory activities of the BFT are largely driven by signals received from various bodies in the Netherlands. The Special Investigations Support Team evaluate and prioritise the received signals from 1 (very urgent) to 3 (less important). A signal received from the Dutch Netherlands Police is rated higher than a signal received from an individual. The BFT has introduced automated desk-based monitoring in 2016 under a project called Digin Wwft, for administration offices. The system delivers automated notifications to OEs concerning their compliance with the Wwft. Approximately 1100 OEs received letters in 2020. OEs are asked to complete a questionnaire comprising of high-level questions concerning the Wwft, office procedures and training. Based on the results of analysis, several of the offices are selected to visit onsite or additional inquiries are made. Both the selection of the OEs and the choice of the region where they are located are risk-based.

217. Between 2018 and 2020, on-site examinations were conducted by the BFT, on average, on 8 civil-law notaries, 6 accountants and auditors and 36 tax advisors. Tax advisors across this three-year period were consistently found not to comply with a number of Wwft requirements: KYC and CDD (2018 29 violations, 2019 29 violations and 2020 33 violations); transaction monitoring (2018 20 violations, 2019 19 violations and 2020 27 violations) and STR filing-subjective (2018 21 violations, 2019 20 violations and 2020 16 violations). Tax advisor examinations began to include reviews of their internal controls and group policies following transposition of the 4th AMLD. In 2019 and 2020 tax advisors examined were found not to have complied with the controls requirement (22 violations in 2019 and 29 violations in 2020) and the group policy requirements (24 violations in 2019 and 25 violations in 2020). It is understood that a significant proportion of these violations involved administration offices in particular. These figures suggest ongoing and systemic concerns regarding those entities' understanding about and application of the Wwft requirements.

218. Because each case is considered on an individual basis, statistics are not maintained as a matter of course to identify possible trends in the types of violations found across OEs. Of the cases where violations were identified in 2019 and 2020 for tax advisors, the most common supervisory response was to require a performance improvement plan (19 in 2019 and 18 in 2020) followed by warning notices (9 in both 2019 and 2020).

219. Several sectoral guidance documents have been published to assist OEs in understanding their Wwft obligations. These include detailed descriptions of typologies and case studies. The professional organisations (in particular NOB, RB, KNB and NBA) actively inform their members about the obligations under the Wwft as well as about relevant case law. The

professional organisations answer questions of members about practical situations. the NOB, NBA and the RB, among others, have developed e-learning modules. Any findings from reviews performed by the SRA and RB that require follow-up from the OE are followed-up by the professional organization that performed the review.

220. BFT also answers questions from OEs related to their obligations under the Wwft. Where the BFT has been involved directly in investigating the activities of an OE, and remedial action is required, the OE will be required to confirm its completion of those actions directly to the BFT. .

221. The supervisory approach adopted by the BFT does not appear to be effective in achieving desired levels of compliance by tax advisors. Although risk factors from the NRA are understood, it is unclear how the BFT ensures they are considered as part of supervisory activities. Reliance placed upon professional bodies to raise and assess OE's awareness of and compliance with Wwft does not appear to be effective, in relation to the respective tax advisors within professional bodies' remit. The BFT does not currently work to a methodology with which to assess the effectiveness of its supervisory activities and whether they achieve the desired outcome. . The supervisor has not evaluated its past activities against the results produced, to determine if there are more effective and efficient ways in which to supervise OEs and achieve the desired level of compliance. The BFT has commenced an initiative through which to perform enhanced supervision of administration offices, due to the elevated risk concerns related to their compliance with the Wwft requirements.

222. The BTWwft organises its supervisory activities around three areas: risk-based signals, a thematic approach, and other supervision methods. A total of 90 signals were registered in 2019, 82 of which were provided by external stakeholders. Well over 70% of the investigations completed in 2019 concerned an institution within the meaning of the Wwft. Supervision is undertaken in a variety of ways, determined on a risk-basis. In addition to on-site inspections, the BTWwft also makes use of individual information visits, on-site observations, and compliance meetings. Off-site inspections, such as telephone re-inspections, conducting telephone inquiries, the provision of information, and desk-research.

223. When it starts supervising new sectors, the BTWwft issues new OEs questionnaires to obtain an overview of the risks that may present themselves. This has most recently included two different sectors involved in trading high value items to assess the extent to which their transactions are cash-based and their application of the required Wwft measures.

224. The BTWwft has adjusted its supervisory approach since 2017 by relying heavily on off-site inspections, in order to increase the number of OEs reviewed. Sector descriptions are prepared for supervisory staff outlining the specific financial crime risks associated with different OE sectors, which reflect the risks identified in the NRA and SNRA and other sources to ensure these areas are reviewed during examinations. Supervision is customised on the basis of the expected individual risk signals and risk signal that are sector specific (communication about enforcement and sectoral observations). Planning is undertaken so risks are prioritised, both within the various BTWwft branches and between them, at to their seriousness and the effectiveness of supervision. External signals provided by inter alia the Netherlands Police, the Tax and Customs Administration, the AMLC, the OM, Customs, and the Fiscal Information and Intelligence Service are used and prioritised to initiate targeted investigations.

225. The BTWwft also focuses on subsets of risks identified in the NRA, specific to certain OEs. Particular attention is paid to several areas including cash-intensive businesses operated by OEs, domiciles and the real estate sector. For example, closer supervision has been undertaken of brokers involving the sale of holiday homes to foreign owners (2017). Supervisory measures have been undertaken as a result in relation to approximately 30% of the brokers reviewed. The BTWwft undertakes re-inspectiosn of those entities where areas of non-compliance with Wwft requirements were found. Real estate agents are subject to the largest number of re-inspections following identification of non-compliance with the Wwft In 2018, 198 re-inspections were performed and that in 91 (approximately 50%) the BTWwft identified possible new instances of non-compliance, albeit in most cases these were not determined to be as serious such as to warrant a referral to the penalty fine officers. For those cases where compliance deficiencies had not yet been resolved, supervisory action, including referrals to penalty officers and fines inmposed, in response. The vehicle industry has also been the subject of closer supervision in relation to its connection to several risk areas identified in the NRA.

226. Resourcing for the BTWwft appears sufficient relative to the size of the OE population. The BTWwft tracks its hourly usage of staff time across the differed supervisory approaches it applies. In 2018, for example, the BTWwft records a total of 27,436 hours were spend on supervisory activities, investigations consume the most time equivalent to 562 hours across all OEs, averaging 40 hours per OE investigated. Communications via phone involve 244 hours in total, and average 3 hours per OE. The number were roughly equivalent in 2019. The BTWwft has employed several innovative approaches to the efficient use of its resources, to manage its available resource capacity as the scope of its supervisory oversight had expanded under the 4th AMLD.

227. The BTWwft invests time in educating and raising the awareness of OEs about their obligations under the Wwft. This involves one on one discussions with OEs, periodic meetings and community outreach and presentations. It has published a number of guidance documents to assist OEs to understand their WWft obligations, detect financial crime risks and incorporate controls to effectively mitigate those risks.

228. The legal profession's supervisory approach is largely incorporated as part of the wider supervision of lawyers and their compliance with their professional requirements. For the legal profession, Pursuant to Article 1 and 1a(4)(c) of the Wwft, the Wwft only applies to lawyers to the extent they render advice or assistance in the context of the services as referred to in this Article. Article 1a(5) of the Wwft provides the so-called "lawsuit exemption". The Wwft is not applicable to lawyers to the extent that they carry out work for a client relating to the determination of the client's legal position, representation and defence in law, the provision of advice prior to, during or after a legal action, or the provision of advice on the institution or avoidance of legal action.

229. Supervisory activities are planned based on discussions held among Local Bar Presidents. The local Bar President is responsible for the supervision of all lawyers in the judicial district. The local Bar Presidents are charged with supervising compliance with Wwft by lawyers with registered offices in the local Bar President's district based on Article 35(4), Article 45a(1) and Article 45a(1) of the Advw in conjunction with Article 24(2) Wwft. The Local Bar Presidents are authorised to request information and demand inspection of business data and documents and make copies, under the Awb. Local Bar presidents and NOvA have laid down policy rules and guidelines on providing Wwft services.

230. Local Bar Presidents are assisted by the council of the local bar, local bar staff and by experts from the Legal Profession Financial Supervision Unit (unit FTA) Information on the presence and role of a Legal Profession Supervision Unit within the Netherlands Bar (DTA) was provided by the authorities only after the on-site visit and therefore all references below are to the FTA. The FTA assists the local Bar Presidents with Wwft investigations. The FTA unit is comprised of 4 individuals.

231. Lawyers whose activities fall within the scope of the Wwft are identified as part of a broader Central Check questionnaires (CCV) which they are required to complete. The CCV includes questions about the number of cases treated as Wwft files and the number of reports of unusual transactions in that calendar year. The 2019 CCV disclosed that approximately 900 firms confirmed they performed Wwft services in that year and an average of 10% of all their legal services are Wwft-related. A further questionnaire is sent to lawyers requesting information allowing the Local Bar Presidents to understand their risk profiles based on the nature and scope of the legal services they provide, and their customers.

