Wetenschappelijk Onderzoek- en Documentatiecentrum

2020-11a Report

Dutch National Risk Assessment on Money Laundering 2019

H.C.J. van der Veen
L.F. Heuts

With the cooperation of
E.C. Leertouwer

Cahier
The 'Cahier' series comprises concise reports of research conducted by and/or on behalf of the WODC. Inclusion in the series does not mean that the contents reflect the point of view of the Dutch Minister of Justice and Security.

Contents

Abbreviations — 5

Summary — 7

1 Introduction — 16
1.1 Reason for the study — 16
1.2 What is money laundering? — 17
1.3 Research objective and questions — 18
1.4 Lessons from the first Money Laundering NRA — 19
1.5 Reading guide — 20

2 Research methodology — 22
2.1 Key concepts of the NRA — 22
2.2 Performing the NRA in accordance with the ISO 31000 framework — 23
2.3 Methods used — 24

3 What makes the Netherlands vulnerable to money laundering? — 35
3.1 Geographic and demographic characteristics — 35
3.2 Sociocultural characteristics — 36
3.3 Economic characteristics — 37
3.4 Criminological characteristics — 43
3.5 Conclusion — 45

4 Insight into the greatest threats in the field of money laundering — 47
4.1 Background — 47
4.2 Identification of the greatest money laundering threats — 48
4.3 Insight into the greatest money laundering threats — 51

5 Resilience of the policy instruments — 64
5.1 Organisation of anti-money laundering actions — 64
5.2 Available policy instruments — 65
5.3 International laws and regulations — 66
5.4 National laws and regulations — 68
5.5 Other policy instruments — 70
5.6 Possibilities for improving resilience — 73

6 Greatest money laundering risks in the Netherlands — 77
6.1 Assessment of the potential impact of the greatest money laundering threats — 77
6.2 Assessment of the resilience of the available policy instruments — 78
6.3 Greatest money laundering risks in the Netherlands — 80

7 Conclusions — 83
7.1 Answers to the research questions — 83
7.2 Evaluation of the second NRA — 88
7.3 Lessons for the next NRA — 93

References — 95

Appendices_

1 Composition of the Scientific Advisory Committee — 101
2 List of interviewed experts — 102
3 List of participants at the expert meetings — 104
4 Money laundering threats in FLUU Survey — 105
5 Email survey on policy instruments — 107
6 Results of the expert meetings — 109
7 Quantitative data analysis — 115

Abbreviations

ABN-AMRO	Algemene Bank Nederland, Amsterdam-Rotterdam Bank
AFM	Dutch Authority for the Financial Markets (*Autoriteit Financiële Markten*)
AIU	Anonymous, International, Unregulated (AIO, *Anoniem, Internationaal, Ongereguleerd*)
AMLC	Anti-Money Laundering Centre
AMON	Anti-Money Laundering Operational Network
ANBI	Public Benefit Organisation (ANBI, *Algemeen Nut Beogende Instelling*)
BES	Bonaire, Sint Eustatius and Saba
BFI	Special Financial Institutions (*Bijzondere Financiële Instellingen*)
BFT	Financial Supervision Office (*Bureau Financieel Toezicht*)
GDP	Gross Domestic Product
BTWwft	Wwft Monitoring Office (*Bureau Toezicht Wwft*)
BV	Private limited company (*Besloten vennootschap*)
CARIN	Camden Asset Recovery Inter-agency Network
CBS	Statistics Netherlands
CIA	Central Intelligence Agency
CJIB	Central Fine Collection Agency (*Centraal Justitieel Incassobureau*)
CPB	CPB Netherlands Bureau for Economic Policy Analysis (*Centraal Planbureau*)
CPI	Corruption Perceptions Index
CV	Limited partnership (*Commanditaire vennootschap*)
DNB	De Nederlandsche Bank (Dutch central bank)
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area
EFECC	European Financial and Economic Crime Centre
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EU	European Union
EFTA	European Free Trade Association EVA External Referral Application (*Externe Verwijzingsapplicatie*)
FLUU	Facts/cases, Likely, Unlikely and Unknown (*Feiten/casus, Aannemelijk, Niet aannemelijk en Onbekend*)
FATF	Financial Action Task Force
FCInet	Financial Criminal Investigation network
FEC	Financial Expertise Centre (*Financieel Expertise Centrum*)
FIU-NL	Financial Intelligence Unit-the Netherlands
FIOD	Fiscal Information and Investigation Service (*Fiscale Inlichtingen- en Opsporingsdienst*)
G7	Group of Seven
GDR	Group Decision Room
ICO	Initial Coin Offering
iCOV	Information Exchange on Criminal and Unexplained Wealth (*infobox Crimineel en Onverklaarbaar Vermogen*)
IND	Immigration and Naturalisation Service (*Immigratie- en Naturalisatiedienst*)
ING	Internationale Nederlanden Groep
IOCTA	Internet Organised Crime Threat Assessment
ISO 31000	Risk Management according to the standards of the International Organization for Standardization
J5	Joint Chiefs of Global Tax Enforcement

KMar	Royal Netherlands Military and Border Police (*Koninklijke Marechaussee*)
KNB	Royal Dutch Association of Civil-Law Notaries (*Koninklijke Notariële Beroepsorganisatie*)
Ksa	Netherlands Gambling Authority (*Kansspelautoriteit*)
LIEC	National Information and Expertise Centre (*Landelijk Informatie en Expertise Centrum*)
MCA	Multi-criteria Analysis (*Multi Criteria Analyse*)
MDMA	3,4-Methylenedioxymethamphetamine
NBA	Netherlands Institute of Chartered Accountants (*Nederlandse Beroepsorganisatie van Accountant*s)
NOvA	Netherlands Bar Association (*Nederlandse Orde van Advocaten*)
NRA	National Risk Assessment
NV	Public limited company (*Naamloze Vennootschap*)
NVB	Dutch Banking Association (*Nederlandse Vereniging van Banken*)
NVGTK	Dutch Money Transfer Association (*Nederlandse Vereniging van Geldtransactiekantoren*)
NVM	Dutch Association of Real Estate Brokers and Valuers (*Nederlandse Vereniging van Makelaars en Taxateurs*)
OECD	Organisation for Economic Co-operation and Development
OM	Public Prosecution Service (*Openbaar Ministerie*)
PSD2	Second Payment Service Directive
RABO	Raifeissen Bank, Boerenleenbank
R&D	Research and Development
RIEC	Regional Information and Expertise Centre (*Regionaal Informatie en Expertise Centrum*)
RPI	Residual Potential Impact (*Resterende Potentiële Impact*)
SNRA	Supranational Risk Assessment
UBO	Ultimate Beneficial Owner
VFN	Dutch Finance Houses' Association (*Vereniging van financieringsondernemingen in Nederland*)
VOF	Commercial partnership (*Vennootschap onder firma*)
WED	Economic Offences Act (*Wet op de economische delicten*)
Wet Bibob	Public Administration Probity Screening Act (*Wet bevordering integriteitsbeoordelingen door het openbaar bestuur*)
WODC	Research and Documentation Centre (*Wetenschappelijk Onderzoek- en Documentatiecentrum*)
Wft	Financial Supervision Act (*Wet op het financieel toezicht*)
WTR	Wire Transfer Regulation
Wtt 2018	Trust and Company Service Providers (Supervision) Act 2018 (*Wet toezicht trustkantoren 2018*)
WvSr	Penal Code (*Wetboek van Strafrecht*)
WvSv	Code of Criminal Procedure (*Wetboek van Strafvordering*)
Wwft	Money Laundering and Terrorist Financing Prevention Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*)

Summary

Background

Dutch policy to prevent and combat money laundering is based on the recommendations of the Financial Action Task Force (FATF) and European Union (EU) directives and regulations. The FATF – an intergovernmental body set up by the G7 in 1989 – focuses on global prevention and combat of money laundering, terrorist financing and other related threats to the integrity of the international financial system. Members of the FATF, including the Netherlands, are committed to implementing the FATF recommendations aimed at taking preventive and repressive measures by 'reporting institutions'[1] and to implement measures to improve national legal and regulatory systems and international cooperation in this field. In addition, the FATF monitors the correct functioning and effectiveness of those (legal) rules. The majority of the FATF's recommendations has been adopted into the fourth EU Anti-Money Laundering Directive and the amendments thereof, applicable to all EU Member States. Article 7 of this directive obliges EU Member States to implement a risk-based policy against money laundering and terrorist financing and to establish a National Risk Assessment (NRA). In 2017, the Research and Documentation Centre (WODC) carried out the first NRA on money laundering and on terrorist financing for the European part of the Netherlands. A year later, the WODC also conducted an NRA on both topics for the Caribbean Netherlands: the islands Bonaire, Sint Eustatius and Saba.

The WODC has carried out a second NRA for the European Netherlands on money laundering, with the aim of identifying the greatest risks in the field of money laundering. These are money laundering risks with the greatest residual potential impact. To this end, the money laundering threats with the greatest potential impact have been identified, an estimate has been made of the impact these threats can have and the 'resilience'[2] of the policy instruments aimed at preventing and combating money laundering has been determined. The residual potential impact is the impact that threats still have following the application of policy instruments to prevent or mitigate the potential impact of the threats. This means that the objective of the second NRA is slightly broader than the objective of the first NRA, which was limited to separately estimating the potential impact of the identified risks and the resilience. Other differences with the first NRA are that this second NRA provides more insight into the nature and 'mechanisms'[3] of the identified risks and that a first step has been taken to use quantitative data. In accordance with the first NRA, this NRA also describes some lessons learned, which can be taken into account in carrying out the following NRAs. The WODC carried out the second NRA on terrorist financing (for the European part of the Netherlands) simultaneously.

1 In the Netherlands, the Money Laundering and Terrorist Financing Prevention Act (Wwft) requires many institutions to report unusual transactions to the Financial Intelligence Unit-the Netherlands (FIU-NL).

2 Resilience is the ability of the policy instruments to prevent threats or mitigate the impact of threats, whereby the higher the resilience, the better the threats are mitigated. It concerns the content/scope as well as the implementation of the policy instruments.

3 The mechanisms relate to the process of a risk, the way a certain risk precisely works.

What is money laundering?

Legal and economic approach

A legal and economic approach can be distinguished in money laundering. The legal approach to money laundering is based on Articles 420bis, ter and quater in the Penal Code. These articles describe the circumstances in which someone is guilty of money laundering. From a legal perspective, money laundering is when somebody hides or conceals the true nature, source, place where it was found, disposition or movement of an object; or concealing or disguising who the legal owner is or who is in possession of the object; despite knowing that or being in a position in which they should reasonably suspect that the object in question was either directly or indirectly obtained as a result of any offence. 'Object' stands for all goods and property rights. In addition, it is possible to prosecute for 'simplified' money laundering in case of 'deliberate/intentional' money laundering as well as 'culpable' money laundering (articles 420bis.1 and 420quater.1 respectively). 'Simplified' money laundering, the mere acquisition or possession of an object immediately from one's own criminal conduct is sufficient. The 'concealing or disguising' criterion, the active act, is not applicable in case of 'simplified' money laundering.

For the NRA, the economic approach, which describes the process, is applied. The economic approach focuses on how money of criminal origin is returned to the legal money circuit and used economically, so that the origin of the money is concealed. In addition, in the NRA the so-called 'consumptive' money laundering, the spending of criminally obtained funds on the basic necessities of life, has been included.

The money laundering process

The money laundering process according to the economic approach can be divided into three phases, which are not always fully completed and which do not always follow each other chronologically. The FATF distinguishes the following phases:

- *Placement.* In this phase, a criminal places money to be laundered into the financial system, which gives it a cashless character. Crime such as drug trafficking often involves mostly large amounts of cash that a criminal wants to place in the financial system. In other forms of crime, the money may already be in the financial system, for example in the case of tax fraud.
- *Layering.* In this phase, which can take place both during and after the placement phase, a criminal conceals his/her identity and/or the origin of the criminal money in order to minimise the chance of being caught. Layering methods can be relatively simple but also very complex in nature.
- *Integration.* In this last phase, a criminal integrates the criminally obtained money – whether or not concealed – into the financial system, for example through spending on his own subsistence or investments in large-value products or real estate.

Research methodology

As in the first Dutch NRA on money laundering of 2017, the applied research approach is structured on the basis of the ISO 31000 framework for risk management. In short, the research methodology used involves the following:

- A context analysis has been conducted in which the specific, relatively fixed characteristics of the Netherlands that may influence the prevalence of money laundering are outlined. A literature study was carried out for this context analysis.

- A literature study was also carried out for an inventory of threats in the field of money laundering. The so-called FLUU survey was then carried out, in which expert organisations[4] were asked to indicate on a long list of money laundering threats whether they are aware of facts/cases of the threats and to what extent they consider the prevalence of the threats likely or not, based on the information available at their organisation.
- In a first expert meeting, experts subsequently identified the money laundering threats with the greatest potential impact. In the phase after this first expert meeting, the WODC held in-depth interviews with experts, which focused on the nature and mechanisms of the identified greatest money laundering threats. In a second expert meeting, experts assessed the potential impact of the further specified fifteen greatest money laundering threats using a Multi Criteria Analysis.
- In a third expert meeting, experts assessed the resilience of the available policy instruments to prevent and combat the fifteen greatest money laundering threats. Prior to the third expert meeting, a survey among experts provided insight into the policy instruments available for preventing and combating money laundering.
- By balancing the estimated potential impact of the greatest money laundering threats against the estimated resilience, the WODC has gained insight into the greatest money laundering risks in the Netherlands, ranked by their residual potential impact.
- In the final phase of the study, the WODC conducted validating interviews with six key experts, with the main aim of examining to what extent they recognise the ranking of the identified money laundering risks and how these risks can be further mitigated.
- In addition to the above, mainly qualitative research methods, in collaboration with Justis, the screening authority of the Ministry of Justice and Security, the WODC carried out a limited quantitative data analysis for one of the money laundering risks.

A lesson learned in the first NRA was that the second NRA (and subsequent NRAs) should focus more on substantiating and providing in-depth insight in the greatest money laundering threats identified by experts. In the NRA that has now been carried out, the WODC has paid more attention to this in various ways: by setting up the FLUU survey, a larger number of expert meetings (three instead of two) with more time for a plenary discussion of money laundering threats, a large number of in-depth interviews with experts, including case descriptions in the report and conducting a survey among experts on the policy instruments for preventing and combating money laundering.
Another lesson learned from the first NRA on money laundering is that a quantitative data analysis should be conducted in the second NRA. The intention was, as a first step, to conduct a quantitative data analysis in the NRA for the risks 'money laundering via legal entities', 'money laundering via ABC transactions' and 'money laundering via loan back constructions'. To this end, the WODC initially sought to collaborate with iCOV (Information Exchange on Criminal and Unexplained Wealth), which has access to a large number of data sources.[5] Unfortunately, the necessary

4 Expert organisations concern the following types of organizations: supervisory authorities under the Money Laundering and Terrorist Financing Prevention Act (Wwft); government agencies or government-affiliated organisations that play a role in preventing and/or combating money laundering; and private entities under Wwft supervision and sector/umbrella organisations of those private entities.

5 Via iCOV data from, among others, the Tax and Customs Administration, the Netherlands Police, the Public Prosecution Service, the Dutch Fiscal Intelligence and Investigation Service, the Netherlands Police Internal

declarations of consent from the various data source holders were not completed within the time frame of the study. When this became clear, the WODC contacted Justis and a quantitative data analysis was carried out via Justis for the risk of 'money laundering via legal entities', based on data from the Commercial Register of the Chamber of Commerce, which was assumed in advance to contribute to a further explanation of the risk. The analysis carried out demonstrated that, on the basis of such a data analysis without linkage to other data sources, such as data on suspicious declared transactions by the Financial Intelligence Unit – Netherlands and other criminal or fiscal information, no direct relationship with money laundering can be determined. The analyses only provide limited insight into a number of 'unusual situations'.