232. Local Bar Presidents are responsible for risk categorizing OEs under their supervision and deciding the level of supervision to apply. Selection of lawyers or law firms for examination is decided by local Bar Presidents who decide this based on the extent to which they provide services covered by the Wwft based on the CCV or if the lawyer is deemed prone to ML risks. Attention is also paid to those lawyers who report they do not provide services covered by the Wwft. The local Bar Presidents, via the FTA, also base their supervision on signals received from other bodies with whom they attend periodic meetings. According to the NOvA, these meetings have not led to any concrete signals that indicate any unusual activities by lawyers resulting in disciplinary cases. Attention is also paid to those lawyers who report in the CCV that they do not provide services covered by the Wwft, whenever there are indications to the contrary.

233. The Wwft Supervision Policy Rules 2018 (Policy) introduced in January 2019 described the method of supervision to be undertaken by the Local Bar Presidents deans. This comprises mainly office inspections which must be prepared for based on uniform preparatory information. During inspections certain records listed in Article 20.4 the Policy may be requested. These records relate specifically to the services to which lawyers must apply the Wwft requirements. The Policy does not appear to provide examiners with the power to ask for further information beyond this list. This may impede the FTA examiner's ability to obtain further information to verify lawyers' technical compliance with the WWft and effectiveness of their compliance programmes. The Policy also states that follow-up inspections will specifically focus on monitoring compliance with obligations arising from the Wwft. It is unclear whether this stipulation would otherwise limit the scope of information that can be requested to assess whether required remediation was completed, or in relation to new risks identified.

234. Examinations performed by the FTA will depend upon the nature and size of the lawyer or law firm. Estimates of time required for an examination are: small law firms: 1.5-2 days, medium size firms: 2-3 days and big law firms: 4-5 days, depending on the issues found. These estimates include pre-examination preparatory work, drafting the findings (estimated to take approximately 5 – 7 hours). The times estimated are extremely short and suggest that the reviews undertaken are very high-level and driven by the limited resources available in the FTA to complete the number of examinations requested by district presidents.

235. Local Bar Presidents can compel the production of information but are not able to share this information with other Local Bar Presidents or other supervisory bodies, by virtue of a duty of confidentiality. It is unclear whether the local dean can delegate these powers to the FTA who perform the examinations on its behalf. Also, it is unclear not clear whether this power includes the ability to request that OEs to produce client files which are classified as falling outside the scope of the WWft, to confirm whether this assessment is correct. Currently, this topic is not included in the list of topics that can be reviewed under the Policy.

236. Local Bar Presidents are aware of the specific risks in the NRA, relevant to lawyers. These include: ML via offshore companies, misuse of clients' accounts for ML, ML via complex company structures, obscure flows of money coming in from abroad, bribery and corruption, supply chain transactions within the real estate sector, ML by moving cash from/to the Netherlands, misuse of foundations. However, these topics do not appear to be canvassed in any detail in either planned examinations or in the thematic examination conducted in 2019. Several guidance documents have been published to assist OEs in understanding their WWft obligations and assist in the drafting of a risk policy.

237. Several OEs interviewed have or are planning to rely on different forms of technology to support AML/CFT compliance controls. This does not appear to be considered as a risk factor considered as part of examinations.

238. The local Bar Presidents and FTA do not currently work to a methodology with which to assess the effectiveness of its supervisory activities and whether they achieve the desired outcome. It would be of benefit for the parties to evaluate its activities against the results produced, to determine if there are more effective and efficient ways in which to supervise OEs and achieve the desired level of compliance.

239. Based on the estimated number of OEs (5,618) the local deans have stated that for supervisory purposes this is "manageable", from a resourcing perspective. This, however, assumes that current examinations continue to be performed at the speed noted above. Local deans plan to monitor these numbers and perform additional research to verify the accuracy of this assessment. If necessary, the deans will amend their risk identification and risk profiles of lawyers at a later stage. It is recommended that the deans may wish to instead consider adjusting their supervisory approach based on the risk profile of the OEs and the sector, rather than to accommodate supervisory resource requirements.

Sub-theme (b): Sanctions

Articles 58

240. The Wwft provides for a wide range of enforcement measures at the disposal of the DNB and AFM, ranging from corrective measures and pecuniary sanctions to suspension of operation and revoking of licenses. The Wwft includes specific criteria that must be considered to determine and calculate sanctions, such as the gravity and duration of the breach, the financial strength of the OE, the benefit derived from the breach, and any previous breaches thereof.

241. The DNB has imposed a variety of sanctions (referred to as enforcement measures), which it classifies as either formal or informal. Formal measures include instructions, fines, order subject to a penalty, license withdrawal and appointment of a curator. Over the period 2015 to 2019, fines were imposed to varying degrees –approximately 2 were imposed in 2015 while 7 were imposed in 2019; 1 licence withdrawal occurred 2019; Instructions were issued in

varying degrees, ranging from approximately 3 in 2015 to 7 in 2019. Approximately 31 formal measures in total were imposed in 2015 while 35 formal measures in 2019. The timing of imposing sanctions is influenced by the time period over which a case is investigated and a final decision on the necessary enforcement measure made and also involve coordination externally with the WP-WW (OM and the FIOD) in case of punitive enforcement measures. The DNB has also undertaken, in limited cases, the escalation of formal enforcement measures where OEs have failed to remediate previously identified Wwft deficiencies.

242. Figures concerning trust offices show the same trend. In total, approximately 20 formal enforcement measures were imposed in 2015 with an equal number imposed in 2019. Use of enforcement measures against trust offices was most frequent in 2016 (25 measures) because of a large thematic investigation into trust offices.

243. The most serious enforcement measures to date reported in the Netherlands, involving ING and ABN Amro, were the subject of financial penalties (ABN AMRO €480m), the latter agreed by way of settlement with the public prosecutor.

244. The DNB published its first Wwft based instructions made against an OE in 2020, following a thematic visit in 2020 related to trade finance, where shortcoming regarding transaction monitoring and the risk identification process.

245. The DNB believes that its use of formal enforcement measures acts as an effective deterrent along with the informal enforcement measures it employs (which are, in effect, supervisory activities). However, based on the figures provided to the assessment team, the number of formal enforcement actions taken is regarded as low given the number of violations identified across OE sectors supervised. There was no clear indication during the interviews, that the OEs would consider the enforcement action taken by the DNB to act as an effective deterrent. The team notes but cannot concur therefore with the DNB explanation that informal enforcement measures are more effective to ensure OEs take all necessary measures to address identified deficiencies where and in case the OE shows it is willing and able to remediate the violations within a timeframe the DNB assesses as acceptable. The criteria to be applied when selecting an enforcement measure are laid out in the Enforcement Policy.

246. Similar findings are made with respect to the AFM in terms of the use of informal and formal enforcement measures. The AFM imposes far fewer formal enforcement measures. In the period between 2017 and 220, 8 formal enforcement measures were imposed, an average of 2 measures per year, on investment firms. The same average applies for investment managers. This seems disproportionate given the number of findings of non-compliance with the Wwft identified during this period. In comparison, in 2019, 38 informal enforcement measures were imposed on investment managers. The deterrent effect of the measures used do not appear to result in a reduction in the level of non-compliance, or alternatively, reveal a broader scope of non-compliance within the sector than originally understood. This is concerning given the reasons for which investment firms and managers were rated medium risk, because of the risk exposure to several of the risks identified in the NRA.

247. The BFT has imposed a variety of formal sanctions against OEs for non-compliance with the Wwft. Over a five-year period, from 2015 to 2020, the most common enforcement measure was the imposition of a performance improvement plan (31 in 2015 and 22 in 2019). The second most common form of enforcement measure was the imposition of a fine (18 in 2015 and 21 in 2019). Disciplinary complaints in relation to civil-law notaries were negligible across this period. Tax advisors appear, from 2015 to 2020, to consistently be found to have violations in

relation to KYC and CDD requirements. The same violations were also found in relation to accountants, auditors and notaries albeit of smaller proportions. The total amount of fines imposed the same period against tax advisors has ranged from €32,250 in 2015 to €69,990 in 2020. The total amount of fines imposed against accountants and auditors has consistently been over €126,000 between 2016 and 2019, while the total amount of fines against civil-law notaries have ranged from €10,000 in 2016 to over €129,000 in 2020.

248. While it is understood that the level of supervision undertaken by the BFT has increased and is partly attributable to the increased detection of violations, the findings indicate there continue to be challenges with OEs in these sectors applying the Wwft requirements. Further findings in this same period disclosed that violations related to the filing of subjective suspicious transactions appear to have been found again in larger proportions for tax advisors (in particular administration offices), with moderate fluctuation in violation numbers for notaries, external auditors and accountants. Finally, shortcomings in internal controls, first reviewed following the transposition of the 4th AMLD, were highest in relation to tax advisors (22 advisors in 2019 and 29 in 2020). This suggests that either (a) a systemic problem with KYC and CDD compliance by tax advisors and administration offices, in particular, for which existing approach to supervision is not effective and/or (b) sanctions imposed in response to these violations are not having the desired deterrent or preventative effect. This is particularly serious given the important role these OEs play in detecting the misuse of legal entities, shell companies, complex structures, foundations and other risk areas identified in the NRA. Steps have recently been taken by the BFT to address this risk by launching a dedicated project devoted to raising the awareness within the administration office community about its Wwft obligations and their fulfilment.

249. Civil-law notaries can also be sanctioned by way of a disciplinary complaint or an administrative fine. Which sanction regime applies, depends on the specific circumstances. When there are also breaches identified with other regulations (in particular Wna), a disciplinary complaint will be filed with the disciplinary judge (Kamer voor het Notariaat). If only Wwft breaches are identified, a fine will be imposed by the BFT. In one case, for example, a notary failed to perform customer due diligence in relation to a trust office that was being misused. The judge ruled the notary should have performed due diligence on the clients of the trust office and had failed to comply with UTR requirements. The notary was suspended for two weeks and a fine of €10,000 was imposed. The BFT relies on the publication of disciplinary procedures as a deterrent. No evidence was provided to indicate that other professional bodies use their disciplinary procedures to enforce compliance with the Wwft.

250. The BTWwft has imposed a variety of sanctions based on a proportionate intended to reflect the seriousness of the violations identified. In 2018 vehicle traders were fined almost €135,000 for approximately 107 violations of the Wwft committed by 24 OEs, mainly related to CDD and KYC deficiencies. 31 sanctions were imposed against real estate agents, 24 of which were due to violations of the KYC and CDD requirements and failures to file subjective STRs. These included fines of over €7,000. In 2019, 19 sanctions were imposed against real estate agents were sanctions for Wwft violations, which includes and fines of €30,000, along with a €10,000 cease and desist order.

251. As a result of the BTWwft 's thematic review of vehicle dealers in 2019, 41 dealers were found to have violated the Wwft comprising a total of over 500 violations. Sanctions were imposed in form of fines of approximately €171,000 and cease and desist orders totalling €392,000. The BTWwft also consults the OM and investigative services via the non-reporting institutions committee about the possible criminal prosecution of offenders. In two criminal cases the

Higher Court imposed fined for violations of the Wwft. These concerned two sellers of goods (f €500,000 and €200,000). Two cease and desist orders were forfeited in 2020. These concerned a company service provider (€50,000) and a seller of goods (€1,000).

252. Sanctions have also been imposed on domicile providers. In July 2020, an OE received a fine €50,000 related to its failure to remediate previously identified Wwft deficiencies. However, as a at the time of the assessment, the website of the tax office is being adapted so that the imposed sanctions can be published.

253. The legal profession undertook over 800 inspections of OEs in 2020 and over 1100 inspections in 2019. Local Bar Presidents are authorised to take enforcement action against violations of the rules referred to in the Wwft by issuing an instruction, imposing an order subject to a penalty or imposing an administrative fine. They may also publish a warning given or a statement, specifying the violation and the violating party or impose a fine, based on the Administrative Fines (Financial Sector) Decree. To date, no administrative sanctions for AML/CFT violations have been imposed on OEs. Local Bar Presidents can file a complaint against a lawyer with the professional disciplinary body for non-compliance with the Wwft. The assessment team was advised that steps are being taken to amend the enforcement policy to address the relative complexity of the process that must be followed two apply administrative sanctions.

Article 59

254. The DNB and the AFM have extensive supervisory powers which can be used to address AML noncompliance, comprising both formal (e.g., fines) informal enforcement measures (e.g., warning letters). A list of factors based on the Enforcement Policy published by DNB/AFM is taken into account in deciding whether enforcement action is required, including all relevant circumstances of the case and balance the interests directly involved in the decision, such as the severity of the violation, culpability and compliance-oriented attitude. Formal enforcement measures may be corrective or penalising. The supervisors must publish each formal enforcement measure it imposes in connection with a violation of the provisions of the Wwft once the sanction decision has become final. The supervisors must also publish two types of sanctions decisions before they become final - administrative fines imposed due to a serious violation of the Wwft, and orders subject to a penalty, provided the penalty is incurred, i.e., once the term within which the order could have been complied with without penalty has lapsed. In certain cases, DNB may decide to publish an anonymised version of the administrative sanction, to delay publication, or not to publish the sanction.

255. In practice and based on the data provided to the assessment team, both supervisors do not make use of all of the full range of sanctions at their disposal. For example, there is limited publication of cases of non-compliance, the power for which was introduced in mid-2018, which are made known to the wide OE community. As reflected in the data provided, there seems to be a preference for using informal enforcement measures and other forms of supervisory oversight by both DNB and AFM. This appears to be attributable to following factors: (a) The DNB applies a comprehensive decision-making process in deciding whether to impose a sanction and if so, in what form. This can be a complex and time-consuming process. This may unintentionally act to deter the supervisor from recommendation more severe sanctions, or a combination of sanctions which may prove to be a more effective deterrent. (b) the process for publishing a decision is very complex in practice. Other legal considerations are partially attributable to this. However, this acts to chill the use of this sanction, which would be a more effective and efficient as a deterrent, relative to the individualised supervision activities

identified above; and (c) there is an overall lack of appetite to pursue more serious sanctions. Although national coordinating bodies or meetings to decide how to proceed with a particular case, supervision of more complex cases tend to be undertaken in a more informal way and there was feedback from supervisors that there is too much of being careful and cautious and so informal measures are used to try and progress these cases and coordinate them more effectively.

256. The BFT determines the enforcement measure to apply based on the BFT enforcement policy decree of 2015. Each case is assessed based on seriousness and degree of culpability. The BFT has implemented an internal finding policy to supplement those described in the Wwft. A percentage based on the turnover of the company is applied taking account of the seriousness duration and culpability. Where these determinants are found to be very high or very serious there will be coordination with the OM to determine whether a criminal prosecution should be undertaken. A wide range of sanctions are available to the BFT, who has used these as noted above.

257. The BTWwft has imposed a variety of sanctions on the OEs it supervises. The BTWwft uses an enforcement matrix, which assesses the number of transactions where violations have been detected and whether this is the first instance in which violation have been identified or a repeat occurrence. The OE is also score on culpability. Where violations occur unknowingly or unintentionally, the case typically results in a formal instruction to improve AML procedures. Offences are discussed with the OE and what improvements are needed. If there are evidence violations were intentional or the overall score reaches the set threshold (45 points or more), the case is handed over to the penalty fine officer. Penalties that can be imposed include monetary fines and cease and desist orders. The BTWwft applies an escalating process when selecting sanctions to reflect both the seriousness of the violation and the desired outcome (e.g. to deter future violations). The BTWwft is in the process of writing down its enforcement and find policy as a formal decree which will be published so that there is greater transparency around how it arrives at these decisions.

258. The range of sanctions the BTWwft can impose, however, appears to have been constrained, to a limited degree, by supporting infrastructure. For example, In July 2020, an OE received a fine €1,000 related to its failure to remediate previously identified Wwft deficiencies. A decision was made to publish the fine. The OE did not object to this decision. However, the Tax office website is not configured the notice to publish the fine was sent to the owner of the business in May 2020 who did not object to the decision to publish. However, at the time of the assessment, the tax office was still in the process of adapting its website so that the notice could be published on it.

259. While local Bar Presidents are empowered to impose a variety of sanctions, in practice the use of administrative sanctions is very complex. The procedures required under the Enforcement Policy includes requirements and restrictions that are not applied in other regulated sectors. For example, if a lawyer is found to have committed a violation for which an instruction and a penalty can issued, the local Bar President must, as far as possible, impose in instruction unless it can be shown that a penalty is more appropriate. The local Bar President must also first issue an order subject to a penalty instead of imposing an administrative fine unless it can be shown that a penalty is more appropriate.

260. Similar complex requirements are imposed in relation to publication of a statement concerning the violation. Each intended warning or statement must be discussed by the local Bar President with the Wwft Knowledge Centre and the FTA to determine whether there were reasons to

proceed with the publication. Consideration should also be given to whether the warning should be published on the website of the local Bar Association and sent to the NoVA to be published on its website. This procedure has the effect of dissuading local Bar Presidents from applying administrative sanctions, opting instead for informal enforcement measures or professional disciplinary proceedings. This appears to be the main reason why reliance is placed instead on the professional disciplinary process. The local deans advised the assessment team that steps are being taken to review and simplify the process described in the Enforcement Policy.

Compensatory Measures and Detrimental Factors

261. The supervisory approach taken by the AFM could expose other Member States to risk where it fails to effectively supervise OEs who subsequently establish a branch in another Member State by way of passporting arrangements. The reliance placed by Member States on one another to ensure that AML/CFT obligations are effectively applied by OEs, requires that supervision of OEs in that sector be appropriate, and responses to non-compliance timely and decisive.

262. The situation with the supervisory responsibilities over legal professionals as discussed above has a detrimental effect on the effectiveness of the application of the 4th AMLD requirements despite the formal completeness and conformity of the transposition as noted in COM analysis.