If including additional data sources in a subsequent NRA will be possible, it is unlikely that this analysis will provide insight into the prevalence of the money laundering risk in question. After all, a direct relationship with money laundering cannot be determined without further criminal investigation. Another complicating factor in implementing a more data-based NRA is the wide variety in the nature of the money laundering risks and the required data sources. The NRA is an overall analysis of all risks. The different data sources must therefore be analysed in relation to each other. This requires meeting quality requirements in terms of completeness, reliability, validity and mutual compatibility of data sources. There is currently insufficient knowledge regarding to what extent this can be met. It is recommended to carry out a separate exploratory study, so that it can be examined how the separately available relevant data sources can be made compatible and suitable in a subsequent NRA, and can become available for a meaningful data analysis.

What makes the Netherlands vulnerable to money laundering?

For this second NRA, a context analysis has been carried out that examines the characteristics of the Netherlands that may relate to the prevalence of money laundering in our country. The geographical, demographic, socio-cultural, economic and criminological characteristics of the Netherlands were examined. The Netherlands is characterized by an open, trade-oriented economy, a large and internationally oriented financial sector and a fiscal attractiveness for large foreign companies. The country is one of the most competitive economies in the world, has one of the largest airports and ports in the world and is one of the world's largest exporters. The Dutch economy is characterised as a service economy. All these characteristics make the Netherlands attractive for criminals to launder their illegally obtained money. The Netherlands can also be characterised – in comparison with other European countries – as a low cash intensive country and a high degree of digitalisation. These factors can influence the money laundering methods used by criminals. A socio-cultural factor that is characteristic of the Netherlands is the culture of tolerance, in which tolerance with regard to (soft)drugs in particular can contribute to the prevalence of drug crime and money laundering. Based on the culture of the so-called 'Polder Model', Dutch organisations usually seek alignment and cooperation with other organisations. The Netherlands is therefore distinguished from many other countries by the relatively high prevalence and large variety of

Investigations Department, FIU-NL, the Chamber of Commerce, the Netherlands' Cadastre, Land Registry and Mapping Agency and De Nederlandsche Bank can be accessed.

partnerships that have been established to prevent and combat money laundering. This concerns both public-public and public-private partnerships.

Money laundering threats with the greatest potential impact

The fifteen money laundering threats with the greatest potential impact according to money laundering experts are shown categorised in table S1. The level of the potential impact of the threats has been determined by means of an MCA. Experts used the following six criteria to make quantitative estimates that ultimately determined the level of the potential impact: 'deterioration in the stability of the financial system', 'undermining of authority and the legal order', 'damage to the regular economy', 'disruption of the social order', 'damage to the image of the Netherlands abroad', and 'reduction of subjective/objective security'.

The money laundering threat that experts say has the greatest potential impact is 'money laundering via wire transfers by licensed banks'. 'Money laundering via the physical movement of cash' has the lowest potential impact. Most money laundering threats have a potential impact with an impact level of 50 to 59 on a 0 to 100 scale.

Table S1 The fifteen greatest money laundering threats

Threats	Potential impact level (scale from 0-100)
Money laundering via wire transfers by licensed banks	60 to 69
Money laundering via structures by trust offices Money laundering via offshore companies Money laundering via legal entities Money laundering via dealers of high value services/goods Money laundering via trade-based constructions involving services Money laundering via the use of intermediaries Money laundering via investment institutions/companies Money laundering via trade-based constructions involving goods Money laundering via ABC transactions Money laundering via loan back constructions Money laundering via fictitious company turnover Money laundering via crypto currencies	50 to 59
Money laundering via underground banking, including unlicensed payment service providers Money laundering via the physical movement of cash	40 to 49

One of the identified fifteen greatest money laundering threats has a 'future' character: money laundering via investment institutions/companies. Experts believe that this threat is already occurring, but cannot yet indicate how and on what scale. There appears to be hardly any knowledge and/or information about this money laundering method. Therefore, this NRA does not contain a case description of money laundering via investment institutions/companies. In a validating interview, it was noted that the greatest risk is expected to lie with unlicensed and/or foreign-based investment institutions/companies.

A multitude of methods can be used to launder criminal money, whether or not in combination with each other. Money laundering methods can take place in the different phases of the money laundering process (placement, layering and integration phase). In this second NRA, for each identified money laundering threat, the nature and mechanisms of the threat have been addressed, in most cases these are clari-

fied using case descriptions. Some of the identified threats concern money laundering methods that are quite simple in nature, others are methods of a very complex nature. Some identified money laundering threats can be part of other threats, and many of the identified threats can be deployed in combination.

With regard to predicate offences, a recent study into the nature and size of criminal spending shows that drugs and financial fraud together account for more than 90% of the money laundering needs of criminals in the Netherlands. In that study, the size of fraud is estimated to be about three times higher than of drug crime. The in-depth interviews and expert meetings that took place as part of the NRA have not shown that certain money laundering methods can be related in particular to specific types of crime. It has, however, been mentioned that drug crime has a greater use of cash compared to financial fraud, which influences the need (or lack of it) to place the criminal money in the financial system, which in turn has consequences for the types of money laundering methods that a criminal uses.

Resilience of policy instruments

The available policy instruments for preventing and combating money laundering include all relevant instruments arising from international and national laws and regulations, municipal bylaw and regulations, sectoral and sector-oriented regulations, and regulations at organisational level. However, in this NRA, the term 'policy instrument' is interpreted more broadly than just laws and regulations. According to experts, guidelines and policy plans of organisations that play a role in preventing and/or combating money laundering can also be seen as policy instruments. Partnerships between organisations with a role in preventing and/or combating money laundering are also seen by experts as a policy instrument. Table S2 provides an overview of the policy instruments that were available in 2019 to prevent and combat money laundering.

Money laundering experts have estimated the mitigating effect of the total package of existing policy instruments on the potential impact of the fifteen greatest money laundering threats. In their assessment of the resilience of the policy instruments, experts took into account the policy instruments that existed at that time. This means that, in their assessment, they have not taken into account laws and regulations and other policy instruments that have been or will be introduced since the start of 2020. The results of the expert meeting are shown categorised in table S3.

Table S2 Policy instruments prevention and combat of money laundering

International laws and regulations	National laws and regulations	Other policy instruments
FATF-recommendations EU Anti-Money Laundering Directive EU Regulation on Controls of Cash Wire Transfer Regulation 2	Money Laundering and Terrorist Financing Prevention Act Financial Supervision Act Penal Code Code of Criminal Procedure Trust and Company Service Providers (Supervision) Act 2018 Public Administration Probity Screening Act Legal Entities Supervision Act Commercial Register Act 2007 Tax legislation Economic Offences Act Right to report Tax and Customs Administration 2003	National partnerships International partnerships Sectoral and sector-oriented regulations and terms and conditions Guidelines and policy plans

Resilience scores above 60% for one money laundering threat, namely for 'money laundering via wire transfers by licensed banks'. This means that, according to experts, the total available policy instruments counteract this money laundering threat by more than 60%. Other threats in which the available policy instruments, according to experts, have a relatively high resilience are 'money laundering via structures by trust offices' and 'money laundering via investment institutions/companies'. An important note here is that the experts have estimated the resilience to these threats as high because they based their assessment on *licensed* institutions incorporated *in the Netherlands*. The resilience to money laundering through constructions with *foreign* offshore companies is much lower. Validating interviews confirmed that the resilience to *foreign* and/or *unlicensed* institutions/companies is relatively low.

Table S3 Resilience total package of policy instruments per money laundering threat

Threats	Resilience level (scale from 0-100)
Money laundering via wire transfers by licensed banks	60 to 69
Money laundering via structures by trust offices Money laundering via investment institutions/companies	50 to 59
Money laundering via fictitious company turnover Money laundering via legal entities Money laundering via ABC transactions Money laundering via the use of intermediaries Money laundering via loan back constructions	40 to 49
Money laundering via dealers of high value services/goods Money laundering via trade-based constructions involving goods Money laundering via offshore companies Money laundering via the physical movement of cash	30 to 39
Money laundering via trade-based constructions involving services Money laundering via crypto currencies	20 to 29
Money laundering via underground banking, including unlicensed payment service providers	10 to 19

Although the available instruments clearly have a mitigating effect on the fifteen greatest money laundering threats that are central to this NRA, these threats can still have a greater or lesser impact. The extent to which the so-called AIU principle, already introduced in the first NRA, applies to money laundering threats, affects the resilience of the policy instruments. Most money laundering methods have one or more of the following three components: Anonymity (the method conceals the identity of the money laundering criminal), International (the method has an international character and is used via or from abroad) and Unregulated (the method relates to or is used in an unregulated sector). The more the AIU elements apply to money laundering threats, the lower the resilience of the policy instruments for preventing and combating the threats. With such threats, the money laundering criminal's chance of being caught is therefore relatively low.

Effective prevention and combating of money laundering threats with a strong international component requires close cooperation and exchange of information at international level between supervisory, investigative and law enforcing authorities, something that is often difficult to realise in practice, partly due to different money laundering definitions, law enforcement practices and different legal systems. The available policy instruments are, according to experts, only equipped to a limited extent to effectively counter money laundering threats at (financial) institutions and service providers operating without a license, for example in underground banking. Finally, relatively low resilience is found for methods that increase the anonymity of transactions, such as money laundering via crypto currencies, underground banking and the physical movement of cash.

Greatest money laundering risks in the Netherlands

Table S4 Residual Potential Impact (RPI) of the fifteen greatest money laundering risks

Risks	Residual Potential Impact (scale from 0-100)
Money laundering via crypto currencies Money laundering via trade-based constructions involving services Money laundering via underground banking, including unlicensed payment service providers Money laundering via offshore companies Money laundering via dealers of high value services/goods	36 to 40
Money laundering via trade-based constructions involving goods Money laundering via legal entities Money laundering via the use of intermediaries	31 to 35
Money laundering via ABC transactions Money laundering via loan back constructions Money laundering via the physical movement of cash Money laundering via structures by trust offices Money laundering via fictitious company turnover Money laundering via investment institutions/companies	26 to 30
Money laundering via wire transfers by licensed banks	21 to 25

By balancing the estimated potential impact of the greatest money laundering threats against the estimated resilience, the WODC has gained insight into the greatest money laundering risks in the Netherlands, ranked by their residual potential impact (RPI). Five of the fifteen money laundering risks are in the

highest category with an RPI score of 36 to 40 on a scale that can theoretically run up to 100. ‘Money laundering via wire transfers by licensed banks’ has the lowest RPI score, which is the result of the relatively highly estimated resilience concerning this risk. It can be concluded that the impact that money laundering threats can have, is considerably mitigated by the available policy instruments.

1 Introduction

1.1 Reason for the study

Dutch policy to prevent and combat money laundering is based on the recommendations of the Financial Action Task Force (FATF)[6] and European Union (EU) legislation. The FATF is an intergovernmental body set up by the G7[7] in 1989, which focuses on the global prevention and suppression of money laundering, terrorist financing and other related threats to the integrity of the international financial system. Members of the FATF, including the Netherlands, are bound by recommendations stipulating that reporting institutions[8] must take appropriate preventive and suppressive measures and measures to improve national legal systems and international cooperation. In addition, the FATF monitors the correct functioning and effectiveness of these measures, whether or not they are laid down by law.[9] For EU Member States, the majority of the FATF's recommendations have been adopted as part of the amendment to the Fourth Anti-Money Laundering Directive.[10] Article 7 of this directive obliges EU Member States to implement a risk-based policy against money laundering and terrorist financing and to establish a National Risk Assessment (NRA). In 2017, following a study of relevant methods and data, the Research and Documentation Centre (WODC, *Wetenschappelijk Onderzoek- en Documentatiecentrum*) of the Ministry of Justice and Security conducted the first Money Laundering NRA and the first Terrorist Financing NRA for the European part of the Netherlands. A year later, the WODC also carried out an NRA in both fields for the Caribbean Netherlands, i.e. the islands of Bonaire, Sint Eustatius and Saba.[11]

A second Money Laundering NRA has now been carried out for the European Netherlands, with the aim of identifying the greatest risks in the field of money laundering. This concerns the money laundering risks with the greatest residual potential impact (RPI, *resterende potentiële impact*). To this end, the money laundering threats with the greatest potential impact have been identified, an estimate has been made of the impact that these threats may have and the resilience[12] offered by the policy instruments aimed at preventing and combating money laundering.

---

6 FATF (2012).

7 The G7 is an intergovernmental forum of the seven leading industrial countries in the world and the European Union. It includes Canada, Germany, France, Italy, Japan, the United Kingdom, the United States and the European Union.

8 In the Netherlands, the Money Laundering and Terrorist Financing Prevention Act (Wwft, *Wet ter voorkoming van witwassen en financieren van terrorisme*) requires a large number of institutions to report unusual transactions to the Financial Intelligence Unit-the Netherlands (FIU-NL). More information about this Act and the ensuing obligations for institutions can be found in Chapter 5.

9 www.fatf-gafi.org.

10 See the list of References for the formal titles and sources of the laws and regulations.

11 Van der Veen & Ferwerda (2016), Van der Veen & Heuts (2017a), Van der Veen & Heuts (2017b) and Van der Veen & Heuts (2018). At the time, it was decided to implement separate NRAs for the European and Caribbean parts of the Netherlands, owing to the significant differences in geographical, demographic, economic and sociocultural characteristics that could make these territories more or less vulnerable to money laundering and terrorist financing. There are also differences between the two territories in terms of the existing policy instruments for combating the risks as well as how these instruments are applied.

12 Resilience refers to the functioning of the policy instruments where the higher the resilience, the better the threats are countered. It concerns the content or scope as well as the implementation of the policy instruments.

This means that the objective of the second NRA is slightly broader than that of the first NRA, which had limited itself to only identifying the potential impact of the identified risks and resilience. Other differences with the first NRA are that this second NRA offers greater insight into the nature and mechanisms[13] of the identified risks and that a first step has been taken towards using quantitative data. In line with the first NRA, this NRA also describes a number of lessons learned that could be taken into account when carrying out subsequent NRAs.

Along with the implementation of the second Money Laundering NRA, the second Terrorist Financing NRA was also performed (for European Netherlands).[14]

1.2 What is money laundering?

Legal and economic approach
Money laundering can be defined based on a legal or economic approach. The legal approach to money laundering is based on Articles 420bis, ter and quater in the Penal Code (WvSr, *Wetboek van Strafrecht*). These articles describe the circumstances under which money laundering is carried out. In legal terms, money laundering is the act of hiding or concealing the true nature, origin, location, sale or movement of an object or the concealment of the identity of the party entitled to or in possession of the object, despite it being known or reasonably suspected that the object in question has been directly or indirectly obtained as the proceeds of crime. For the purpose of this definition, 'object' includes all goods and property rights.[15] In addition, it is also possible to prosecute for self-laundering in case of either intentional money laundering or culpable money laundering (Article 420bis.1 and Article 420quater.1 respectively).
In the case of self-laundering, simply acquiring or being in possession of an object that originates directly from a person's own criminal activity is considered a sufficient ground for prosecution. The criterion of 'hiding or concealing', i.e. the actual act, is not relevant in the case of self-laundering.

For the NRA, the economic approach for describing the process of money laundering has been applied. The economic approach focuses on how funds originating from crime are re-introduced into the legitimate financial system and used for economic activities such that the origin of the funds is disguised.[16] In addition, this NRA also takes into account the so-called consumption-related money laundering, i.e. the spending of illegally obtained resources on basic day-to-day necessities.[17]

13 Here, the term 'mechanisms' refer to the precise manner in which a certain risk functions or works.

14 A separate second NRA is being carried out for the Caribbean part of the Netherlands.

15 Penal Code, Articles 420bis, ter and quater; see the References section for the formal titles and sources of the laws and regulations.