Conclusions (supervision and sanctions)

263. The assessment team has identified **major deficiencies** in the practical application of the supervision of financial institutions and designated non-financial businesses and professions with **major impact** on the effectiveness, including:

a. DNB - Absence of clear methodology of the assessment of risks related to channels of delivery and technology in determining the risk profile of OEs results in an incomplete understanding of the risks based upon which supervisory activities are applied;

b. DNB – Application of uniform risk assessment methodology across all OEs results in an incomplete understanding of the risks associated with particular OEs based on the business models and activities; this may result in some OEs being inaccurately rated lower risk in terms of their potential impact.

c. DNB – Failure to scale resourcing and expertise commensurate with the growth and use of technology by OEs to properly evaluate the risks and controls required to mitigate them.

d. DNB - number and scope as well as duration of onsite visits undertaken appears to be inadequate in view of the risks identified in the NRA and the findings from previous examinations of Wwft compliance.

e. BFT – ineffective risk rating considerations for OEs, including risk rating of OEs based on professional body membership.

f. With regard to law firms on-site inspections are performed on a very limited time scale and therefore to a limited extent; there are limited powers available to request information from OEs; the effectiveness of examinations as supervisory tool is impacted by the limitations to share information and the scope of examination is limited.

g. All supervisors – lack of methodology to assess effectiveness of approach taken in supervising OEs.

h. There is over-reliance on professional bodies for tax advisors to verify fitness and propriety of members and absence of review process to determine fitness and propriety of OEs who are not members of a professional body.

i. With regard to accountants there was no evidence provided to the assessment team to ascertain monitoring the provision of services without prior authorisation. Tax advisors, administration offices, domicile providers and real estate offices are not subject to a specific registration or licensing requirement and not subject to comprehensive monitoring with regard to fitness and propriety.

Sanctions

264. The assessment team has identified **major deficiencies** in the practical application of the Supervision of financial institutions and designated non-financial businesses and professions with **major impact** on the effectiveness, including:

a. Concerns as to whether formal enforcement measures imposed by DNB, AFM and BFT (in particular administration offices) have a deterrent effect across OEs in light of ongoing deficiencies observed relating to WWft violations identified.

b. Concerns about the justification for the use of informal enforcement measures by DNB and AFM; Complexity of administrative decision-making process to impose sanctions may inadvertently favour the use of informal enforcement measures (DNB and AFM).

c. Lack of data collected by supervisors or analysis undertaken to determine whether the sanctions imposed are effective in achieving the desired deterrent effect and level of Wwft compliance.

265. The assessment team has identified **limited deficiencies** in the practical application of the Sanctions requirements with **limited impact** on the effectiveness, including:

a. Lack of supporting mechanism to allow for the publication of notices (BTWwft).

b. Restrictions created by Enforcement Policy prevent Local Bar Presidents from effectively using all available administrative sanctions, commensurate with the violation(s) in question.

c. Lack of appetite within National case coordinating committees to support the pursuit of more formal sanctions for Wwft deficiencies.

CHAPTER 9. Application of national cooperation and coordination requirements (Article 49) (law enforcement agencies excluded)

Status of Transposition

266. There are no issues of completeness of transposition or conformity noted in COM analysis with regard to this Article of the Directive.

Analysis of Application in Practice

Article 49

267. There is a robust framework for domestic cooperation and coordination, with various platforms among competent authorities as well as private public partnerships (e.g., the FINTEL alliance) which are a strength of the Dutch system. The Minister of Finance and the Minister of Justice and Security are responsible for the central management of the prevention and repression of ML and FT. From 2015 onwards the Netherlands has developed a policy cycle in order to ensure a national risk-based AML/CFT policy. The Minister of Finance and the Minister of Justice and Security regularly meet in a Ministerial Committee for ML. In 2019 the Ministerial Committee drew up a joint ML Action Plan, which should help operationalizing the risk-based approach.

268. There are a number of platforms and fora aimed at ensuring domestic cooperation. For example, the Financial Expertise Centre (FEC) is a permanent cooperation between supervisory, financial intelligence, investigative and enforcement agencies (the AFM, the Tax and Customs Administration, DNB, the FIU-NL, the FIOD, the OM and the Netherlands Police; other parties (for example other supervisors) can participate on a project basis. Examples of such projects are those with government authorities on TCSPs, digitisation and virtual assets and cash money, as well as public-private projects on investment fraud, TBML, foundations, corruption and AML related to human beings trafficking and exploitation. The Anti Money Laundering Centre (AMLC) enhances cooperation between partners involved in the criminal prosecution of ML. It is a platform where parties involved share their knowledge and experience and work together on the operational level. The AMLC provides a meeting place for public agencies, but also for non-government partners (domestic and international), such as banks, virtual asset service providers and universities. The AMLC contributes to the formulation of new high-end ML typologies for use in criminal investigations on ML, draws up specific phenomenon descriptions, runs projects, launches major ML investigations and builds and manages unique data availability, for example the AMLC Suite. The iCOV was established in 2013 to link data among public services in order to track criminal and unexplainable assets, uncover ML and fraud arrangements, and collect unpaid government claims.

269. In spite of the extensive cooperation framework, there are a number of issues that could affect both the level of policy-making and the more operational ones. The most significant is related to issues of data ownership and sharing, which have affected the quality of both NRAs (ML and FT). As the protocols in place between the participating institutions of iCOV did not specifically contemplate the exchange of the types of data required for the NRA, for which new consenting procedures had to be put in place. However, these procedures could not be finalized in time and, as a result, sharing of data among the iCOV for the purpose of the NRA was not possible. Other issues related to access to data (e.g., TRACK, on the use of data related to legal entities, see analysis of article 30) are also noted in the NRA.[24] Similar issues were noted in the national assessment of the FT risk.

270. More in general, questions can be raised on the quality of the NRA, which affect the policies and action plan and therefore subsequent cooperation, that should theoretically rely on the findings of the NRA. The NRA is primarily based on experts' judgement and only, to a limited extent, on quantitative data, for the reasons explained above. The analysis remains very high-level, i.e., the analysis of the resilience is almost exclusively based on the existence of a legal

[24] 2019 NRA – Money Laundering, pages 33 and 34.

framework, without taking into thorough account its effective implementation. Participation of stakeholders was limited (e.g., one representative only from the public prosecutor in the ML NRA and no involvement of the secret service in the FT, NRA because of the unavailability of this agency to participate in this exercise) which can undermine the soundness of the findings, particularly as they are based on experts' judgements. Stakeholders were not always fully aware of the findings of the NRA, as their role in it seems to have been more limited to providing the data, rather than in its active analysis, which may have determined "buy-ins" and ownership issues of those assessments' findings and conclusions.

271. It is also noted that some additional areas of concern were identified with respect to the cooperation mechanisms in place. The FEC information platform has seen a gradual reduction in the number of signals reported. At the same time, the signals have become more complex with a corresponding increase in the time needed to generate information about a signal. In some instances, processing time in 2019 was up to 100 days. The reason for this is thus the increasing complexity of the signals received and the analysis required. There is a risk that without sufficient resourcing, the value this initiative provides is declining. Authorities involved with this initiative are aware of these developments and the need for further resourcing.

272. Not all supervisors are members of the mechanisms. For example, the BTWwft is not a member of the FEC, iCOV and RIEC (though some legislative amendments are pending, please see below). It is also understood that the BFT may also not be authorised to participate in all the mechanisms.

273. Reference was made during the assessment to a restriction on the sharing of information within these mechanisms and in general. The sharing of information is only permitted to the extent legally possible. At the FEC for example, signals and responses are shared with all partners as much as possible, "taking into account legal possibilities". Supervisors advised they cannot take action on the basis of this information. It only provides them with indication of where risks may exist in relation to the OEs they supervise. If they wish to act on this information, they must independently seek to obtain it via their own administrative law powers.

274. The Wwft Supervisors Consultation is a regular meeting of all Wwft supervisors in the Netherlands: DNB, the AFM, the BFT, the BTWwft, the Ksa and the local Bar Presidents of the Netherlands Bar. During the meeting, the committee members discuss the interpretation of the law, case studies, cooperation, and the exchange of information. However, it is understood that according to the law local Bar Presidents are not permitted to share information about the OEs they supervise. The sharing of information is only permitted to the extent it involves the FIU if necessary and to the extent the information is useful for the performance of the FIU's statutory duties, with the determination as to its useful being decided by the Bar President. The Bar Presidents also do not participate in other cooperation mechanisms noted above for similar reasons.

Compensatory Measures and Detrimental Factors

275. Not applicable.

Conclusions (national cooperation and coordination)

276. The assessment team has identified **major deficiencies** in the practical application of national cooperation and coordination, having a **limited impact** by affecting national cooperation and coordination as follows:

    a. Issues of data ownership, having affected the sharing of information (for the purpose of the NRA, FIU access to information), have repercussions on the understanding of risks and developing of a response to ML/FT risks at policy level.

    b. The effectiveness of the various cooperation initiatives in place is impacted by limitations in their composition and information sharing arrangements.

    c. Limited role of stakeholders in assessing risk (top-down approach instead of bottom-up, resulting in risks of lack of ownership of findings of risks assessments).

CHAPTER 10. Application of measures for international cooperation (Articles 52-57, 45.4, 48.4, 48.5 and 58.5)

Status of Transposition

277. The analysis of COM does not note any issue of conformity or transposition with regard to these Articles. However, the evaluation team notes that Article 52, para 2, which provides that the FIU to whom a request of assistance is made "is required to use the whole range of its available powers which it would normally use domestically" cannot be considered implemented, as the power of the FIU to request additional information to OEs (including those that may have not filed a UTR) cannot be used in the context if a request of international cooperation (see Article 17, which sets this power, but limits it only to the circumstances envisaged by Article 13, lett. a and b – receipt and analysis of inf, and not to Article 13a, which regulates international cooperation).