16 Soudijn & Akse (2012).

17 In studies on money laundering, the inclusion of consumption-related money laundering as a study subject has both its supporters and opponents. Van Duyne et al. (2018) addresses this discussion on page 119-120.

Money laundering process

The money laundering process, based on the economic approach, can be subdivided into three phases, but these phases do not always occur and do not always follow one another sequentially. The FATF distinguishes the following phases:[18, 19]

- *Placement:* in this phase, a criminal introduces the money to be laundered in the financial system, thus converting it into money in accounts. A form of crime such as drug trafficking usually involves large amounts of cash that a criminal wants to place in the legitimate financial system. In some forms of crime, the money is already in the financial system, for example, in the case of tax fraud.
- *Layering*: in this phase, which may occur both during and after the placement phase, a criminal conceals his/her own identity and/or the origin of the criminal money in order to minimise the chance of being caught. Layering methods may be relatively simple or very complex in nature.
- *Integration:* in this final phase, a criminal integrates the criminally obtained funds, whether or not in a disguised manner, into the financial system, in the form of day-to-day expenditure for supporting himself/herself or investments in high-value products or real estate.

1.3 Research objective and questions

This second Money Laundering NRA has a threefold objective. First of all, the purpose of the study is to ensure that the money laundering threats with the greatest potential impact are identified by representatives of expert organisations in the field of money laundering.[20] Secondly, the study should provide more insight into the nature and mechanisms of the identified threats. Finally, the NRA must determine the resilience of the policy instruments aimed at preventing and combating the identified threats. By combining the expert assessments of the potential impact and resilience, this Money Laundering NRA provides insight into the greatest money laundering risks in the Netherlands, ranked by the RPI of these risks.

As in the case of the first NRA, the structure of the second NRA is determined by the ISO 31000 risk management framework. Based on this, the NRA consists of the following phases:

- A context analysis phase in which the specific and relatively fixed characteristics of the Netherlands that may influence the prevalence of money laundering are outlined.
- A risk identification phase in which the money laundering threats with the greatest potential impact (hereinafter referred to as: the greatest money laundering threats) are determined and ranked. The greatest money laundering threats are selected from a longlist of threats by representatives of expert organisations in the field of money laundering.
- A risk analysis phase, which offers insight into the extent to which the available policy instruments for preventing and combating money laundering effectively counteract the greatest money laundering threats, i.e. the resilience of these

18 www.fatf-gafi.org/faq/moneylaundering/.

19 In addition, a four-phase model has been developed, with justification as a separate phase. See Van Koningsveld (2013).

20 Expert organisations include the following types of organisations: (1) supervisory authorities under the Wwft, (2) public services or government-affiliated organisations that play a role in preventing and/or combating money laundering and (3) private parties subject to supervision under the Wwft and the sector/umbrella organisations of these private parties.

instruments. A comparison of the expert assessments of the potential impact and resilience provides insight into the greatest money laundering risks, ranked by their RPI.

The NRA provides an answer to the following research questions:

1 What are the context-related factors that may influence the prevalence of money laundering in the Netherlands?
2 What can be said about the nature, mechanisms and potential impact of the greatest money laundering threats and the types of predicate crime that may precede these threats?
3 What are the money laundering threats that have not yet been identified in the Netherlands but could become relevant in the future?
4 What policy instruments are available in the Netherlands for preventing and combating the greatest money laundering threats?
5 What can be said about the resilience of the available policy instruments for preventing and combating the greatest money laundering threats?
6 What money laundering threats are considered by experts as the greatest money laundering risks (i.e. the risks with the greatest residual potential impact)?
7 To what extent can the data available from expert organisations be used for a quantitative data analysis of the greatest money laundering risks?
8 What further data do we need to gain more insight into the greatest money laundering risks?
9 What points of improvement can be applied for future NRAs?

1.4 Lessons from the first Money Laundering NRA

The first Money Laundering NRA in 2017 taught us a number of lessons on how to conduct the study in the future.[21] One of the lessons learned was that quantitative research results should play a greater role in the second NRA (and subsequent NRAs). This will ensure that the NRAs are less dependent on expert assessments that may be partly subjective in nature and therefore reduce the risks associated with this. The aim is to make the research results more reliable by substantiating them, in so far as possible, with more detailed quantitative data. This is why quantitative data have been used to a greater extent in this NRA (also see Chapter 2).

Another lesson learned from the first NRA is that the second NRA (and subsequent NRAs) should pay more attention to substantiating and gaining a deeper understanding of the money laundering threats that, as identified by experts, have the greatest potential impact. During the expert meetings for the first NRA, there was not always enough time to focus on substantiating all the expert opinions and developing the sample cases. This – along with the fact that some experts were not permitted to share their knowledge in full and that they sometimes lacked the relevant knowledge – resulted in parts of the first NRA being somewhat shallow in nature. In addition, it was not always clear during the expert meetings for the first NRA whether the assessments formed by the experts present were based on their own experiences with the money laundering threats or on information acquired

21 Van der Veen & Heuts (2017a).

elsewhere. The present NRA has devoted more attention to substantiating and gaining a deeper understanding of the research findings in a number of ways:[22]

- Via an email survey containing a longlist of money laundering threats, experts were asked to indicate whether they are aware of facts or cases relating to the threats and to what extent they consider the prevalence of the threats likely or not, based on the information available within their organisation. This survey, hereinafter referred to as the FLUU Survey (see Chapter 2 for more information), offered insight into whether or not expert organisations were familiar with facts or cases relating to the threats on the longlist, which helped identify the organisations that needed to be invited to the expert meetings.
- At the first expert meeting, the entire longlist of money laundering threats as well as the threats added to the list based on the email survey were discussed extensively with all the participating experts. Since the number of expert meetings for the second NRA was increased from two to three, much more time was available for this discussion than during the first NRA. When discussing each threat, participants were asked about the cases known to them. Based on this discussion, the longlist was partially adjusted (merging of multiple threats, splitting of a single threat into multiple threats and a more precise formulation). After the plenary discussion of the money laundering threats, the experts identified the money laundering threats that they thought had the greatest potential impact.
- After the first expert meeting, in-depth interviews were held with representatives of the expert organisations in order to gain more insight into the greatest money laundering threats identified at the meeting. In these interviews, further questions were asked about the nature and mechanisms of the money laundering threats and concrete examples of cases involving these threats. The results were discussed at the beginning of the second expert meeting, which led to a further refinement of the list of the greatest money laundering threats.

1.5 Reading guide

Chapter 2 goes into the details of the research methods used in this second Money Laundering NRA. It also contains a description of the key concepts that play an important role in the NRA and which are also referred to in this report.

Chapter 3 describes how the Netherlands is vulnerable to money laundering based on information from previous assessment and substantiates this by outlining a number of geographical, demographic, sociocultural, economic and criminological characteristics of the Netherlands that may influence the prevalence of money laundering.

Chapter 4 describes the main money laundering methods used in this NRA. These are methods that criminals may use to launder their criminal proceeds. This chapter describes the results of the first expert meeting where experts identified the money laundering threats with the greatest potential impact.

Chapter 5 examines the policy instruments available for preventing and combating the greatest money laundering threats. The chapter concludes by describing some options for further improving the resilience of the policy instruments.

22 Section 2.3 provides a more detailed description of the changes made in this second NRA. Section 7.2 adds a number of other changes that have also resulted in an improved substantiation and a deeper understanding of the research findings.

Chapter 6 describes the results of the second and third expert meetings where, respectively, experts made a quantitative estimate of the potential impact of the greatest money laundering threats and the resilience of the policy instruments. The chapter concludes by relating these two elements to one another, thus creating the list of the greatest money laundering risks in the Netherlands ranked by the RPI of these risks.

The final chapter (Chapter 7) starts by answering the research questions that are of central importance to this NRA. Subsequently, it evaluates the implementation of the NRA and draws some lessons that can be taken into account in the implementation of subsequent NRAs.

2 Research methodology

This chapter describes the research approach selected for this second NRA. First, the key concepts in the NRA are introduced and defined. The research plan and the methods applied are described with reference to the three phases of the NRA: context analysis, risk identification and risk analysis. These phases are part of the ISO 31000 risk management method[23] that – just as in the first NRA of 2017 – has been selected as the central framework for this NRA.

2.1 Key concepts of the NRA

Similar to the first Money Laundering NRA, this NRA also adheres to the definitions provided by the FATF Guidance[24] for the key concepts of threats, consequences and vulnerabilities:

- In this NRA, **threats** include all the methods that may be used by persons or groups of persons to launder money obtained from criminal activities. This refers to methods by which the criminal money is placed and/or integrated into the financial system, as well as the layering methods that may be used to reduce the chance of being caught. Use of these methods may involve misuse of the services of financial and non-financial institutions such as banks, payment service providers, accountants, civil-law notaries, brokers, etc.
- **Consequences** are the effects that may occur as the result of the threats. In the NRA, these consequences are referred to as the potential impact of the money laundering threats. Money laundering threats may differ in the extent to which they affect the stability of the financial system, authority and legal order, the regular economy, the social order, the image of the Netherlands abroad and subjective and objective security.[25]
- **Vulnerabilities** are relatively established factors that affect the prevalence of threats. This NRA looks into the geographic, demographic, economic, sociocultural and criminological context-related factors that may influence the likelihood of threats occurring in the Netherlands and/or influence the consequences thereof.

As in the first NRA of 2017, the element of resilience has been added to the above key concepts:

- **Resilience** refers to the effectiveness of the policy instruments available in the Netherlands for preventing and combating money laundering. This concerns both the content/scope of the policy instruments as well as the implementation of these instruments. Resilience can determine the likelihood of the threats occurring and the extent of the potential impact of the threats. The principle is: the higher the resilience, the better the threats will be countered. While the vulnerabilities consist of factors that are relatively insensitive to policy changes, the resilience element comprises factors that can be influenced. In fact, this NRA deals with the specific policy decisions and the implementation of these decisions that can help prevent the occurrence of money laundering.

23 Risk management according to the standards of the International Organization for Standardization.

24 FATF (2013).

25 The elements listed here form the criteria that have been applied in the Multi-criteria Analysis that is performed in this NRA to determine the scope of the potential impact of the money laundering threats. Section 2.3 goes into the details of this.

Risk, the last key concept, brings together the four elements mentioned above, i.e. threats, consequences (or potential impact), vulnerabilities and resilience. The elements that determine the risk of each threat in the NRA are an elaboration and refinement of the time-honoured and still-commonly-used risk definition where risk is determined by impact and probability.[26]

- In this NRA, **probability** refers to the likelihood of the threats actually occurring. This probability is determined based on the elements of vulnerabilities and resilience. Here, a distinction is made between context-related characteristics that are difficult to influence through policy (vulnerabilities) and policy characteristics that can be directly influenced by policymakers (resilience). After all, the probability that a money laundering threat may or may not arise is determined by the contextual factors that influence the Dutch vulnerabilities as well as the resilience of the existing Dutch policy instruments for preventing and combating money laundering based on the major threats identified.
- **Impact** is equivalent to the above-mentioned concept of consequences or potential impact. In this NRA, the potential impact is determined using a Multi-criteria Analysis (MCA), where the potential impact of the major threats is assessed by experts based on a number of criteria such as the stability of the financial system and disruption of the social order (see Section 2.3 for more information about the MCA and the specific criteria applied).
- Finally, the **risk** of each threat is determined by bringing together the above-mentioned key elements.[27]

2.2 Performing the NRA in accordance with the ISO 31000 framework

The NRA has been carried out based on the ISO 31000 risk management framework.[28] A wide range of methods can be used within this internationally standardised framework. The FATF Guidance also follows the broad outlines of this framework.[29] The NRA presented here does not cover the entire ISO 31000 risk management cycle, but limits itself to the phases dealing with context analysis, risk identification and risk analysis. The remaining phases, i.e. risk evaluation and risk treatment, require decisions to be made about the extent to which risks are acceptable or tolerable and whether new or adjusted policies are necessary. Making such normative decisions is incompatible with the academic approach of the present NRA. Accordingly, risk evaluation and risk treatment have been excluded from the scope of the present NRA.

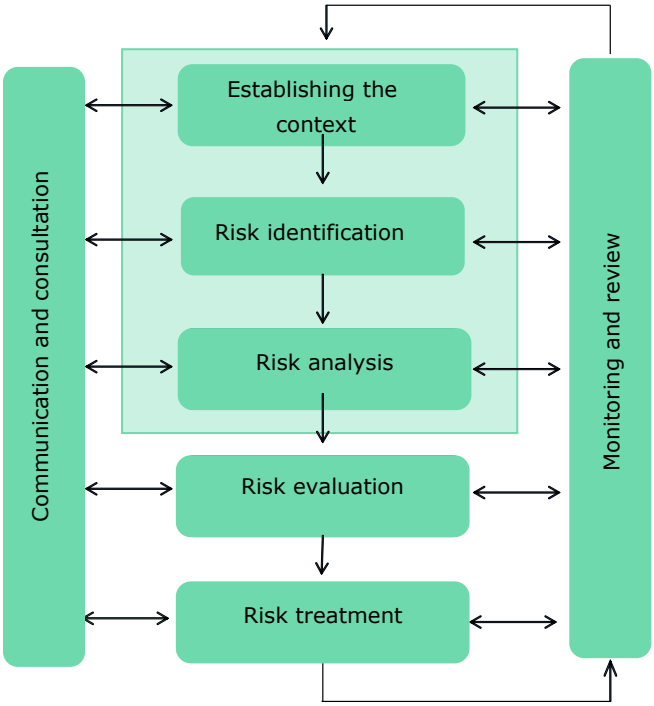
26 Lees (1980).

27 The following equation is applied with respect to each threat: Risk = Vulnerability*Potential Impact*Resilience.

28 ISO 31000:2009 (2009a), ISO/IEC 31010:2009 (2009b).

29 FATF (2013).

Figure 1 Risk management process based on the ISO 31000 framework, with the focus fields of the NRA in light-green



2.3 Methods used

Various activities have been carried out to answer the research questions posed in this second NRA. These activities are indicated for each phase.

Context analysis phase
The 2017 NRA included a comprehensive context analysis focusing on the various factors that may affect the prevalence of money laundering in the Netherlands. This included geographic, demographic, economic and criminological characteristics of the European part of the Netherlands. Where necessary, the information on these characteristics has been updated in this second NRA with information from relevant public sources and scientific literature. What is new for the present NRA is that the context analysis also pays attention to certain sociocultural characteristics that may influence the prevalence of money laundering in the Netherlands.

Risk identification phase
1 Updating the longlist of money laundering threats
The longlist of money laundering threats drawn up in the first Money Laundering NRA[30] was updated after studying recent reports (published since 2018) such as

30 Van der Veen & Heuts (2017a). This longlist has been drawn up based on a literature study and a stocktaking survey via email conducted among expert organisations. Expert organisations include the following types of organisations: supervisory authorities under the Wwft, public services or government-affiliated organisations that play a role in preventing and/or combating money laundering, private parties subject to supervision under the Wwft and the sector/umbrella organisations of these private parties.

foreign NRAs and the European Supranational Risk Assessment (SNRA).[31] The updated longlist of money laundering threats consists of placement methods and channels as well as concealment methods.

2 FLUU Survey
The updated longlist, consisting of 25 money laundering threats, was sent to the expert organisations as part of the FLUU Survey via email (see explanation below). The provisional list of the organisations to be approached was first submitted to the Scientific Advisory Committee (SAC), after which some organisations were added to the list. Expert organisations include the following types of organisations:
- Supervisory authorities under the Wwft.
- Public services or government-affiliated organisations that play a role in preventing and/or combating money laundering.
- Private parties subject to supervision under the Wwft and the sector/umbrella organisations of these private parties.

In the FLUU Survey, experts were asked to indicate, on the longlist of threats sent to them, whether they are aware of facts or cases relating to the threats and to what extent they consider the prevalence of the threats likely or not based on the information available within their organisation. The experts had to indicate one of the following letters for each threat on the longlist:
- An **F** (*Feiten/Casus*) if, according to the expert, this threat is present and one or more facts or cases relating to the threat are known to his or her organisation.
- An **L** (*Aannemelijk*) if, according to the expert, it is likely that this threat is present but no actual offences or cases are known to his or her organisation.
- A **U** (*Niet aannemelijk*) if, according to the expert, it is unlikely that the threat is present, based on the information available to his or her organisation.
- A **U** (*Onbekend*) if it is unknown to the expert whether or not the threat is present because his or her organisation has no information regarding this.

In this FLUU Survey, experts were also given the opportunity to add the money laundering threats that they felt were missing from the longlist. A total of 30 expert organisations were approached for the survey, of which 25 organisations completed and returned the email survey.[32] Table 1 lists the organisations that completed and returned the survey.

The use of the FLUU Survey is an initial step towards an evidence-based risk identification. Since it provided insight into whether or not expert organisations were familiar with the facts or cases relating to the threats in the longlist, it became clear which organisations should be invited to the first and second expert meetings (see below for more information). To allow for evidence-based risk identification, both the identification of money laundering threats with the greatest potential impact as well as the assessment of the impact of these threats are performed by parties that have indicated that they have operational knowledge of and experience with the threats in question. The FLUU Survey also helped identify (1) the participants from the first expert meeting that could be requested to provide sample cases and (2) the organisations with which in-depth interviews could be organised later on.

31 See the References section for references to the consulted Risk Assessments.

32 The list of expert organisations was submitted in advance to the SAC to check whether any relevant parties are missing. To protect the anonymity of the organisations, the names of the organisations that have not completed the FLUU Survey have not been included.

Table 1 List of FLUU Survey respondents

Organisation	Organisation
ABN-AMRO	Netherlands Police
Anti-Money Laundering Centre (AMLC)	Netherlands Institute of Chartered Accountants (NBA, *Nederlandse Beroepsorganisatie van Accountants*)
Dutch Authority for the Financial Markets (AFM, *Autoriteit Financiële Markten*)	Netherlands Bar Association (NOvA, *Nederlandse Orde van Advocaten*)
Financial Supervision Office (BFT, *Bureau Financieel Toezicht*)	Dutch Money Transfer Association (NVGTK, *Nederlandse Vereniging van Geldtransactiekantoren*)
Wwft Monitoring Office (BTWwft, *Bureau Toezicht Wwft*)	Dutch Association of Real Estate Brokers and Valuers (NVM, *Nederlandse Vereniging van Makelaars en Taxateurs*)
Holland Quaestor*	Public Prosecution Service (OM, *Openbaar Ministerie*)
De Nederlandsche Bank (DNB)	PaySquare**
Customs Service	Rabobank
Financial Intelligence Unit – the Netherlands (FIU-NL)	Association of Estate Agents in the Netherlands (*VBO Makelaars*)
Holland Casino	De Volksbank
ING	
International Card Services***	
Netherlands Gambling Authority	
Royal Netherlands Military and Border Police (KMar, *Koninklijke Marechaussee*)	
Royal Dutch Association of Civil-Law Notaries (KNB, *Koninklijke Notariële Beroepsorganisatie*)	

* Holland Quaestor is an association of Dutch trust offices. Holland Quaestor members represent approximately 75% of the market share of the sector. See: https://hollandquaestor.nl.

** PaySquare handles the acceptance of credit, debit and international payment cards such as VISA, MasterCard, American Express, UnionPay and Maestro.

*** International Card Services is a Dutch credit card issuer. It is a part of ABN AMRO.

3 First expert meeting

The results of the FLUU Survey provided the starting point for an expert meeting consisting of representatives from 18 expert organisations (see Table 2). The participants were selected based on the FLUU Survey, depending on the extent to which organisations were aware of facts or cases relating to money laundering threats. Although many more large banks were familiar with facts or cases relating to money laundering threats, it was decided to include only one large bank in the expert meeting, to prevent the banks from gaining a majority vote at the meeting. After consultation with the Scientific Advisory Committee, it was decided to invite ING to this meeting and the following expert meetings.

In the invitation email for the first expert meeting, expert organisations were asked to delegate a person with operational knowledge of the money laundering threats. The expert meeting started with a joint discussion of the entire longlist of money laundering threats. When discussing each threat, participants were asked about the cases known to them. During the plenary discussion of these cases, all the participants at the expert meeting got the opportunity to gain at least a basic level of knowledge of the nature, mechanisms and prevalence of the threats on the longlist. This helped bring all of them on the same page in terms of information about and understanding of the threats. In addition, the joint discussion of the money laundering threats led to adjustments in some parts of the longlist, as experts were of the opinion that some threats should be merged into a single threat, one particular threat should be split into two threats, and the wording of some of the threats needed to be made more precise.

Table 2 List of participants at the first expert meeting

Organisation	Organisation
Anti-Money Laundering Centre	Royal Netherlands Military and Border Police
Dutch Authority for the Financial Markets	Royal Dutch Association of Civil-Law Notaries
Financial Supervision Office	Netherlands Police
Wwft Monitoring Office	Netherlands Institute of Chartered Accountants
Corpag (on behalf of Holland Quaestor)	Netherlands Bar Association
De Nederlandsche Bank	Dutch Money Transfer Association
Customs Service	Dutch Association of Real Estate Brokers
Financial Intelligence Unit – the Netherlands	and Valuers
ING	Public Prosecution Service
Netherlands Gambling Authority	

After discussing the 25 money laundering threats on the longlist, the threats that the experts had added to the FLUU Survey were also discussed. Prior to the expert meeting, the WODC had analysed and clustered the list of threats added to the FLUU Survey. The added threats were discussed jointly, and for each threat, it was decided whether or not to add it to the longlist. This led to the addition of three money laundering threats to the longlist (see Chapter 4 for more information), so that the final longlist consisted of 28 money laundering threats.

In the first expert meeting, the experts selected the 10 threats from the longlist that, in their opinion, scored highest in the Dutch context in terms of their potential impact and prevalence. In this and subsequent expert meetings, the Delphi Method (Box 1) was applied within a Group Decision Room (GDR) environment (Box 2).

Box 1 Delphi Method

The Delphi Method was developed in the 1950s* at the start of the Cold War when, during a project being conducted for the United States Air Force, it was found that traditional scientific methods did not offer a sufficient basis for developing new techniques for international warfare. In the Delphi Method, the views of experts or a group of experts are combined for taking decisions on subjects for which reliable, scientifically verifiable information is lacking. Gaps in knowledge are compensated for based on expert assessments, experiences and intuition. Through a process of anonymous feedback and further substantiation of these assessments, experiences and intuition, the experts get a chance to revise their initial assessments. This leads to a greater consensus for a solution. The process takes place over a number of rounds. Advantages of the Delphi Method are:

- Increases the transparency of complex decision-making processes and makes these processes more systematic.
- Makes better use of existing knowledge and information, since all the experts share their knowledge and information.
- This often results in a greater consensus regarding the 'best' solution.

However, the Delphi Method involves a risk of groupthink. Groupthink occurs when the decision-making process is so focused on gaining consensus that this is achieved at the expense of the quality of the decision-making.** Experts may mistakenly assume that all relevant aspects have been taken into account in the decision-making.

* www.rand.org/topics/delphi-method.html.

** Kroon (1992).

Groupthink was prevented by appointing a professional independent chairperson for the expert meetings. This chairperson encouraged the experts to, together with the researchers, substantiate, explain, ask further questions about and provide sample cases for the assessments they made in the GDR environment. In the GDR, the use of ICT methods, such as the submission of individual digital votes by the experts, is alternated with group discussions. This helped in improving the organisation and structure of the expert meetings (see Box 2 for more information). Within the constraints of the available time, attempts have been made to give the experts as much opportunity as possible to explain, substantiate, ask each other questions about and discuss their assessments. Research bureau Significant APE provided the chairperson for the expert meetings and drew up the reports.[33]

Box 2 Group Decision Room (GDR)

As in the first NRA, the expert meetings made use of a GDR. A GDR is an electronic meeting system that enables participants to generate a large number of ideas and opinions within a short period of time through the use of ICT technology alternated with plenary discussions. During the expert meetings for this NRA, participants were given the opportunity to vote digitally via a laptop network in order to identify the risks (first expert meeting), estimate the potential impact of the greatest money laundering threats (second expert meeting) and assess the resilience of the policy instruments (third expert meeting). The responses of the participants are collected and stored centrally. The experts were able to enter their assessments and scores via the laptop, after which the aggregated results were presented in real-time.

In the case of the first NRA, the use of a GDR proved to be a fruitful approach. During the self-evaluation process of the first NRA, it was found that the use of the GDR environment, compared to a regular meeting environment, was not just time-efficient, but also created the opportunity to explore the results in greater depth via plenary discussions. Through the use of the GDR and group discussions alternated with the submission of scores/assessments on a laptop, it was ensured that the experts continued to participate actively throughout the meeting. Another advantage of the GDR was that the final numerical score of the potential impact of the threats and the resilience was determined based on the data presented by all experts present in the GDR environment. All relevant perspectives are therefore represented in these final scores. Finally, the use of the GDR also facilitated the collection of the data.

4 In-depth interviews with expert organisations

In order to gain more insight into the precise nature and mechanisms of the greatest money laundering threats identified, in-depth interviews were conducted with 39 representatives from 21 expert organisations (see Table 3). In these interviews, further questions were asked about the nature and mechanisms of the greatest money laundering threats identified at the first expert meeting, concrete examples of cases involving these threats and future money laundering threats. In addition to the interviews, relevant reports, news articles and other sources from the internet or elsewhere that reveal more about the nature and mechanisms of the threats were studied.

33 The GDR functionality was provided by the company Spilter. Spilter employees provided technical support at the expert meetings.

Table 3 In-depth interviews

Organisation	Number of interviewees	Organisation	Number of interviewees
ABN-AMRO	4 employees	Financial Intelligence Unit – the Netherlands	2 employees
Anti-Money Laundering Centre	2 employees	ING	2 employees
Dutch Authority for the Financial Markets	3 employees	Justis**	2 employees
Tax and Customs Administration	2 employees	Chamber of Commerce	1 employee
Financial Supervision Office	2 employees	Royal Dutch Association of Civil-Law Notaries	2 employees
Wwft Monitoring Office	2 employees	Netherlands Police	1 employee
Corpag (on behalf of Holland Quaestor)	1 employee	Dutch Association of Real Estate Brokers and Valuers	2 employees
De Nederlandsche Bank	2 employees		
Customs Service	1 employee		
Europol	2 employees	Public Prosecution Service	1 employee
Financial Expertise Centre (FEC, *Financieel Expertise Centrum*)*	2 employees	Rabobank	1 employee
		De Volksbank	2 employees

* The FEC is a partnership of the AFM, Tax and Customs Administration, DNB, FIOD, FIU-the Netherlands, Netherlands Police and OM. The Ministry of Finance and the Ministry of Justice and Security act as observers. Chapter 5 discusses the FEC in more detail. Also see: www.fec-partners.nl.

** Justis, the screening authority of the Ministry of Justice and Security, implements the Legal Entities (Supervision) Act (*Wet controle op rechtspersonen*).

Thanks to the interviews, a better understanding was gained of the mutual relationship between money laundering threats as well as the relationship between the threats and any underlying offences. As a result of these interviews, the list of the 10 greatest money laundering threats (see Chapter 4) discussed with the experts at the beginning of the second expert meeting was provisionally adjusted and expanded.

5 Second expert meeting

Representatives from 16 expert organisations took part in the second expert meeting (see Appendix 3). Most of these were the same persons who took part in the first expert meeting.[34] The earlier subsection discussed how the in-depth interviews led to a provisional adjustment and expansion of the list of the greatest money laundering threats. These changes were discussed with and approved by the experts at the beginning of the second expert meeting. This resulted in a more precise formulation of some of the identified money laundering threats, the breakdown of some money laundering threats that were still combined as a single threat in the first expert meeting (therefore, these were broken down into multiple money laundering threats) and the decision to not include one of the money laundering threats in the next assessment phase. The final list of the 15 greatest money laundering threats (see Table 10 in Chapter 4) formed the basis for the second and third expert meetings.

After having jointly arrived at a final list of the 15 greatest money laundering threats at the second expert meeting, the experts assessed the potential impact of these threats. This was done via a Multi-criteria Analysis (Box 3).

34 Three expert organisations delegated a different representative than at the first expert meetings. In addition, two organisations that were invited, i.e. FIU-the Netherlands and Holland Quaestor, were not present at the second expert meeting.

Box 3 Multi-criteria Analysis (MCA)

An MCA is a method of arranging a series of policy or decision-making alternatives as rationally as possible. A set of criteria is prepared for assessing and ranking the decision-making alternatives based, for example, on aspects such as costs, safety, environmental quality, social consequences, feasibility and acceptability. For each alternative and each assessment criterion, weighting scores are assigned by experts or other parties involved, which are subsequently standardised. After this, the scores are added up for each decision-making alternative. The alternative with the highest score is regarded as that which best meets the requirements of the specific decision-making situation.
For example, when it comes to purchasing a new car, criteria such as purchase costs, fuel consumption and colour may play a role in the decision-making. The decision-making alternatives consist of the two cars remaining after a pre-selection process: a blue Volkswagen and a red Ford. The purchase decision is determined based on the criteria of purchase costs, fuel consumption and colour.
These criteria may differ in the extent to which they are considered important for the decision to be taken. In an MCA, the criteria are assigned a weight, for example, on a scale of 1 to 10. For example, purchase costs are assigned a weight of 8, fuel consumption a weight of 9 and the colour of the car a weight of 6. Then it is determined how the cars score on these criteria (on a scale of 0 to 100). This results in a table in the following format:

Criteria:	Criterion weight	Volkswagen	Ford
Purchase costs	8	60	75
Consumption	9	90	60
Colour	6	80	60

The purchase costs of the Volkswagen are higher than the Ford, but the fuel consumption is much lower and the buyers find the colour of the Volkswagen more attractive. Using an MCA helps to organise the decision-making alternatives. The effects matrix resulting from the above data shows that the choice for the Volkswagen is the most rational choice.

Criteria:	Volkswagen	Ford
Purchase costs	48	60
Consumption	81	54
Colour	48	36
Total score	**177**	**150**

In the NRA, the MCA has been applied within the previously described GDR environment (see Box 2). One of the lessons learnt in the first NRA was that although using an MCA adds value, the criteria used for the analysis need to be reconsidered. Therefore, some adjustments have been made to the criteria used for this second Money Laundering NRA (see Table 4).[35] The aim of using an MCA is to reduce the

35 The MCA criteria used in the first Money Laundering NRA of 2017 were as follows: (1) the stability of the financial system, (2) the regular economy, (3) society: social order and legal order, (4) the degree to which regular society is interwoven with the criminal underworld, (5) the manifestation or facilitation of crime or terrorist activities, (6) the (perceived) feeling of safetyand (7) the Netherlands' image/reputation. In practice, some of the criteria turned out to be less distinctive in nature since they were scored above average for almost every risk by the experts. This mainly concerns the criteria of the degree to which regular society is interwoven with the criminal underworld and the manifestation or facilitation of crime or terrorist activities.

effect of some potential drawbacks of an expert-oriented approach, in the sense that the expert assessments are partly subjective and/or determined by organisational or other interests.