Analysis of Application in Practice

Sub-theme (a): International cooperation between FIUs

Articles 52 and 57

278. There are no limitations in the exchange of information that stem from the nature of the foreign FIU and no restrictions for cooperation with FIUs with a different organisational status. FIU-NL cooperates with foreign FIUs regardless of their organizational status and has provided several examples of good cooperation with different types of FIUs (including of administrative nature).

Article 53

279. The FIU exchanges information with foreign counterparts spontaneously or upon request. The FIU-NL can provide information related to ML even if the exact predicate offence has not been identified at the time of the request for assistance by another FIU. Based on information provided from the authorities, there were no cases where cooperation has been refused.

280. There are issues in the legal framework which affect the ability of the FIU-NL to use the same powers which it would normally use domestically for receiving and analysing information pursuant to a foreign FIU's request of assistance; and in particular:

    a. The FIU-NL has no power to request information it has no direct access to other competent authorities and has confirmed that it cannot request it also in the case of a request of international cooperation;

    b. The FIU-NL has no explicit power to request OEs information pursuant to a request of a foreign FIU; as Article 13a (which entitles the FIU to exchange information with its foreign counterparts) is not among the provisions referred to in Article 17 (which sets the tasks for which the FIU-NL can request additional information to OEs, i.e., those in Article 13 points a) and b) only.

    c. The FIU-NL has no power to postpone or block a transaction (therefore it cannot act in the case in which the request to postpone or block comes from a foreign counterparts).

281. The authorities have explained that if a transactions and underlying funds need to be blocked, they can ask the prosecution service to seize the funds (however a founded suspicion is required for the request). Authorities also explained that a request from a foreign FIU that requires obtaining additional information can be treated as a domestic UTR (which would enable them to request additional information from an OE), although the legal basis of this approach is not entirely clear. The FIU-NL does not maintain statistics on the number of foreign requests that have been responded including by obtaining additional information from OEs, however they did indicate that during the period 13-07-2021 to 13-09-2021 FIU-NL out of 341 requests for additional information to OEs, 37 were based on requests from foreign FIUs.

Article 54 and Article 55

282. The assessment team has not identified any deficiencies in the application of the respective articles, which are deemed to be implemented effectively. The FIU-NL may disclose the information received from foreign counterparts only with their prior consent.

Article 56

283. The assessment team has not identified any deficiencies related to the use of protected channels for communication. FIU-NL uses the Egmont Secure Web (ESW) and the FIU.net as the only channels for secure exchange of information with counterpart FIUs.

Sub-theme (b): International cooperation between supervisors

Articles 45.4

284. No instances were reported to the assessment team where the Netherlands has been required to make such a notification. There is evidence of strong, positive dialogue between the Netherlands various enforcement bodies and supervisors and European authorities. There is evidence of positive dialogue between the various enforcement bodies and supervisors and European authorities.

Article 48.4

285. The Netherlands prioritises international cooperation and has mechanisms in place to ensure international cooperation for AML/CFT supervisory purposes. As regards measures involving OEs located in the Netherlands and with operations in another Member State, the DNB works closely and cooperates with the European Central Bank and with other national bodies. The DNB engages in regular interaction with various supervisors of Member States both on an informal level and in the exchange of supervisory information related to AML/CFT compliance about OEs.

286. Information is provided with the notice given to the DNB or AFM when an OE passports into the Netherlands. This includes information about their AML/CFT compliance. This information is provided by the DNB or AFM when an OE they oversee passports into other Member State. This makes the effective supervision of OEs critically important in sectors where passporting is possible as Member States will rely on the DNB or AFM to be effectively supervising the home OE. The concerns raised regarding the supervisory approach and sanctions activity of the AFM impacts upon the reliability of data it provides to Member States about an OE's compliance with the Wwft.

Article 48.5

287. The Netherlands has several mechanisms that enables its policy makers, the FIUs, supervisors and other competent authorities involved in AML/CFT to cooperate and coordinate domestically concerning the development and implementation of policies and activities to combat ML and FT. Some areas of concern, however, were identified with respect to these mechanisms which would have repercussions on obtaining relevant information necessary in the context of international cooperation (please refer also to the section on national cooperation).

288. Several mechanisms involve the sharing of information about actors or cases involving ML/FT or other financial crime. However, the information cannot be shared further outside of these mechanisms without the express consent of the party who has shared it. It is unclear whether this requirement impedes the timeliness or extent to which information concerning signals or incidents can be shared between supervisors and/or other authorities. It is also unclear what criteria must be met for consent to be granted and whether this is also an impediment.

289. The exclusion of some supervisors from the cooperation mechanisms at national level limits their access to signals relevant to the risks identified in the NRA that may be associated with the OEs they supervise. It also prevents participants from receiving information from these supervisors to ensure a complete view about possible signals and emerging risks are understood. It is noted that the local Bar Presidents are not permitted to share information about the OEs they supervise. The Bar Presidents also do not participate in other cooperation mechanisms noted above for similar reasons.

290. Reference was made during the assessment to a restriction on the sharing of information within these mechanisms and in general. The sharing of information is only permitted to the extent legally possible. At the FEC for example, signals and responses are shared with all partners as much as possible, "taking into account legal possibilities". Supervisors advised they cannot take action on the basis of this information. It only provides them with indication of where risks may exist in relation to the OEs they supervise. If they wish to act on this information, they must independently seek to obtain it via their own administrative law powers. This applies not only to use of information for supervisory purposes but also enforcement. The ability to act quickly in response to signals is greatly compromised in

requiring supervisors to, in effect, re-investigate the same signal, before it can initiate any supervisory response.

Article 58.5[25]

291. In the Netherlands, authorities exercise their power to impose administrative sanctions and measures in accordance with the relevant AML/CFT laws directly and in collaboration with other authorities. They endeavour to cooperate closely to ensure those administrative sanctions or measures produce the desired results and coordinate their action, however limited information was provided with regard to cross-border cases, with the exception of DNB. There were several case examples demonstrating the relevant and extensive cooperation and exchange of information by the DNB mainly with regard to the supervision of PSPs in the cross-border context, including cases of revoked licences.

292. Nevertheless, no information was provided with regard to the relevant exchange conducted by other supervisors and no statistics were provided by the authorities with regard to the cases of coordination of sanctioning in cross-border cases. This is of a particular concern in view of the overall international exposure of the Netherlands.

293. Local Bar Presidents are restricted by their duties of confidentiality to share information received about OEs they supervise regarding their Wwft compliance. The sharing of information is only permitted to the extent it involves the FIU if necessary and to the extent the information is useful for the performance of the FIU's statutory duties, with the determination as to its useful being decided by the Dean. This may also restrict their ability to share information relevant to other Netherland AML/CTT supervisors and for cross border investigations. It is unclear whether steps have been taken to address this restriction.

Compensatory Measures and Detrimental Factors

294. Some of the issues noted in the legal framework concerning the implementation of Article 53 (e.g., the lack of a specific power to request additional information to OEs in the case of a foreign FIU's request) are partly compensated in the practice of the FIU-NL.

295. Some of the issues noted with regards to limitations concerning passporting information are to be compensated by the introduction of AML/CFT colleges in 2021 to specifically include the supervision of such entities.

Conclusions

International Cooperation between FIUs

296. The assessment team has identified **limited deficiencies** in the practical application of the international cooperation between FIUs, with **limited impact**, as follows.

[25] 4th AMLD: In the exercise of their powers to impose administrative sanctions and measures, competent authorities shall cooperate closely in order to ensure that those administrative sanctions or measures produce the desired results and coordinate their action when dealing with cross-border cases.

a. The information the FIU can obtain information from domestic counterparts, if such information is needed to process a request from a foreign FIU, is limited to those instances where the FIU has direct access to the requested information.

b. The FIU has no power to stop or postpone a transaction on its own which has repercussions on the effectiveness of cooperating with foreign FIUs to postpone operations.

International Cooperation between Supervisors

297. The assessment team has identified **limited deficiencies** in the practical application of the cooperation between supervisors with **limited impact** on the effectiveness, as follows:

c. The limited participation of the BFT and the local Bar Presidents in collaboration and information sharing mechanisms limits affects the effectiveness of information-sharing in cross-border cases with regard to OEs under their supervision.

d. Restrictions on the sharing and use of information at national level may impede supervisors' abilities to react quickly to international cases.

e. Not demonstrated cooperation with regard to ensuring the effect of sanctions and administrative measures in cross-border cases, with the exception of DNB.

f. Cascading effect of supervisory approach and sanctioning policy of the AFM impacts upon the completeness of data provided to other Member States about an OE's compliance with the Wwft.

CHAPTER 11. Overall Level of Practical Application and Impact

The summary table of effective application of the respective provisions of the 4th AMLD aims to reflect on any potential or determined significant impact for the Member State and at the supranational level of the European Union. Any further horizontal issues could be noted here as well.