The experts were first asked to assign a weight to the six criteria that form part of the MCA. This clearly indicated the criteria that experts considered more or less important in determining the potential impact of the threats (see Table 5 for the applied criteria). The mean values of the weights assigned by the experts were determined. These mean values served as the applied criterion weights used to calculate the potential impact.

Table 4 MCA Criteria

Criteria:
Deterioration in the stability of the financial system
Undermining of authority and the legal order
Damage to the regular economy
Disruption of the social order
Damage to the image of the Netherlands abroad
Reduction of subjective/objective security

Subsequently, for each threat and criterion, the experts assessed the possible consequences of the money laundering threats on the six above-mentioned criteria (on a scale of 0 to 100). Here, the experts were requested to keep in mind the Dutch context within which the money laundering threats might occur. For this, the WODC delivered a short presentation on the Dutch context at the expert meeting prior to the assessment. While assessing the potential impact, the experts were also asked to estimate the probability of the threats occurring. The experts were asked to refrain from assessing the potential impact of the money laundering threats if they felt they were not qualified to do this.

The results[36] of the first round of assessment were then jointly discussed. This was followed by the second and final round of assessment, in which the experts were given the chance to adjust the assigned scores based on the plenary discussion of the first-round results.

6 Third expert meeting

Fifteen experts took part in the third expert meeting; most of them were the same people who attended the second expert meeting (see Appendix 3).[37] Prior to the expert meeting, a longlist of policy instruments was sent to the experts via an email survey. They were asked to indicate how they thought the aforementioned policy instruments contributed to the prevention and/or suppression of money laundering. They were also asked about existing policy instruments that were missing from the longlist sent to them and about other policy instruments that did not yet exist but

36 In the MCA, the Potential Impact of the threats is calculated by applying the following formula:

$Potential\ Impact = \frac{\sum(C_i \times G_i)}{\sum G_i}$, where 'C' and 'G' represent the scores assigned by experts to the criteria (C) and the weights (G) and 'i' refers to the specific criterion. The applied criteria are listed in Table 4.

37 Two expert organisations (the OM and Dutch Customs) delegated a different representative at the third expert meeting than at the second expert meeting. In addition, three organisations were missing from the third expert meeting, i.e. ING, the NVGTK and NOvA. FIU-the Netherlands and Holland Quaestor participated in the third expert meeting despite not having participated in the second expert meeting.

which they felt might contribute significantly to the prevention and/or suppression of money laundering. The findings of the email survey formed the input for the third expert meeting. The plenary discussion of the various policy instruments resulted in an overview of the existing policy instruments that experts believe could play an important or very important role in the prevention and suppression of money laundering (see Chapter 5).

Thereafter, the experts were requested to assess the extent to which the total set of existing policy instruments for the prevention and suppression of money laundering could counteract the greatest money laundering threats. However, the experts were requested to refrain from assessing the resilience if they felt they were not qualified to do this. An initial round of assessment was followed by a detailed plenary discussion of the results. Subsequently, as part of the second round of assessment, the experts were given the opportunity to adjust the earlier assessment based on any new insights that may have arisen after the plenary discussion.

After the end of the third expert meeting, the expert assessments of the potential impact of greatest money laundering threats (second expert meeting) and the resilience of the policy instruments (third expert meeting) were compared. This yielded the final result of the NRA: the list of the greatest money laundering risks in the Netherlands ranked by the RPI (Residual Potential Impact) of these risks.

7 Quantitative data analysis

As noted earlier, one of the lessons drawn from the first Money Laundering NRA was that the second NRA and subsequent NRAs must increasingly become more data-driven and more evidence-based. Supplementing the expert assessments with quantitative data creates the possibility of an initially limited form of triangulation, through which one can determine the extent of convergence between the analysis results obtained from these independent methods and reduce the dependence on the potentially and partly subjective expert assessments.

In the preliminary phase of the second Money Laundering NRA, exploratory interviews were held with nine organisations that could have quantitative data relevant for determining the prevalence and/or potential impact of money laundering risks. Table 5 provides an overview of these interviews.

Table 5 Exploratory interviews for the quantitative data analysis

Organisation	Number of of interviewees
Dutch Authority for the Financial Markets	1 employee
Financial Supervision Office	2 employees
Wwft Monitoring Office	2 employees
De Nederlandsche Bank	3 employees
Customs Service	2 employees
Financial Intelligence Unit – the Netherlands	2 employees
Netherlands Gambling Authority	2 employees
Information Exchange on Criminal and Unexplained Wealth (iCOV, *Infobox Crimineel en Onverklaarbaar Vermogen*)	3 employees
Public Prosecution Service	2 employees

Of the interviewed parties, iCOV turned out to be the most promising party in the context of the assessment.[38] As part of its mandate, iCOV has access to a large number of data sources that could be relevant for carrying out a quantitative data analysis for this NRA. This includes data from the Tax and Customs Administration, Netherlands Police, OM, FIOD, Netherlands Police Internal Investigations Department (*Rijksrecherche*), FIU-the Netherlands, Chamber of Commerce, Netherlands' Cadastre, Land Registry and Mapping Agency (*Kadaster*) and DNB. In cooperation with iCOV, the WODC investigated whether a combination of the data sources available to them could possibly offer in-depth insight into the greatest money laundering risks. Based on this, it was decided to initially focus the quantitative data analysis in the NRA on three money laundering risks, i.e. money laundering via ABC transactions, money laundering via loan-back arrangements and money laundering via legal entities (see Chapter 4 for more information on this).

iCOV operates in accordance with a covenant concluded between the participating organisations (which are mentioned in Footnote 38). The data extraction and analysis reports required for the NRA fall outside the scope of the standard reports that iCOV is able to provide on request to its cooperation partners, so these had to be specially developed for the purpose of the NRA. The protocols that bind iCOV allow scope for this.[39] However, a consent procedure based on a specific research proposal needs to be carried out separately for all the data source holders from whom data are requested. These consent procedures were initiated based on a research proposal for a quantitative data analysis focused on the aforementioned money laundering risks (which is described in more detail in Appendix 7). The proposed quantitative data analysis would be based on data from the Land Registry and Mapping Agency, Tax and Customs Administration and Chamber of Commerce, combined with data on suspicious transactions and financial and economic crime. Unfortunately, despite iCOV's efforts, it failed to complete these consent procedures

38 iCOV is a partnership of the Tax and Customs Administration, Customs Service, Netherlands Police, OM, FIOD, Netherlands Police Internal Investigations Department, FIU-the Netherlands, special investigative bodies of the Human Environment and Transport Inspectorate (*Inspectie Leefomgeving en Transport*), the Dutch Food and Consumer Product Safety Authority (*Nederlandse Voedsel- en Warenautoriteit*) and the Inspectorate SZW (*Inspectie SZW*). In addition, the Central Fine Collection Agency (CJIB, *Centraal Justitieel Incassobureau*), DNB, AFM and Dutch Media Authority (*Commissariaat voor de Media*) are also part of this cooperation. See: https://icov.nl/.

39 This refers to the scope for performing scientific research based on the sources available at iCOV. This is laid down in the iCOV Research and Development Data Processing Protocol 2018 (*Protocol gegevensverwerking iCOV Research and Development 2018*). See: https://zoek.officielebekendmakingen.nl/stcrt-2019-11305.pdf.

for all the relevant parties within the timeframe available for the NRA. As a result, the joint analysis by iCOV and the WODC could not ultimately be performed.

When it became increasingly clear during the course of the research that such a joint analysis was not possible, alternative sources were sought that might enable a quantitative data analysis to be carried out, and Justis, the screening authority of the Ministry of Justice and Security, was contacted for this. As part of its task relating to the supervision of legal entities, the TRACK department of Justis has access to the Commercial Register of the Chamber of Commerce. For individual risk reports or for the purpose of identifying the networks surrounding a specific legal entity, criminal and tax data can also be added to the data from the Chamber of Commerce. The legal basis for this is laid down in the Legal Entities (Supervision) Act (also see Chapter 5). However, this Act does not contain a provision for more large-scale use of criminal and tax data for scientific research. Therefore, such information cannot be added to the other data from the Chamber of Commerce for the purpose of a quantitative data analysis as intended in this NRA. This means that only the data from the Commercial Register could be used for compiling the aggregated data sets as described in our research proposal. Hence, the quantitative data analysis is limited to the risk of money laundering via legal entities.

8 Validating interviews

In the final research phase, the list of the greatest money laundering risks ranked by their RPI was presented to and discussed with representatives of the AMLC, FIU-the Netherlands, ING, the Ministry of Finance (Financial Markets), the Ministry of Justice and Security (Directorate for Law Enforcement and Crime Fighting) and the OM. In the interviews, the list of greatest money laundering risks was reviewed and the respondents were asked whether they agreed with the listed risks and the ranking of the risks and whether they could identify any opportunities for improvement with regard to the resilience of the policy instruments.

Table 6 Validating interviews

Organisation	Number of of interviewees
Anti-Money Laundering Centre	1 employee
Financial Intelligence Unit – the Netherlands	2 employees
ING	2 employees
Ministry of Finance	2 employees
Ministry of Justice and Security	2 employees
Public Prosecution Service	1 employee

3 What makes the Netherlands vulnerable to money laundering?

The first step in the ISO 31000 risk management system is to perform a context analysis. The context analysis presented in this chapter is structured based on the characteristics that might influence the prevalence of money laundering in the Netherlands. The chapter starts by describing a number of geographic and demographic characteristics of the Netherlands and then goes on to examine various sociocultural, economic and criminological characteristics of our country.

3.1 Geographic and demographic characteristics

The Netherlands, located in the north-west of Europe, is one of the 27 Member States of the EU (i.e. the number of remaining Member States after the exit of the UK from the EU on 31 January 2020). The Netherlands has over 17 million inhabitants.[40] With about 500 inhabitants per square kilometre, the Netherlands is, after Malta, the most densely populated country in the EU (excluding some European city-states).[41] Under the Schengen Agreement, citizens of the 26 participating countries in Europe, which includes the Netherlands, can travel freely within the Schengen Area; border controls have been discontinued between Schengen member countries.[42] The Netherlands is also part of the European Economic Area (EEA). The EU and three of the member countries of the European Free Trade Association (EFTA) – i.e. Liechtenstein, Norway and Iceland – together form the EEA.[43] Within the EEA, there is free movement of goods, persons, services and capital.[44]

Since 2010, the islands of Bonaire, Sint Eustatius and Saba (the so-called BES islands) in the Caribbean, with a total of approximately 25,000 inhabitants, have been part of the Netherlands as three separate public bodies (special municipalities).[45] The BES islands are also referred to as the Caribbean Netherlands. Until 2010, the three islands were part of the Netherlands Antilles, a former country within the Kingdom of the Netherlands. Besides the Netherlands, the Kingdom of the Netherlands also consists of the three other countries: Aruba, Curaçao and Sint Maarten.

The Netherlands is a low-lying country: 26% of the Netherlands is below sea level. Without dunes and dikes, 60% of the Dutch surface area would regularly be underwater.[46] Several major rivers such as the Rhine, Maas and Waal flow through the Netherlands and serve as important trade routes. The country lies at the North Sea

40 Statistics Netherlands (CBS, *Centraal Bureau voor de Statistiek*). See: https://opendata.cbs.nl/statline/#/CBS/nl/.

41 https://ec.europa.eu/eurostat/web/population-demography-migration-projections/data/main-tables.

42 www.europa-nu.nl/id/vh1alz099lwi/schengen_en_visabeleid.

43 At the time of writing the report (March 2020), it is still unclear whether the UK will remain a part of the EEA after Brexit.

44 www.europa-nu.nl/id/vh7dosyo6lu1/europese_economische_ruimte_eer.

45 This NRA does not address the money laundering risks with respect to the BES islands. A separate NRA is carried out for the BES islands.

46 Ministry of Infrastructure and the Environment (2015).

with one of the largest ports in the world, the Port of Rotterdam, situated nearby (see the next section).

3.2 Sociocultural characteristics

In 'Discovering the Dutch', a standard reference work on Dutch politics, economy, history, culture and society, the Netherlands is characterised as a modern, densely populated, internationally oriented country with a multitude of foreign trade relations, migration movements, cultural exchanges, networks, alliances and partnerships.[47] The Netherlands is a constitutional monarchy with a long democratic tradition, an internationally oriented economy with an extensive welfare system and a consensus-based political culture. According to Besamusca and Verheul, the key elements for Dutch culture and society can be summed up in the interrelated concepts of 'pillarisation' (separation of Dutch society based on the 'pillars' of society), tolerance and the 'Polder Model' (Dutch practice of policymaking by consensus between government, employers and the trade unions).[47] These elements are discussed below.

Until the mid-1960s, the Netherlands was largely organised based on the so-called pillars of society, i.e. along the lines of religious and political denominations. Institutions such as schools, associations, political parties, trade unions and broadcasting organisations separated by denomination existed alongside one another and separate from one another. In the sixties, the process of secularisation picked up in the Netherlands and the extent of 'pillarisation' gradually decreased. But this does not alter the fact that Dutch society today still shows many traces of its 'pillarised' past, for example, in its political parties, broadcasting organisations, employee organisations and educational institutions.

Dutch tolerance dates back to the sixteenth century, when the Republic of the United Netherlands was the first country in the world to introduce a form of religious freedom.[48] This attracted an influx of religious refugees from other countries. However, a closer look reveals that Dutch religious freedom was more about a kind of 'toleration in law' by not enforcing certain laws, rather than tolerance in the full meaning of the term. At the time, authorities had insufficient power to enforce religious conformity. They also recognised the importance of maintaining good mutual relationships between various communities.[48]

With the rise of secularisation, a new, more individual-oriented view of mankind emerged in the Netherlands from the 1960s, with an emphasis on personal development, entrepreneurship, creativity and self-expression. This cultural revolution did away with the old values of conformity and formed the basis for a new period of 'toleration in law' and tolerance, especially in the fields of homosexuality, emancipation, abortion, same-sex marriage, soft drugs and euthanasia.

During the same period, the Dutch economy developed rapidly and vigorously, partly as a result of the exploitation of the enormous natural gas field discovered in Slochteren in 1959. The hitherto-indigenous Dutch labour force could not meet the growing demand for labour, and as a result, workers were recruited from abroad who would temporarily work and stay in the Netherlands. At first, these migrant

47 Besamusca and Verheul (2010).

48 Mijnhardt (2010).

workers came from southern European countries with a Christian culture, but they later also came from Islamic countries, especially Turkey and Morocco. Many of these immigrant workers ended up settling permanently in the Netherlands. Hence, by 2019, nearly 25% of the Dutch population had a migration background, almost half of whom had been born in the Netherlands.[49] Following the 9/11 attacks in New York and other attacks in Europe by jihadist-inspired terrorists, tolerance towards Muslims in the Netherlands declined. This is reflected in the rise of anti-Islamic political parties in the Netherlands. On the other hand, the Netherlands has also recently seen the rise of political parties that focus specifically on promoting the interests of population groups with a migration background.[50]

The Polder Model is characterised by a collaboration between parties with differing interests, where the parties seek consensus and compromise.[51] Although the application of the Polder Model involves a time-intensive process, it offers a great advantage in the sense that all the relevant parties are involved and their interests can be taken into account in the decision-making. Decisions taken via the Polder Model can, therefore, count on broader support. The Polder Model is widely applied, for example, in negotiations on working conditions and wages between government, trade unions and employer organisations, as well as in the decision-making on care and education. The Polder Model approach can also be seen in the formation of Dutch governments. In the Dutch elections, none of the political parties can count on obtaining an absolute majority of votes. Parties must therefore collaborate and form coalitions with other parties to form a government. Therefore, in keeping with the culture of the Polder Model and compared to most other countries, a relatively large number of initiatives for preventing and combating money laundering have been developed in the Netherlands, whereby organisations seek to cooperate with other organisations to counter money laundering in a more effective manner (see Section 5.5). This includes public-public, public-private and private-private partnerships.