4th AMLD Themes	Deficiencies	Impact Areas
Risk assessment, internal controls and group policies	Major	Major impact related to uneven implementation and limited guidance and feedback in conjunction with the international exposure of the country
CDD	Major-Limited	Major in view of limited application of some CDD measures by certain sectors highly relevant from ML/FT risk perspective (tax advisors, real estate agents, payment service providers)
CDD for PEPs	Limited	Major in view of the international exposure of the country
CDD related to performance by third parties	Limited	Limited
Transparency of BO	Major	Major in view of some concerns on the accuracy and availability of data in conjunction with some difficulties encountered by OEs with regard to BO identification of complex structures
Functioning of the FIU	Major	Limited mainly related to the limited access to certain types of information and not fully demonstrated results regarding the outcome of analysis
Suspicious transaction reporting	Major	Major in view of the underreporting and concerns about the quality and relevance of significant part of reports
Data protection and record-retention	Limited	Limited

Supervision	Major	Major related to limited fit and proper assessment for a large segment of DNFBPs as well as issues related to the risk assessment and impact of supervision of major categories of OEs
Sanctions	Major	Major as the dissuasiveness and proportionality was not demonstrated with regard to large segments of the FIs and DNFBPs
National cooperation and coordination	Major	Limited impact in view of the number of information sharing and coordination arrangements
International cooperation between FIUs	Limited	Limited
International cooperation between supervisors	Limited	Limited

ANNEX 1: STATISTICAL INFORMATION

Table 1. The categories of information the FIU receives other than STRs (pursuant to Article 32.3)

Type of information available or submitted to the FIU	Entity providing the information	Can trigger operational analysis? (Y/N)	2018		2019		2020	
			Number	Total Amount (EUR)	Number	Total Amount (EUR)	Number	Total Amount (EUR)
Unusual transaction reports (please specify any subcategory and provide statistics)	**Obliged entities** *(all)*		**753.352**		**2.462.973**		**722.247**	
	Authorities *(please specify)*							
Large value or threshold transaction reports *(please specify any subcategory and provide statistics)*	**Obliged entities** *(all)*		**112.8282**		**211.148**		**304.811**	
	Authorities *(please specify)*							
Cash transaction reports *(please specify any subcategory and provide statistics)*	**Obliged entities** *(all)*		**12.454**		**13.980**		**9474**	
	Authorities (please specify)							

Cross-border transportation of currency and bearer instruments	*Cash-entry - Customs*		**2147**		**2042**		**896**	
	Cash entry - other		**19**		**20**		**9**	
	Cash transit-customs		**852**		**835**		**487**	
	Cash exit - customs		**3953**		**3599**		**2267**	
	Cash exit – other		**19**		**21**		**2267**	
	Customs - cargo		**4**		**1**		**0**	
Cross-border reports received pursuant to Article 53, paragraph 1, subparagraph 3	*(please specify any subcategory and provide statistics)*							
Others *(please specify and add further rows as applicable)*	**Obliged entities** *(all)*		**284**		**167**		**131**	
	Authorities *(please specify)*							

Table 2: Number of STRs per reporting year and per possible type of offence (own investigation and LOvJ-requests)

Type of offence[1]	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**Total**
ML	8.371	12.916	15.195	20.939	19.871	54.231	131.523
Terrorism/Sanctions Act	1.323	3.237	2.204	2.788	2.101	3.601	15.254
Fraud	3.888	8.304	3.508	1.583	2.121	5.964	25.368
Hard drugs	1.713	3.626	2.540	1.479	1.585	578	11.521

Other[1]	1936	640	828	329	145	698	4.576
Soft drugs	479	795	937	509	228	77	3025
Human trafficking/smuggling	3332	3874	1329	2462	4012	875	15.884
Murder/homicide	981	987	635	400	199	170	3372
Corruption	15	141	407	6.194	316	9.432	16.505
Weapon trade	69	155	360	101	351	447	1483
Synthetic drugs	97	580	213	54	111	373	1428
Cybercrime	161	5	7	11	2	33	219
Child porn	193	388	27	284	1.200	1.640	3.732

Table 3: Predicate offences that are associated with the STR-case files

Type of obliged entities	**2018**	**2019**	**2020**
	Total	**Total**	**Total**
Money laundering[26]	1,469	1,790	6,601
Terrorism/Sanctions Act[27]	560	429	408
Fraud	267	195	1,219
Hard drugs	129	121	25
Other[28]	70	13	122
Soft drugs	58	32	11

26 A transaction of which the etity has reason to believe it might be related to ML or FT. Since Dutch law requires no particular predicate offence in order to ascertain a case of ML, any predicate offence can be reported as such. Obliged entities are therefore legally required to report any unusual transaction relating to any predicate offence, ML or FT.

27 This figure is a grand total of the number of files FIU-NL investigated on Counter Terrorism and Terrorism Financing and Terrorism Sanctions indications. Not for all cases the relation to terrorism was found. In these cases the files were declared suspicious (STRs) on other criminal offences, for example trafficking in, or possession of fire arms, fraud or people smuggling. This is an example of the close nexus between Terrorism and Crime.

28 Others can include crimes such as; violence, robberies, burglaries, environment and street robbery

Smuggling/Human trafficking	100	70	50
Murder/Homicide	26	26	13
Corruption	43	62	87
Arms trading	16	130[29]	90
Synthetic Drugs	6	8	5
Cybercrime	3	1	1
Child pornography	13	5	8
Total	*2,760*	*2,883*	*8,639*

Table 4. Supervision of Payment Service Providers

Type of obliged entities	**Money Remittance**			**Payment Service Providers**		
Years	**2018**	**2019**	**2020**	**2018**	**2019**	**2020**
Responsible Supervisor(s) *(please use abbreviations)*	**DNB**	**DNB**	**DNB**	**DNB**	**DNB**	**DNB**
Total number of obliged entities	8 (providers)	9 (providers)	8 (providers) 860 (agents)	30	41	67

29 Experiences during previous years show a high result of STRs on arms trading in 2019. Within the framework of the activities in the FT-Platform (see IO9), new fire arms dealers were discovered and the results are shown in this figure. Most purchases of illicit firearms by terrorism resemble those that take place in the criminal world. Most financial transactions regarding the procurement of illegal firearms are transactions in cash, or purchases on the DarkWeb with cryptocurrencies. Not all fire arm purchases could be linked to terrorists. A small number was linked to Jihadi groups and individuals linked to extremist right-wing groups.

Full scope AML/CFT on-site inspections conducted	**3**	**5**	**3**	**4**	**2**	**2**
Targeted / Themed AML/CFT on-site inspections conducted	2	0	1	2	1	4
Total number of AML/CFT on-site inspections conducted	**5**	**5**	**4**	**6**	**3**	**6**
Number of separate AML/CFT specific on-site inspections conducted	**5**	**5**	**4**	**6**	**3**	**6**
Number of AML/CFT combined with other prudential supervision on-site inspections	**0**	**0**	**0**	**0**	**0**	**0**
Number of joint inspections with other domestic supervisors/other authorities *(if applicable)*	**0**	**0**	**0**	**0**	**0**	**0**
Number of joint/coordinated inspections with other MS supervisors	**0**	**0**	**0**	**0**	**0**	**0**
Responsible Supervisor(s) *(please use abbreviations)*	**DNB**	**DNB**	**DNB**	**DNB**	**DNB**	**DNB**
Full scope AML/CFT off-site inspections conducted	**1**	**1**	**1**	**1**	**2**	**1**
Targeted / Themed AML/CFT off-site inspections conducted	2	0	2	1	**0**	46
Total number of AML/CFT off-site inspections conducted	**3**	1	3	1	2	47
Number of AML/CFT specific off-site inspections conducted	**3**	1	3	1	2	47
Number of AML/CFT combined with other supervision off-site inspections	0	0	0	0	0	0
Number of joint inspections with other domestic supervisors/other authorities *(if applicable)*	0	0	0	0	0	0
Number of joint/coordinated inspections with other MS supervisors	0	0	0	0	0	0
Number of inspections having identified AML/CFT infringements	**5**	**5**	**6**	**8**	**6**	**20**

Table 5: Sanctions imposed by BTWwft (real estate, traders in goods, domicile providers)

Real estate agents	**2018**	**2019**	**2020**
Total number of administrative and criminal sanctions and measures applied	31	12	2
Fines	18	10	1

Other persons trading in goods (art. 2.1.3.e)	**2018**	**2019**	**2020**
Infringements STR reporting	180	788 Correct figure is 792)	520 Correct figure is 521
Total number of administrative and criminal sanctions and measures applied	30	30	7
Fines (Art. 59.2.e)	19	14	4

Domicile providers	**2018**	**2019**	**2020**
Fines (Art. 59.2.e)	0	3	1

Table 6: Number of breaches per category/theme included in the AML legislation (Wwft) (per sector/profession, over the period 2015-2020) and sanctions imposed

	CDD - KYC (art. 3 lid 2)					
Per FI/DNFBP	2015	2016	2017	2018	2019	2020
Notaries	2	8	9	9	7	5
External accountants/ auditors	12	5	2	2	4	3
Tax advisors	20	12	27	29	29	33
Total	**34**	**25**	**38**	**40**	**40**	**41**

	CDD - UBO (art. 3 lid 2 onder b)					
Per FI/DNFBP	2015	2016	2017	2018	2019	2020
Notaries	0	0	1	0	0	1
External accountants/ auditors	0	0	0	0	2	0
Tax advisors	0	0	1	2	2	0
Total	**0**	**0**	**2**	**2**	**4**	**1**

	Monitoring of transactions (art. 3 lid 2 onder d)					
Per FI/DNFBP	2015	2016	2017	2018	2019	2020
Notaries	0	5	3	3	4	1
External accountants/ auditors	3	4	1	3	3	3
Tax advisors	2	2	13	20	19	27
Total	**5**	**11**	**17**	**26**	**26**	**31**

	STR filing obligation (art. 16) (objective)					
Per FI/DNFBP	2015	2016	2017	2018	2019	2020
Notaries	0	0	0	0	0	0
External accountants/ auditors	0	0	0	0	0	0
Tax advisors	0	0	0	0	0	0
Total	**0**	**0**	**0**	**0**	**0**	**0**

	STR filing obligation (art. 16) (subjective)					
Per FI/DNFBP	2015	2016	2017	2018	2019	2020
Notaries	2	8	8	9	3	5
External accountants/ auditors	8	6	1	4	4	1
Tax advisors	16	6	21	21	20	16
Total	**26**	**20**	**30**	**34**	**27**	**22**

	Record keeping (art. 33)					
Per FI/DNFBP	2015	2016	2017	2018	2019	2020
Notaries	0	1	2	3	1	0
External accountants/ auditors	3	0	0	0	1	0
Tax advisors	1	3	6	13	11	16
Total	**4**	**4**	**8**	**16**	**13**	**16**

	# shortcomings internal controls (art. 2b)					
Per FI/DNFBP	2015	2016	2017	2018	2019	2020
Notaries	0	0	0	0	2	1
External accountants/ auditors	0	0	0	0	1	1
Tax advisors	0	0	0	0	22	29
Total	**0**	**0**	**0**	**0**	**25**	**31**

	# shortcomings group policy (art. 2a)					
Per FI/DNFBP	2015	2016	2017	2018	2019	2020
Notaries	0	0	0	0	3	1
External accountants/ auditors	0	0	0	0	0	0
Tax advisors	0	0	0	0	24	25
Total	**0**	**0**	**0**	**0**	**27**	**26**

	Cease-and-desist orders per sector			
	Civil-law notaries	External accountants/auditors	Tax advisors	**Total**
2015				**8**
2016	-	**4**	**7**	**11**
2017	-	-	**7**	**7**
2018	-	2	6	**8**
2019	-	-	13	**13**
2020	-	-	**4**	**4**
Total	**-**	**6**	**33**	**51**

	Performance improvement plans per sector			
	Civil-law notaries	External accountants/auditors	Tax advisors	**Total**
2015	-	31	-	**31**
2016	-	17	3	**20**
2017	1	-	11	**12**
2018	-	21	-	**21**
2019	1	2	19	**22**
2020	-	-	18	**18**
Total	**2**	**71**	**51**	**124**

	Warning notices per sector			
	Civil-law notaries	External accountants/auditors	Tax advisors	**Total**
2015	-	9	6	**15**
2016	1	3	1	**5**
2017	2	**4**	9	**15**
2018	3	14	-	**17**
2019	-	2	9	**11**
2020	-	2	9	**11**
Total	**6**	**34**	**34**	**74**

	Number and amount of fines imposed by the BFT per sector											
	Civil-law notaries			External accountants/auditors			Tax advisors			Total		
	Total #	Total €	Avg € per fine	Total #	Total €	Avg € per fine	Total #	Total €	Avg € per fine	**Total #**	**Total €**	**Avg € per fine**
2015	-	-	-	8	44.975	5.622	10	32.250	3.225	**18**	**77.225**	**4.290**
2016	1	10.000	10.000	23	175.140	7.615	3	36.980	12.327	**27**	**222.120**	**8.227**
2017	1	6.000	6.000	6	126.222	21.037	7	19.500	2.786	**14**	**151.722**	**10.837**
2018	2	51.000	25.500	16	146.133	9.133	1	45.000	45.000	**19**	**242.133**	**12.744**
2019	1	8.500	8.500	20	212.995	10.650	-	-	-	**21**	**221.495**	**10.547**
2020	3	129.300	43.100	-	-	-	11	69.990	6.363	**14**	**199.290**	**14.235**
Total	**8**	**204.800**	**25.600**	**73**	**705.465**	**9.664**	**32**	**203.720**	**6.366**	**113**	**1.113.985**	**9.858**

ANNEX 2: AGENDA OF THE ON-LINE ASSESSMENT, THE NETHERLANDS, SEPTEMBER 2021

European Union - Council of Europe Assessment of the Concrete Implementation and Effective Application of the Fourth Money Laundering Directive (4th AMLD) in the Netherlands

and

European Banking Authority's AML/CFT implementation review of De Nederlandsche Bank approach to the AML/CFT supervision of banks

Online Assessment

Day 1 – 20 September 2021	
	Joint Meeting: Council of Europe and European Banking Authority
09:00 – 10:15	**Opening Meeting: Introduction of the Council of Europe and European Banking Authority Reviews, National Cooperation in the AML/CFT area** *Participants:* Representatives of the Ministry of Finance and Ministry of Justice and Security, Ministerial Committee for ML (if relevant), Financial Expertise Centre (FEC), Anti Money Laundering Centre (AMLC), Joint Counter-Terrorism Committee (GCT)
10:20 – 13:00	**Overview of DNB approach to AML/CFT (banks)** *Participants:* head(s) of AML/CFT team(s), head of AML/CFT supervision; staff responsible for supervision of banks; staff responsible for sanctions *Themes:* Supervision of financial institutions, including recent reforms, organisation, resources, understanding of risks, guidance, supervisory procedures and application of RBA, off-site and on-site supervision (Articles 47-48) Sanctions on financial institutions (Articles 58-59) International cooperation between supervisors (Articles 45.4, 48.4, 48.5 and 58.5) Transparency of BO (Articles 30 and 31) National cooperation (Article 49)
Lunch Break **13:00 – 14:00**	
Council of Europe	**European Banking Authority**

14:00 – 15:15	**FI 1** *Themes:* • Risk assessment, internal control and group policies (Articles 8, 45, 46) • General customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3) • CDD for PEPs (Articles 20-23) • CDD related to performance by third parties (Articles 25, 26, 27, 28, 29) • Cooperation with FIU (Article 32) • Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) • Data protection and record-retention (Article 40) (AML relevance) • Supervision and sanctions (Articles 47-48, 58-59)	14:30 – 17:30 *(short coffee break at 16:00)*	**ML/FT Risk Assessment** *Participants:* head of AML/CFT supervision; head(s) of other team(s) as appropriate; staff in charge of carrying out risk assessments
15:25 – 16:40	**FI 2** *Themes:* • Risk assessment, internal control and group policies (Articles 8, 45, 46) • General customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3) • CDD for PEPs (Articles 20-23) • CDD related to performance by third parties (Articles 25, 26, 27, 28, 29) • Cooperation with FIU (Article 32) • Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) • Data protection and record-retention (Article 40) (AML relevance) • Supervision and sanctions (Articles 47-48, 58-59)		
16:50 – 17:50	**Transparency of beneficial ownership:** **Economic Enforcement Bureau of the Tax and Customs Administration** **Chamber of Commerce (verification of discrepancies)** **Other authorities responsible for verification and sanctioning (if applicable)**		

	Participants: representatives of authorities responsible for enforcement of the BO register requirements *Themes:* Transparency of BO (Articles 30 and 31)		

Day 2 – 21 September 2021			
	Joint Meeting: Council of Europe and European Banking Authority		
08:45 – 09:45	**ML/FT risk, national cooperation and coordination and cooperation of the FIU-NL for AML/CFT supervisory purposes** *Participants:* representatives of the Dutch Financial Intelligence Unit (FIU-NL), including FIU representatives responsible for coordination within FEC, AMLC and GCT *Themes:* - ML/FT risks - Contextual factors - National cooperation (Article 49)		
Council of Europe		**European Banking Authority**	
09:55 – 12:15	**Dutch Financial Intelligence Unit (FIU-NL)** *Themes:* - Financial Intelligence (Article 32) - Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) - International cooperation between FIUs (Articles 52-57)	10:15 – 13:00 (short coffee break at 11:30)	**AML/CFT supervision: supervisory practices and allocation of resources** *Participants:* head of AML/CFT supervision; head(s) of other team(s) as appropriate; AML/CFT onsite and offsite supervisors
12:25 – 13:25	**Supervision of legal professionals: NOvA** *Participants:* staff responsible for market entry and fit and proper checks; staff responsible for supervision; staff responsible for sanctions *Themes:* - Supervision (Articles 47-48) - Sanctions (Articles 58-59) - International cooperation between supervisors (Articles 45.4, 48.4, 48.5 and 58.5) - Transparency of BO (Articles 30 and 31)		
Lunch Break **13:25 – 14:30**			
Council of Europe		**European Banking Authority**	