3.3 Economic characteristics

General
In 2018, the Netherlands recorded a Gross Domestic Product (GDP) of USD 53,106 per capita. According to the Organisation for Economic Co-operation and Development (OECD), the Netherlands has one of the world's highest GDPs per capita.[52] In 2019, the Netherlands was ranked fourth among the most competitive economies in the world by the World Economic Forum.[53] This made it the highest-ranked European country. According to the World Economic Forum, the high position of the Netherlands is due to its optimal score of 100 on macroeconomic stability (inflation and debt), a world-class infrastructure, high-quality health care, a highly skilled workforce and a continuing focus on innovation. Other strong economic sectors in the Netherlands include the chemical, logistics and horticultural sectors.[54]

49 www.cbs.nl/nl-nl/dossier/dossier-asiel-migratie-en-integratie/hoeveel-mensen-met-een-migratieachtergrond-wonen-in-nederland-.

50 https://nos.nl/artikel/2216178-aanbod-aan-migrantenpartijen-sterk-toegenomen.html.

51 Van Zanden (2010).

52 https://stats.oecd.org/index.aspx?DataSetCode=PDB_LV#.

53 World Economic Forum (2019).

54 www.topsectoren.nl/.

In the Dutch economy, the contribution of the services sector has rapidly increased in recent decades. In 1969, the share of commercial and non-commercial services was less than 56% (and that of the goods sector therefore as high as 44%). In contrast to this, in 2016, the share of the services sector was as high as 78%.[55]

Schiphol and the Port of Rotterdam
The Netherlands has one of the largest airports in the world. According to Airports Council International, Schiphol ranks eleventh in terms of passenger numbers with more than 71 million passengers in 2018, which includes both domestic and international flights. Only London Heathrow Airport and Paris-Charles de Gaulle Airport rank higher within Europe. When it comes to international air traffic, Schiphol ranks fourth and only Dubai International Airport, London Heathrow Airport and Hong Kong International Airport have higher passenger numbers than Schiphol. With regard to freight transport, Schiphol occupies the twentieth position in the world and the fourth place in Europe.[56]

According to the 2019 edition of the 'One Hundred Ports' report published by Lloyd's List, the Port of Rotterdam was the tenth largest container port in the world in 2018. Rotterdam is preceded by seven Chinese ports and ports in Singapore, Malaysia and the United Arab Emirates. The Port of Rotterdam occupies the highest position in Europe.[57]

The ports of entry to the Netherlands are used for the import and export of laundered money and criminal proceeds, for example, for international movements of cash and the transport of high-value or other products.

Financial sector
The Netherlands has a relatively large and internationally oriented financial sector, with assets worth more than seven times (725%) the GDP in the third quarter of 2019).[58] This represents a decline compared with the amount stated in the first Money Laundering NRA of 2017[59], when the size of the financial sector was 770% of GDP.

In terms of asset size, the banking sector forms almost half of the financial sector and is largely made up of three major banks: ING, Rabobank and ABN-AMRO.
In 2018, the balance sheet total of all banks amounted to EUR 2,234 billion.[60] ING is the largest bank with a balance sheet total of EUR 887 billion, followed by Rabobank (EUR 590 billion) and ABN-AMRO (EUR 381 billion). In the third quarter of 2019, assets of Dutch banks amounted to more than three times (319%) the Dutch GDP.[61] Although this is a decrease compared to figures in the first Money Laundering NRA

55 CBS (2017).

56 These are provisional figures, since the final figures had not yet been published on 20 February 2020. https://aci.aero/news/2019/03/13/preliminary-world-airport-traffic-rankings-released/.

57 https://lloydslist.maritimeintelligence.informa.com/one-hundred-container-ports-2019/.

58 Own calculation based on figures from DNB (https://statistiek.dnb.nl/downloads/index.aspx#/?kindofproduct=mainproduct) and the GDP from the 2020 Budget Memorandum (*Miljoenennota*).

59 Van der Veen & Heuts (2017a).

60 www.banken.nl/nieuws/21731/ranglijst-grootste-nederlandse-banken-2019.

61 www.ebf.eu/the-netherlands/.

(385%),[62] the Dutch banking sector remains relatively one of the largest banking sectors in Europe.[63]

Within the Dutch financial sector, insurance companies comprise the smallest sector, with assets amounting to 67% of GDP, a slight decrease compared with the first NRA (75%).[64] The Dutch pension system is relatively the largest in the world with a volume of almost 220% of GDP in the third quarter of 2019, an increase of 20% compared with the figures from the first Money Laundering NRA.[65] Finally, the relative size of investment institutions in the Netherlands in the third quarter of 2019 amounts to 118% of GDP. In the first Money Laundering NRA, this was 113%.[66]

Many of the money laundering methods make use of the financial sector, for example, wire transfers by banks, trade-based structures involving services or goods, ABC transactions, loan-back arrangements, etc. (see Chapter 4 for more information on these money laundering methods).

Table 7 Size of the financial sector in the Netherlands (third quarter of 2019)

Sector	Number of institutions	Assets (in billions of €)	% Total assets	% GDP
Banks	78	€2,614	44%	319
Insurers	152	€549	9%	67
Pension funds	227	€1,800	30%	220
Investment institutions	1,676	€969	16%	118
Total	**2,133**	**€5,932**	**100%**	**725**

Source: De Nederlandsche Bank (https://statistiek.dnb.nl/downloads/index.aspx#/?kindofproduct=mainproduct; consulted on 26 February 2020) and the GDP from the 2020 Budget Memorandum.

Tax attractiveness and the role of trust offices

At the end of 2018, the CBS (Statistics Netherlands) reported that the majority of incoming foreign investments do not remain in the Netherlands but are immediately channelled abroad via special financial institutions[67] (BFI, *Bijzondere Financiële Instellingen*) or letterbox companies. In 2015, there were more than 14,000 BFIs in the Netherlands. The CBS indicates that minimising tax payments is the most important motivation for multinationals to set up a BFI in the Netherlands. The Netherlands is one of the countries worldwide with the highest levels of incoming and outgoing foreign direct investment, including share capital and lending. In 2017,

62 Van der Veen & Heuts (2017a).

63 www.banken.nl/bankensector/bankensector-nederland.

64 Van der Veen & Heuts (2017a).

65 Van der Veen & Heuts (2017a).

66 Van der Veen & Heuts (2017a).

67 BFIs are companies or institutions that, irrespective of their legal entity, are considered resident for tax purposes and in which non-residents directly or indirectly participate or exert influence via share capital or otherwise and which, in combination with other domestic group undertakings or otherwise, have as their object and/or are largely occupied with the following: 1. holding assets and liabilities mostly located abroad and/or 2. channelling turnover consisting of royalty and licensing revenues obtained abroad to foreign group companies and/or 3. generating turnover and expenses that have mainly originated from re-invoicing from and to foreign group companies. See: https://wetten.overheid.nl/BWBR0014656/2018-05-01.

about 80% of these investments – totalling EUR 3,655 billion – went directly to a foreign destination via a BFI.[68]

Various studies have been conducted on the tax attractiveness of the Netherlands for companies. Due to differences between these studies in terms of definitions, scope and methods, the extent of the effective Dutch tax burden for companies is unclear. However, the studies clearly show that the effective tax burden for companies is lower than the official profit tax rate of 25%. In a study conducted by Janský over the period 2011-2015 among 63 countries, including the (then 28) EU member states, the Netherlands emerged as an EU country with a favourable tax climate for large multinational companies. Due to the options offered by the Netherlands for saving on the tax paid on profits, the effective rate in this study emerges as slightly higher than 10%. According to the study, multinationals in four countries in the EU, i.e. Luxembourg, Hungary, Bulgaria and Cyprus, pay lower effective taxes on profits than in the Netherlands.[69]

An OECD study on the effective tax burden for companies has calculated that companies in the Netherlands pay an average of 23% as tax on profits.[70] In this study, no distinction is made between the effective tax burden for different types of companies. Recent research by the CBS focuses on the tax burden of large companies, i.e. non-financial companies with a balance sheet total of more than 40 million euros.[71] The research shows that the effective profit tax burden for these large companies in the Netherlands decreased between 2006 and 2017 from 23.9% to 17.1% and that foreign companies and multinationals with their headquarters abroad pay lower effective taxes on profit than similar large companies established in the Netherlands. These percentages are higher if the loss-making components included by companies on the balance sheet are also taken into account. The CBS exercise makes it clear that determining the effective profit tax burden is a complex matter, where it is not possible to make adjustments for all aspects that are important for determining the effective tax burden of companies.[72]

Partly because of its tax system, the Netherlands is seen by companies as an attractive country in which to set up a business. An unintended side effect of the tax system is that this allows for tax avoidance structures. Various studies have been conducted in recent years on the extent of tax avoidance. According to Lejour, the Dutch tax environment costs the rest of the world an estimated USD 21 billion annually in avoided tax revenue.[73] The European Parliament calculated that the tax regime in the Netherlands for multinationals costs the other EU countries around EUR 11 billion in tax revenue.[74] The results are not entirely clear, partly due to the use of different methods and data sources and the incompleteness and unreliability of the data.[75]

---

68 www.cbs.nl/nl-nl/nieuws/2018/50/80-procent-inkomende-investeringen-direct-doorgesluisd.

69 Janský (2019).

70 OECD (2019).

71 CBS (2019b).

72 CBS (2019b).

73 Lejour (2020). The average tax benefit was determined based on ten international studies of the worldwide tax benefit for multinational companies. The Dutch share was calculated on the basis of incoming and immediately outgoing foreign investments.

74 Lejour (2020).

75 Blouin & Robinson (2019).

From 2021 onwards, the Netherlands will limit the options for tax avoidance available to multinational companies. From then on, tax will be levied on multinational corporate profits on intellectual property that is channelled through the Netherlands to recognised tax havens such as Bermuda or the Cayman Islands.

In recent years, there has been a declining trend in the number of licensed trust offices established in the Netherlands. At the end of 2011, there were 310 trust offices in the Netherlands, but this number decreased to 170 in February 2020.[76, 77] The services provided by a trust office may include serving as a director of a legal entity or company or providing a postal address and administrative services. In addition, a trust office may act as a conduit company[78].

Conduit companies are often used to facilitate the exploitation of intellectual property such as image rights, royalties and licences and for the provision of consultancy services, commercial activities and loans.[79] For internationally operating companies, it may be more efficient to have a Dutch legal entity or company managed by a trust office. The services provided by trust offices are often motivated by tax purposes.

Large companies, artists, top athletes and world leaders use the services of Dutch trust offices because of the related tax benefits. Large amounts are involved in the Dutch trust sector: an estimate by SEO Economic Research in 2013 calculated that approximately EUR 4,000 billion flows in and out of the Netherlands every year via trust offices.[80]

Complex structures by trust offices can be used to disguise the origin of illegally gained funds.

Export

In 2018, the Netherlands was one of the top five largest exporters in the world, with USD 724 billion in exports. Only China, the United States, Germany and Japan are ranked higher than the Netherlands.[81] In 2018, total exports of products and services amounted to 34% of GDP. Almost 71% of exports were to other EU countries, mainly Germany, Belgium, the United Kingdom and France.[82] The main export pro-

76 DNB, Trust Offices Register, see: www.dnb.nl/toezichtprofessioneel/openbaar-register/WTTTK/index.jsp?filter_value=&naam=Statutaire+naam+%2F+Handelsnaam.

77 The interim report on supervision dated 19 November 2019 issued by DNB states that the stricter requirements and the correspondingly strict supervision have made some trust offices realise that it is not possible for them to comply with these tighter requirements. Or they have concluded that the costs associated with this 'are too high, as a result of which it is no longer feasible or profitable to continue these activities'. Annex 920439 Parliamentary Paper 31 477, No. 50.

78 In the Trust Offices (Supervision) Act 2018 (Wtt 2018, *Wet toezicht trustkantoren*), five different types of services are qualified as trust services. One of these services is to offer to act as a conduit company. If a conduit company service is offered to customers, this is considered a trust service. A conduit company (also known as an in-house company) is a company that belongs to the same group as the trust office and that is used by the trust office on behalf of one or more clients. Conduit companies may be used for exploiting intellectual property (for example, image rights, royalties and licences) or for providing consultancy services, commercial activities and loans. See: https://www.toezicht.dnb.nl/2/50-226561.jsp.

79 DNB (2019).

80 Kerste et al. (2013).

81 World Trade Organization (2019).

82 CBS (2019a).

ducts are machines and machine parts, metal and metal products, floriculture, natural gas and high-quality plastics.[83] Compared to the results included in the first Money Laundering NRA[84], there is a noticeable decrease in the export of natural gas. Natural gas is now the fourth-ranked export product, while it occupied the second place in the first NRA.

In addition to goods, the Netherlands also exports many services. Business services and the use of intellectual property form the largest categories. Business services include research and development (R&D), professional and management advisory services and technical business services.[85] Although only about 2% of the Dutch population works in the agriculture and fisheries sector,[86] the Netherlands is the world's largest exporter of food and agricultural products after the United States thanks to its focus on far-reaching innovation and mechanisation.[87]

The export of products or services may be used to launder criminal proceeds, for example, via the use of trade-based structures involving goods or services.

Cash is a less popular means of payment
The number of cash payments in the Netherlands decreased by 42% between 2010 and 2018: from 4.37 billion payments in 2010 to 2.53 billion payments in 2018. In this period, the value of cash payments decreased from EUR 52 billion to EUR 34 billion, a decrease of 34%. Between 2017 and 2018, the share of cash payments of the total number of retail payments decreased from 41% to 37%. The share of debit card payments increased from 58% to 63% during this period.[88]

There are much fewer cash transactions in the Netherlands than in other European countries. According to a study performed by the European Central Bank (ECB), 79% of all retail payments in the Eurozone were made in cash in 2016. Cash was used least in the Netherlands, Estonia and Finland in 2016. In the Netherlands, the percentage of cash transactions was 45%. The Netherlands was the only country in the Eurozone where debit card payments were more frequent (55% of all transactions) than cash payments.[89]

Money laundering via cash remains an important element in criminal sectors where a lot of money is paid in cash, such as in the drugs scene. In legal sectors, a lot of cash transactions still occur via street sales (mainly markets), in the hospitality sector and in services (such as hairdressers, nail studios, massage and beauty salons and laundromats). These cash-intensive sectors are regularly associated with money laundering.

83 www.cbs.nl/nl-nl/nieuws/2019/45/hoogste-exportverdiensten-dankzij-machines; CBS (2019a).

84 Van der Veen & Heuts (2017a).

85 CBS (2019a).

86 www.cbs.nl/nl-nl/visualisaties/dashboard-arbeidsmarkt/banen-werkgelegenheid/toelichtingen /werkgelegenheidsstructuur.

87 www.weforum.org/agenda/2019/11/netherlands-dutch-farming-agriculture-sustainable/.

88 DNB/Dutch Payments Association (2019).

89 ECB (2017).

Digital society[90]
In 2017, the Netherlands had the highest percentage (98%) of households with internet access among all EU countries. Apart from the Netherlands, more than nine out of 10 households had internet access in 2017 in Denmark, Luxembourg, Finland, Sweden, the United Kingdom and Germany as well.

3.4 Criminological characteristics

Recorded money laundering offences and cases
In 2019, according to the CBS, the police recorded approximately 1,400 money laundering offences. In recent years, there has been an upward trend in this type of crime: 600 money laundering offences were recorded in 2016, almost 700 in 2017 and 900 in 2018 (also see Table 8). According to the CBS, a recorded crime is one that is recorded by the police in an official report or in an official report made under oath of office. The OM data shows that the number of people involved in money laundering cases is considerably higher than the number of money laundering offences. In 2016 – the most recent year for which information is available via the Money Laundering Policy Monitor (*Beleidsmonitor Witwassen*) published in 2018 – 1,976 subjects were associated with money laundering cases.[91] The difference between the number of money laundering offences according to the CBS and the number of money laundering cases according to the OM arises from the fact that the OM takes into account the cases registered by all investigative services per individual, whereas the CBS bases its data only on police records that are per case and not per individual. In this context, a single case may involve several individuals.

Unger et al. estimated the volume of money laundering in the Netherlands in 2014 to be EUR 16 billion, based on the estimated money laundering needs of criminals. This amount consists of funds from criminal activities both obtained and laundered in the Netherlands (EUR 6.9 billion in 2014) and the inflow of laundered money from other countries (EUR 9.1 billion in 2014).[92] Based on the transactions declared suspicious by FIU-the Netherlands, the same investigation team estimated the total volume as being EUR 12.8 billion.[93]

Recorded property crime and drug crimes
Money laundering is usually preceded by some form of crime. According to the CBS, approximately 58% of crime recorded in 2019 in the Netherlands includes a property component (which also includes money laundering). Table 8 shows that this mainly concerns crimes such as theft/embezzlement and burglary, fraud and counterfeiting. The number of recorded crimes relating to human trafficking or smuggling as well as the number of recorded drug-related crimes has increased since 2017.

90 https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals/nl#Internettoegang.

91 Slot & De Swart (2018).

92 Unger et al. (2018).

93 https://www.nrc.nl/nieuws/2019/11/13/jaarlijks-wordt-in-nederland-bijna-13-miljard-euro-witgewassen-a3980118. Further information about the new estimate is not available. The report has not yet been published (as on 6 May 2020).

Table 8 Recorded* property crimes, human trafficking, human smuggling and drug-related crimes in 2016-2019

	2016	2017	2018**	2019**
Crimes, total***	930,325	832,950	786,280	817,390
Property crimes	576,445	502,510	457,815	473,310
Theft/embezzlement and burglary	498,285	428,135	380,325	374,160
Fraud	45,150	39,405	41,420	53,480
Counterfeit crime	24,710	27,380	27,725	36,055
Handling stolen goods	5,845	5,255	5,560	6,355
Extortion and intimidation	1,665	1,520	1,765	1,775
Fraudulent bankruptcy	180	115	105	95
Money laundering	610	695	900	1,390
Human trafficking, human smuggling	730	725	875	1,175
Drug-related crime	13,275	12,525	13,390	14,640
Hard drugs	6,760	6,570	7,055	7,840
Soft drugs	6,295	5,740	6,150	6,595
Drug-related crime (other)	220	215	190	200

Source: CBS Statline (2020)

* According to the CBS, the term 'recorded crime' only refers to crimes that are recorded by the police in an official report or in an official report made under oath of office.

** These are the preliminary results for 2018 and 2019.

***This includes property crimes, vandalism, crimes against public order and public authority, violent crimes, sexual crimes, drug-related crimes, traffic offences, crimes involving firearms or other weapons, other crimes defined in the WvSr as well as other crimes described in other laws.

According to the estimates of Unger et al., drugs and fraud[94] are jointly responsible for more than 90% of the money laundering needs of criminals in the Netherlands.[95] According to the Bureau of International Narcotics and Law Enforcement Affairs of the United States Department of State, financial fraud (particularly tax evasion) and drug trafficking generate a significant part of the money laundering activities in the Netherlands. This periodic report indicates that there is evidence of syndicate structures being involved in organised crime and money laundering and that these criminal networks are increasingly active online and use crypto currencies in their illegal activities.[96]

Table 8 does not give a clear indication of any recent shift from traditional forms of recorded property crime such as theft and burglary that are on the decrease, to cybercrime such as internet scams, hacking and identity fraud that are on the increase.[97] Europol's IOCTA report of 2019 also shows that cybercrime continues to develop.[98] In the field of cybercrime, a shift in focus can be observed towards larger and more profitable targets and new technologies. According to Europol, the new threats are arising not only from the use of new technologies but also through the exploitation of long-known vulnerabilities in existing technologies.

94 Fraud is a catch-all term covering many different forms of fraud, including tax fraud, social fraud and identity fraud.

95 Unger et al. (2018).

96 US Department of State. Bureau of International Narcotics and Law Enforcement Affairs (2019a).

97 CBS (2010).

98 Europol (2019).

Production of and trafficking in drugs
In various studies, the Netherlands is regarded as a major producer of and trader in various types of drugs. According to the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), an agency of the European Union, the Netherlands is a producer and exporter of cannabis and synthetic drugs and a transit country for cocaine and heroin.[99] The EMCDDA indicates that the production of MDMA in Europe is mainly concentrated in the Netherlands and Belgium. Amphetamine production in Europe takes place primarily in the Netherlands, Belgium and Poland. As far as methamphetamine is concerned, a small number of illegal laboratories are discovered every year in the Netherlands, including sizeable facilities that mainly produce for markets in the Far East and Oceania.[100] The Bureau of International Narcotics and Law Enforcement Affairs of the US Department of State indicates that the Netherlands is an important transit country for illegal drugs, especially cocaine, via the Port of Rotterdam and that it is an important producer and exporter of synthetic drugs, especially MDMA Ecstasy.[101] The 2020 Factbook published by the American Central Intelligence Agency (CIA) describes the Netherlands as a major producer of synthetic drugs such as Ecstasy, and cannabis. The CIA also describes the Netherlands as an important European 'gateway' for cocaine, heroin and hash.[102]

Low levels of corruption
According to Transparency International, the Netherlands has relatively low levels of corruption. In the most recent Corruption Perceptions Index (CPI) – which indicates the extent of corruption in the public sector in 180 countries based on expert opinions from around the world – the Netherlands ranks eighth on the list of least corrupt nations in 2019.[103] Despite the limitations of the CPI indicator, the World Bank believes that the CPI, along with its own Control of Corruption indicator, offers the most valid approach for determining the level of corruption in different countries.[104]

3.5 Conclusion

This context chapter has examined a number of specific characteristics of the Netherlands that may be connected with the prevalence of money laundering. This includes relatively fixed geographic, demographic, sociocultural, economic and criminological characteristics that cannot be influenced via policy measures or, if so, only to a limited extent and/or in the longer term.

The Netherlands is characterised by an open, trade-oriented economy, a large and internationally oriented financial sector and is fiscally attractive for large foreign companies. The country is one of the most competitive economies in the world, boasts an airport and port that are among the largest in the world and it is one of the largest exporters in the world. The Dutch economy can be described as a service economy. All these characteristics make the Netherlands attractive to criminals for laundering their criminally obtained money. Compared to other European countries, the Netherlands is characterised by relatively few cash payments and a high degree

99 www.emcdda.europa.eu/system/files/publications/11347/netherlands-cdr-2019.pdf.
100 EMCDDA (2019).
101 US Department of State. Bureau of International Narcotics and Law Enforcement Affairs (2019b).
102 www.cia.gov/library/publications/the-world-factbook/geos/nl.html.
103 www.transparency.org/cpi2019.
104 Hamilton & Hammer (2018).

of digitalisation. These factors may influence the money laundering methods used by criminals. A socio-cultural factor typical to the Netherlands is its culture of tolerance where, particularly, the tolerance towards soft drugs may contribute to the occurrence of drug-related crime and the laundering of the proceeds thereof. In keeping with the culture of the Polder Model, it is customary for Dutch organisations to seek consensus and cooperation with other organisations. In this sense, the Netherlands can be distinguished from many other countries by the relatively high prevalence and wide variety of partnerships that have been established to prevent and combat money laundering. This includes public-public, public-private and private-private partnerships.

4 Insight into the greatest threats in the field of money laundering

The purpose of the NRA is to introduce a risk-based classification for the methods possibly used by criminals in the Netherlands to launder criminally obtained funds. Due to this, the NRA's primary focus will be on the methods used for money laundering and it will focus only secondarily on the crime that precedes the money laundering activity.[105] In the Netherlands, it is not necessary to prove the underlying crime in order to criminalise money laundering. As previously stated, the NRA has been drawn up based on a longlist of money laundering threats (see Appendix 4). But not all of these threats are described in equal detail in this chapter. This chapter focuses on the methods identified by experts at the first expert meeting as the threats with the greatest potential impact (Section 4.2) given the specific vulnerabilities of the Netherlands (Chapter 3) and the barriers set up by the Netherlands against money laundering (Chapter 5). The described methods are illustrated using sample cases collected via interviews and from relevant literature and other existing sources. The case descriptions clearly show that criminals may combine different money laundering methods in order to even better conceal the criminal origin of the funds.

4.1 Background

A multitude of methods – whether or not used in combination with one another – may be used to launder criminal money. These money laundering methods may occur during the three phases of the money laundering process as distinguished by the FATF, i.e. the placement, layering and integration phases (see Chapter 1). As noted above, this chapter focuses on the money laundering methods identified by experts in the first expert meeting as those with the greatest potential impact. Moreover, the focus lies on money laundering threats that may arise in the Netherlands and can be targeted by Dutch policy to prevent and combat money laundering. This does not detract from the fact that many of the money laundering methods described in this chapter may also have an international element. However, this second Money Laundering NRA does not take into account money flows that may pass through the Netherlands via complex international money laundering schemes but do not, in principle, remain in our country. A recent example of this is the Troika Laundromat: via a complex system of anonymous companies in tax havens, the Russian Troika Bank laundered billions of funds, of which tens of millions were pre-

105 This is in contrast to, for example, the American NRA that focuses on the crime preceding the money laundering activity.

sumably channelled through the Netherlands.[106] According to Transparency International Nederland, Dutch banks are also involved in the Troika Laundromat.[107]

Section 4.3 examines in greater detail the nature and mechanisms of the greatest money laundering threats in the Netherlands, as assessed by experts. As will become clear in Section 4.3, some methods are quite simple in nature, while others are extremely complex. It will also become evident that some money laundering methods may be part of other methods and that many of the methods described may be used in combination with each other. This relationship between the individual money laundering methods is reflected in the various cases described in this chapter.

4.2 Identification of the greatest money laundering threats

Longlist of money laundering threats
Prior to the first expert meeting, a longlist containing a total of 25 money laundering threats (see Appendix 4) was presented via the FLUU Survey (see Chapter 2) to experts in the field of money laundering. These money laundering threats covered various placement methods and channels as well as layering methods. The experts were asked to indicate, for each threat, whether they are aware of facts or cases relating to the threats or whether or not they consider it likely that the threats are prevalent based on the information available to their organisation. In this survey, experts also had the opportunity to add any money laundering threats they felt were missing from the longlist.

The first expert meeting started with a joint discussion of the complete longlist of money laundering threats and a request for existing cases relating to each of the threats. Based on this discussion, all the experts got the chance to learn about the nature of the threats (in a general sense) and the prevalence of these threats as assessed by experts. This method of working was aimed at creating a common frame of reference regarding the money laundering threats and to ensure that the experts were, as far as possible, on the same page in terms of information about and understanding of the threats. During the plenary discussion, some of the threats were combined while others were split up and/or formulated more precisely. For example, some experts indicated that money laundering via unlicensed banks is not the same as money laundering via underground banking (these threats were combined as a single item on the longlist). As a result, a separate threat of money laundering via underground banking – with the addition of the phrase 'moving money' – was added to the longlist.

After the 25 money laundering threats on the longlist had been discussed, the threats added by the experts in the email survey were also discussed. In this dis-

106 *Trouw* (Dutch daily newspaper), 5 March 2019: 'The Russian money laundering machine also runs through the Netherlands'. According to the article, the Troika Laundromat works in this manner: billions of dubiously obtained funds leave Russia through banks in Lithuania, which channel the money to other countries. This is often not done directly, but via major European banks. This also includes parts of ABN-AMRO that were sold to the Royal Bank of Scotland in 2007. Add to this a network of anonymous companies in tax havens around the world set up from Russia. The result is a washing machine in which money goes round and round and round, but where the origin of the money is not visible from the outside. As far as can be reconstructed, an estimated EUR 3.4 billion goes into the money laundering machine and EUR 3.5 billion comes out of it.

107 Rooijendijk (2019).

cussion, the experts could present their case for why they thought that some money laundering threats *should* and other threats *should not* be added to the longlist. Ultimately, two money laundering threats were added to the longlist.[108]

Identification of the greatest money laundering threats

Subsequently, from the final longlist of 27 money laundering threats, the experts were asked to identify the 10 threats with the greatest potential impact, taking into account the vulnerabilities and resilience specific to the Netherlands. The first round of identification was followed by a detailed plenary discussion of the results. After this, the experts were given the opportunity to adjust their initial assessments and the second and final round of identification took place. Table 9 shows the results[109]: the 'Number of experts' column shows the number of experts who included the threat in question in their top 10 list.

Table 9 The 10 greatest money laundering threats

Threats	Number of experts
Complex legal entities and structures (including offshore companies*, trust structures** and legal entities such as foundations)	18
Trade-based structures (including the legitimisation of value transfers via commercial transactions and over-invoicing/under-invoicing)	16
Use of straw men	16
Correspondent banking	15
Investment schemes (including loan-back arrangements and ABC transactions)	15
Crypto currencies	14
Dealers of high-value goods (cars, jewellery, art, etc.) and other dealers	13
Underground banking/physical movement of money	13
Corporate structures (including the incorporation of one's own company and holding participating interests in other companies)	12
Licensed banks: wire transfers/deposits	12

* This term is explained further in the description of the money laundering threat in question in Chapter 4.

** The trust structure originating from Anglo-Saxon legal systems is, in short, a legal construct where goods are entrusted to a trustee who uses these assets in accordance with a trust deed for one or more beneficiaries. The trust may assume many different forms and is used for different purposes within the business, family, cultural and charitable spheres. See the public consultation on the Explanatory Memorandum to Implementation Act on the registration of ultimate beneficial owners (UBO) of trusts and similar legal arrangements, https://www.internetconsultatie.nl/ubotrust.

The 10 greatest money laundering threats mentioned above formed the basis for the in-depth interviews conducted with experts after the first expert meeting. The interviews provided more insight into the precise nature and existing cases relating to the threats. The interviews also led to proposals for a more precise formulation of some of the identified money laundering threats, a breakdown of a number of threats that had been combined into a single threat at the first expert meeting and the omission of one money laundering threat from the next phase of the assess-

108 These include the threats relating to correspondent banking and currency exchange. The threat of correspondent banking, identified in the first expert meeting as a money laundering threat with the greatest potential impact, is further explained in Section 4.3. The other threat was not considered as a money laundering threat with the greatest potential impact and therefore it is not dealt with further in this NRA.

109 The complete overview of this exercise, which also includes the minor money laundering threats, can be found in Appendix 6.

ment. The experts discussed and approved these proposed changes at the beginning of the second expert meeting.

The money laundering threat relating to complex legal entities and structures has been broken down into three separate threats: money laundering via structures by trust offices, via offshore companies and via legal entities. The money laundering threat relating to investment/investment structures has been broken down into three separate threats: money laundering via investment institutions/firms, via ABC transactions and via loan-back arrangements. The threat relating to trade-based structures has been broken down into two separate money laundering threats: money laundering via trade-based structures involving services and money laundering via trade-based structures involving goods. The threat relating to underground banking/moving cash has been broken down into two separate money laundering threats: money laundering via underground banking (including unlicensed payment service providers) and via the physical movement of cash. Some of the other money laundering threats have been defined more specifically. For example, the threat relating to corporate structures has been further specified as money laundering via fictitious company turnover.