14:30 – 15:45	**FI 3** *Themes:* - Risk assessment, internal control and group policies (Articles 8, 45, 46) - General customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3) - CDD for PEPs (Articles 20-23) - CDD related to performance by third parties (Articles 25, 26, 27, 28, 29) - Cooperation with FIU (Article 32) - Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) - Data protection and record-retention (Article 40) (AML relevance) - Supervision and sanctions (Articles 47-48, 58-59)	14:30 – 15:30	**Supervisory guidance** *Participants:* head of AML/CFT supervision team; head(s) of other team(s) as appropriate; staff in charge of issuing guidance
		15:45-17:00	**Sanctions / administrative measures** *Participant(s):* head(s) of legal/enforcement team(s); head(s) of other team(s) as appropriate
15:55 – 17:10	**Supervision of Trust Offices and Domicile Providers: DNB and Tax and Customs Administration AML/CFT Supervision Office (BTWwft)** *Participants:* staff responsible for market entry and fit and proper checks; staff responsible for supervision; staff responsible for sanctions *Themes:* - Supervision (Articles 47-48) - Sanctions (Articles 58-59) - International cooperation between supervisors (Articles 45.4, 48.4, 48.5 and 58.5) - Transparency of BO (Articles 30 and 31)		
17:20 – 18:00	**Market entry of civil notaries, accountants/auditors and tax advisors** **KNB, NBA, NOB, RB** *Participants:* staff responsible for market entry and fit and proper checks *Themes:* - Supervision (Article 47) - Sanctions (Articles 58-59) – if applicable		

Day 3 – 22 September 2021			
Council of Europe		**European Banking Authority**	
09:00 – 10:15	**Trust Offices and Domicile Providers –** Suggested: 3 trust offices and 1 domicile provider	09:30 – 10:30 and	**Meetings with banks**

	Themes: - Risk assessment, internal control and group policies (Articles 8, 45, 46) - General customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3) - CDD for PEPs (Articles 20-23) - CDD related to performance by third parties (Articles 25, 26, 27, 28, 29) - Cooperation with FIU (Article 32) - Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) - Data protection and record-retention (Article 40) (AML relevance) - Supervision and sanctions (Articles 47-48, 58-59) - Transparency of BO (Articles 30 and 31)	11:00 – 12:00	
10:25 – 11:25	**Legal Professionals: Lawyers and Legal Advisors** Suggested: 3 lawyers (at least one independent/not part of a law company) and 2 legal advisors - Risk assessment, internal control and group policies (Articles 8, 45, 46) - General customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3) - CDD for PEPs (Articles 20-23) - CDD related to performance by third parties (Articles 25, 26, 27, 28, 29) - Cooperation with FIU (Article 32) - Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) - Data protection and record-retention (Article 40) (AML relevance) - Supervision and sanctions (Articles 47-48, 58-59) - Transparency of BO (Articles 30 and 31)		
11:35 – 12:20	**Supervision of Real Estate and High-Value Goods Dealers: Tax and Customs Administration AML/CFT Supervision Office (BTWwft)** *Participants:* staff responsible for market entry and fit and proper checks (if applicable); staff responsible for supervision; staff responsible for sanctions *Themes:* - Supervision (Articles 47-48) - Sanctions (Articles 58-59) - International cooperation between supervisors (Articles 45.4, 48.4, 48.5 and 58.5) - Transparency of BO (Articles 30 and 31)	**12:30 – 13:30**	**Prudential supervision and ML/FT risks** *Participants:* head of banking supervision; head(s) or other team(s) as appropriate; line supervisors
Lunch Break			

12:20 – 13:20/ 13:30 – 14:30 (EBA)			
13:20 – 14:50	**Supervision of Notaries, Accountants, Tax Advisors, Legal Advisors, Administration Offices:** **Financial Supervision Office (BFT)** *Participants:* staff responsible for supervision; staff responsible for sanctions *Themes:* - Supervision (Articles 47-48) - Sanctions (Articles 58-59) - International cooperation between supervisors (Articles 45.4, 48.4, 48.5 and 58.5) - Transparency of BO (Articles 30 and 31)		
15:00 – 16:00	**Legal professionals: Notaries and Notary Firms** Suggested: 2 notaries and representatives of 2 notary firms - Risk assessment, internal control and group policies (Articles 8, 45, 46) - General customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3) - CDD for PEPs (Articles 20-23) - CDD related to performance by third parties (Articles 25, 26, 27, 28, 29) - Cooperation with FIU (Article 32) - Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) - Data protection and record-retention (Article 40) (AML relevance) - Supervision and sanctions (Articles 47-48, 58-59) - Transparency of BO (Articles 30 and 31)	15:00 – 16:00	**Authorisations and assessments of KFH/QH** *Participants:* head of authorisation team; head(s) of other teams as appropriate; authorisations staff
16:10 - 17:10	**FI 4** *Themes:* - Risk assessment, internal control and group policies (Articles 8, 45, 46) - General customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3) - CDD for PEPs (Articles 20-23) - CDD related to performance by third parties (Articles 25, 26, 27, 28, 29) - Cooperation with FIU (Article 32) - Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) - Data protection and record-retention (Article 40) (AML relevance) - Supervision and sanctions (Articles 47-48, 58-59)		
		16:30 – 17:30	**Cooperation (domestic and international)** *Participants:* head(s) of legal/enforcement department(s), head(s) of banking supervision and AML/CFT supervision; head(s) of other team(s) as appropriate
17:20 – 18:00	**Supervision of PSPs (including money remittance/e-money) and currency exchange:**		

	DNB *Participants:* staff responsible for market entry and fit and proper checks (currency exchange); staff responsible for supervision (PSPs and currency exchange); staff responsible for sanctions (PSPs and currency exchange) *Themes:* - Supervision (Articles 47-48) - Sanctions (Articles 58-59) - International cooperation between supervisors (Articles 45.4, 48.4, 48.5 and 58.5) - Transparency of BO (Articles 30 and 31)		

Day 4 – 23 September 2021			
	Joint Meeting: Council of Europe and European Banking Authority		
09:00 – 10:30	**FI 5** *Themes:* - Risk assessment, internal control and group policies (Articles 8, 45, 46) - General customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3) - CDD for PEPs (Articles 20-23) - CDD related to performance by third parties (Articles 25, 26, 27, 28, 29) - Cooperation with FIU (Article 32) - Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) - Data protection and record-retention (Article 40) (AML relevance) - Supervision and sanctions (Articles 47-48, 58-59)		
	Council of Europe		**European Banking Authority**
10:40 – 12:00	**Accountants, tax advisors and administration offices** Suggested: 2 accountants, 2 tax advisors, 1 administration office *Themes:* - Risk assessment, internal control and group policies (Articles 8, 45, 46) - General customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3) - CDD for PEPs (Articles 20-23) - CDD related to performance by third parties (Articles 25, 26, 27, 28, 29) - Cooperation with FIU (Article 32)	10:00 – 10:30	**Training**

	- Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) - Data protection and record-retention (Article 40) (AML relevance) - Supervision and sanctions (Articles 47-48, 58-59) - Transparency of BO (Articles 30 and 31)		
12:10 – 13:10	**Supervision of Investment Firms and Asset Management: AFM** *Participants:* staff responsible for supervision; staff responsible for sanctions *Themes:* - Supervision (Articles 47-48) - Sanctions (Articles 58-59) - International cooperation between supervisors (Articles 45.4, 48.4, 48.5 and 58.5) - Transparency of BO (Articles 30 and 31)	**10:30 – 13:00**	**Placeholder – please keep free for potential additional meetings**
Lunch Break 13:10 – 14:10			
14:10 – 15:10	**Representatives of 2 asset management and 2 investment firms** (including 1 large and 1 small firm in each category, predominantly with non-resident clients) *Themes*: - Risk assessment, internal control and group policies (Articles 8, 45, 46) - General customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3) - CDD for PEPs (Articles 20-23) - CDD related to performance by third parties (Articles 25, 26, 27, 28, 29) - Cooperation with FIU (Article 32) - Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) - Data protection and record-retention (Article 40) (AML relevance) - Supervision and sanctions (Articles 47-48, 58-59) - Transparency of BO (Articles 30 and 31)	14:15 – 15:00	**Placeholder**
15:20 – 16:20	**FI 6** *Themes:* • Risk assessment, internal control and group policies (Articles 8, 45, 46) • General customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3)		

	• CDD for PEPs (Articles 20-23) • CDD related to performance by third parties (Articles 25, 26, 27, 28, 29) • Cooperation with FIU (Article 32) • Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) • Data protection and record-retention (Article 40) (AML relevance) • Supervision and sanctions (Articles 47-48, 58-59)		
16:30 – 17:10	**Meeting with payment service providers (PSPs)** Ant Group (which operates as Alibaba) and Adyen *Themes:* • Risk assessment, internal control and group policies (Articles 8, 45, 46) • General customer due diligence (CDD) (Articles 13.1, 14, 18.1-18.3) • CDD for PEPs (Articles 20-23) • CDD related to performance by third parties (Articles 25, 26, 27, 28, 29) • Cooperation with FIU (Article 32) • Suspicious transaction and other reporting (Articles 33, 34, 35, 36, 46.2) • Data protection and record-retention (Article 40) (AML relevance) • Supervision and sanctions (Articles 47-48, 58-59)		
17:20 – 17:30	**Coordination meeting: EBA and the Council of Europe teams**		
17:30 – 17:40	**Closing Meeting** *Participants:* Ministry of Finance and Ministry of Justice and Security, DNB, FIU-NL, other authorities (if relevant) EBA and Council of Europe Assessment teams		