One of the identified money laundering threats, i.e. money laundering via correspondent banking, was ultimately not included in the final list of the greatest money laundering threats. This was done because this threat is very closely related to the threat involving licensed Dutch banks and their policy on correspondent banks (see Section 4.3 for more information on this). Since the decision of a Dutch bank to cooperate with a particular correspondent bank goes beyond the scope of influence of the money-laundering criminal, this threat may in most cases be regarded as a systemic risk.

These adjustments eventually resulted in the final list of the 15 greatest money laundering threats (Table 10).

Table 10 Final list of the 15 greatest money laundering threats

Greatest money laundering threats identified (First expert meeting)	Final list of the greatest money laundering threats (Second expert meeting)
Complex legal entities and structures	Money laundering via structures by trust offices Money laundering via offshore companies Money laundering via legal entities
Trade-based structures	Money laundering via trade-based structures involving services Money laundering via trade-based structures involving goods
Use of straw men	Money laundering via the use of intermediaries
Correspondent banking	-
Investment structures	Money laundering via investment institutions/firms Money laundering via ABC transactions Money laundering via loan-back arrangements
Crypto currencies	Money laundering via crypto currencies
Dealers of high-value goods and other dealers	Money laundering via dealers of high-value services/goods
Underground banking/physical movement of money	Money laundering via underground banking including via unlicensed payment service providers Money laundering via physical movement of cash
Corporate structures	Money laundering via fictitious company turnover
Licensed banks: wire transfers /deposits	Money laundering via wire transfers by licensed banks

4.3 Insight into the greatest money laundering threats

Money laundering via licensed banks
A criminal may misuse various channels when involved in the money laundering process aimed at the integration of criminal money. In order to introduce the cash obtained via criminal means into the financial system, a criminal may misuse not just the services of licensed banks but also, for example, the services of payment service providers, casinos and dealers of high-value services/goods. Criminal funds held in bank accounts can be misused via channels such as notaries, brokers, accountants, lawyers, tax consultants, trust offices and insurers. Criminals may give their money laundering activities an appearance of legality by using these channels, for example, by purchasing real estate, setting up a company or foundation or issuing invoices for commercial transactions (over-invoicing/under-invoicing) for money laundering purposes. If these professionals are not sufficiently aware of a customer's criminal acts, they may unknowingly cooperate in the money laundering process. In addition, it may be that these professionals are indeed aware of the money laundering intentions of a customer and that they are therefore consciously cooperating in the money laundering practices. Misuse of these channels often also implies misuse of the services of licensed banks because of the non-cash nature of the transactions. Money laundering via wire transfers by licensed banks is often a part of the other money laundering methods described in this chapter.

In its 2019 Financial Markets Risk Report, the Netherlands Bureau for Economic Policy Analysis (CPB, *Centraal Planbureau*) drew attention to money laundering-related risks in the business operations of Dutch banks.[110] Some Dutch banks have been used for money laundering practices and it appeared that the mandatory preventive measures to counter money laundering were not implemented sufficiently at various Dutch banks. In recent years, a number of Dutch banks reached a settlement or were fined for breach of money laundering regulations. The largest settlement was made by ING (EUR 775 million) due to 'longstanding and systematic violation of the Wwft' (see Box 4).

Box 4 Case involving money laundering via wire transfers by licensed banks*

In 2018, ING Netherlands was fined EUR 775 million by the OM for years of systematically violating the Wwft (see Chapter 5 for more information). This had been done in such a way that the bank was also accused of culpable money laundering. According to the OM, ING did not properly fulfil its role as gatekeeper of the financial system. The bank should have noticed that certain flows of money that went through the bank accounts of its own customers were possibly criminal in origin. Bank accounts of ING customers in the Netherlands were used for laundering hundreds of millions of euros between 2010 and 2016, according to the OM. An investigation by the FIOD revealed structural shortcomings at ING in the implementation of its policy to prevent financial and economic crime. Absence or incomplete customer due diligence led to ING accepting customers without sufficiently investigating the risks associated with these customers. In addition, customer relationships and bank accounts were not being sufficiently monitored, and when necessary, terminated by the bank in a timely manner. Moreover, ING Netherlands' compliance department was understaffed and insufficiently trained. According to the OM, the system of transaction monitoring – partly due to the limited

110 CPB (2019)

staff capacity – had been set up by the bank in such a way that it only generated a limited number of warnings of money laundering activities.

* www.om.nl/actueel/nieuws/2018/09/04/ing-betaalt-775-miljoen-vanwege-ernstige-nalatigheden-bij-voorkomen-witwassen.

Criminals may also indirectly misuse the services of licensed banks in the Netherlands, i.e. through so-called correspondent banks. For cross-border payments, a Dutch bank may allow the international transactions to be carried out by a foreign bank (the correspondent bank), for example, when it involves a transaction to a country where the Dutch bank does not operate. In such a situation, a foreign bank acts as agent for a Dutch bank by performing payments or other services for a customer of the correspondent bank. If a foreign correspondent bank fails to properly screen customers and/or monitor transactions, the Dutch respondent bank faces a greater risk that its services will be indirectly misused to launder criminal money. According to DNB, institutions must exercise due care when entering into correspondent banking relationships. In addition to the usual risk-based investigation, a Dutch bank must carry out an extensive customer due diligence if it enters into a correspondent banking relationship with a bank established outside the EU.[111]

Money laundering via the use of intermediaries

Just as in the money laundering threat described above, the use of intermediaries – such as or straw men or front men – is often part of other money laundering methods. This is a relatively simple layering method that criminals may use to conceal their own identity and therefore reduce the chance of being caught. There are many examples of the use of this money laundering method. For example, it may involve money mules who are used to physically move criminal cash abroad. Intermediaries may also be used to integrate criminal cash into the financial system through the purchase of high-value products (such as cars and jewellery). Furthermore, intermediaries may be used by a criminal, for example, by setting up one or more legal entities through a straw man or front man with the aim of disguising the actual control, ownership structure or right to property or an object.

Box 5 Case involving money laundering via the use of intermediaries*

In early 2020, the OM demanded a 4.5-year prison sentence for a man suspected of money laundering and participation in a criminal organisation. According to the OM, the man had laundered more than EUR 4.2 million through the bank accounts of three private limited companies (BV, *besloten vennootschap*). The suspect tried to get away scot-free by using two front men who on paper appeared to be the directors of the companies. These front men were persons with debts who had no knowledge of how to run a business. According to the OM, although the companies probably did not have any legal business activities, millions of euros were deposited into the bank accounts of the companies and transferred to bank accounts in Eastern Europe and South America over a period of about two years. Since large amounts of money were transferred, for example, to Colombia, the OM suspected that these payments were related to drugs.

* www.om.nl/actueel/nieuws/2020/01/16/katvangers-inzetten-om-42-miljoen-euro-te-verhullen.

111 DNB (2015).

Money laundering via dealers of high-value services/goods

In the opinion of experts, money laundering via dealers of high-value services/goods is one of the money laundering threats with the greatest potential impact. A criminal (or his intermediary) may purchase high-value products such as cars, precious metals, jewellery or art with cash in order to integrate illegally obtained funds into the financial system. However, it is important to ensure that the amount of cash does not exceed the level above which dealers are obliged to report such transactions to FIU-the Netherlands under the Wwft. This money laundering method may also involve 'smurfing' where, for example, several people, in collaboration with each other, purchase a certain product from a dealer and ask the dealer to split the amount over several invoices. This is how the criminal and/or the straw men try to remain below the reporting threshold. Criminals may also launder money by using the services of dealers of high-value services/goods such as through the valuing of jewellery. In such cases, a high-value dealer who is intentionally cooperating with the criminal may value the jewellery higher than the actual value. This allows the criminal to legitimise part of the illegal money through the fictitious value of the jewellery.

Box 6 Case involving money laundering via dealers of high-value services/goods*

According to the OM, a man and a woman are guilty of engaging in extensive money laundering practices for years through a business in expensive watches. Cash amounts of approximately EUR 750,000 in total have been laundered via cash deposits and money transfers and through the purchase of expensive cars, watches and other goods. The suspected man carried out large cash transactions through his company for which no personal data records were maintained. According to the OM, the suspect's spending pattern was disproportionate to his income. Although the suspect stated that the money was obtained through profit from the watch trade and loans from family, this could not be substantiated based on the administrative records. The OM accused the man of money laundering and falsification of documents, since there were no administrative records of various transactions, which means that the annual statements of the companies are false. Furthermore, the suspect did not report suspicious cash transactions of more than EUR 15,000 to FIU-the Netherlands. The man also falsified invoices, for example, an invoice for 'a toolbox' worth EUR 20 was sent for a package containing a watch worth EUR 15,000.

* www.om.nl/actueel/nieuws/2018/02/08/celstraf-en-werkstraffen-geeist-voor-witwassen-met-horlogehandel.

Money laundering via fictitious company turnover

A money laundering method through which the illegal origin of cash can be made to appear legal is carried out via small businesses where the use of cash is very common such as nail salons, hairdressers or ice cream parlours. These businesses may be owned by the criminal or by the criminal's straw men. Not only can all business investments be paid for with the criminal cash, but the company turnover can also be falsified. Criminal cash can be mixed with the legal turnover of the company, after which the total amount is reported to tax authorities as the achieved turnover.

Box 7 Case involving money laundering via fictitious company turnover*

A person involved in cannabis cultivation started a taxi company with 12 taxis with the aim of laundering the criminal proceeds. Private loans and turnover were falsified via the company. The stated turnover did not correspond with the data recorded by the taximeters.

* Soudijn & Akse (2012).

Money laundering via underground banking, including via unlicensed payment service providers

Underground banking is a form of financial services offered outside the formal financial system, mainly by transferring cash abroad. The term 'underground banking' in this second NRA includes not only hawala banking and similar forms of banking but also the services of unlicensed PSPs.

Underground banking is an ancient tradition in the Middle East and Far East and is also referred to as hawala (the Middle East and India), hundi (Pakistan) or Fei-chien (China). This form of banking uses a system based on trust and settlement. Under this system, a network of bankers ensures that money deposited in one part of the world can be paid out in another part of the world. The money is settled between the bankers themselves, reducing to a minimum the need for physical transport of cash.[112] In the Netherlands, underground banking is mainly used by migrants. Sometimes these informal financial channels are the only way to transfer money to family members in the country of origin.[113] Normal banking transactions to conflict zones are often not possible via banks, partly because of what is known as 'de-risking'.[114] In the case of de-risking, no services are provided or the business relationship is terminated for certain types of clients or certain regions.

The services of unlicensed PSPs are also classified under this money laundering threat. A payment service provider (PSP) is a non-banking entity that provides payment services to end-users. These payment services include support for and processing of debit card transactions, facilitation of online payment transactions, issue and acceptance of payment cards such as credit cards and provision of international money transfer services. Payment service providers also include money transfer companies engaged in the business of carrying out money transfers or performing activities aimed at effecting such transfers.[115] Payment service providers fall under the Wwft, and pursuant to the Financial Supervision Act (Wft, *Wet op het financieel toezicht*), are required to have a licence for providing payment services. In the Netherlands, these licences are issued by DNB.

Box 8 Case involving money laundering via underground banking*

Investigative services carried out a joint action in 2019 at a business park in Beverwijk based on indications that a large number of telecom companies were engaged in underground banking. It was suspected that the telecom trade was mainly set up to facilitate and disguise the movement of large amounts of money.

112 https://magazines.openbaarministerie.nl/inzicht/2019/03/ondergronds-bankieren.

113 KLPD (2008).

114 www.fatf-gafi.org/documents/news/rba-and-de-risking.html. '...de-risking refers to the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk in line with the FATF's risk-based approach.'

115 www.cn.dnb.nl/nl/toezicht/toezicht_geldtransactiekantoren/markttoegang#geldtransactiekantoor.

Over the years, millions of euros have probably been moved in this way. The joint action of the investigative services uncovered administrative records such as records of underground banking, cash-counting machines, counterfeit branded products of major telephone brands, EUR 262,000 in cash and a shipment of stolen lamps. Previous investigations had shown that the business park was frequently visited by suspected money couriers and underground bankers. There were signs that 'dubious cash' was being brought into a company and that these amounts were then being pumped around between companies in the Netherlands and companies in Eastern European countries and Dubai. After an investigation of the companies, persons involved in four of the companies were identified as suspects in connection with money laundering and underground banking.

* www.om.nl/actueel/nieuws/2019/09/13/administratie-geld-valse-merktelefoons-in-beslag-bij-grootschalige-zoekingen-bedrijventerrein.

The different forms of underground banking offer a number of advantages to criminals. It allows international payments to be made without using official channels. It avoids the risks associated with the physical movement of cash (risk of seizure) or money transfers via a regular banking institution (risk of triggering an unusual transaction report).[116] Illegally gained money can also be mixed up with legal money and settlements may take place via complex transactions, thereby concealing the criminal origin of the money.[117]

Money laundering via physical movement of cash

Criminals who want to place cash in the financial system may first physically move or have it moved abroad (whether or not by intermediaries). After moving the cash, it needs to be introduced into the legitimate financial system of the relevant country. It is particularly advantageous for a criminal to move the money to countries where financial institutions or designated non-financial businesses and professions conduct customer due diligence and/or monitor transactions in a less thorough manner than in the Netherlands. The physical movement of cash is, in fact, a preliminary stage to placing the money in the financial system. This method may also be part of the money laundering method described above, i.e. money laundering via underground banking.

Cash can be moved in various ways, such as via professional or non-professional money couriers or by post. Another method, mentioned in a study by Soudijn[118], is through the so-called bank-to-bank cash transport system in which international cash flows take place between banks via special transport companies that carry the cash as cargo or in mailbags. According to Soudijn, there are no special customs requirements for this transport and it is merely sufficient to indicate how many kilos of paper money are involved. The names of the UBO and the banks involved do not need to be indicated, as a result of which customs authorities have virtually no information to determine whether or not it involves legitimate bank-to-bank transport. A third method of physically moving cash mentioned in the same study by Soudijn is via trade, for example, by hiding the cash between commercial goods. The second case in Box 9 is an example of this: a company that used shipments of frozen chicken to hide and smuggle money.

116 Kruisbergen et al. (2012).

117 KLPD (2008).

118 Soudijn (2017).

Box 9 Case involving money laundering via physical movement of cash

Case 1
At Schiphol, a passenger with packages of money attached to his body was arrested during a security check. Although the passenger presented a customs declaration stating that he was carrying a sum of EUR 250,000, the total amount was actually EUR 459,950. The passenger was unable to substantiate how he had obtained such a large sum of money and made contradictory statements about the origin of the funds. The suspect was sentenced to 16 months in prison and the money was confiscated.*

Case 2
At the beginning of 2018, the Overijssel court sentenced a man to a three-year prison term for laundering more than EUR 8.8 million. The man had packed large amounts of money in chicken roulades that were being shipped to Aruba by container. In June 2015, a sea container was seized in Aruba that had been shipped by the company in which the convicted person was the sole shareholder. Packages containing cash amounting to more than EUR 2.8 million were found in various boxes with chicken products that were being shipped in this container.**

* https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHAMS:2015:3979.

** www.recht.nl/rechtspraak/uitspraak/?ecli=ECLI:NL:RBOVE:2018:421.

Money laundering via crypto currencies
A relatively new method is the laundering of illegally obtained money via crypto currencies. Besides the bitcoin, there are around 6,000 other crypto currencies in circulation in 2020, including the monero and ethereum.[119] Crypto currencies are a regular means of payment on the darknet (the anonymous and hidden part of the internet) and this type of currency is widely used by criminals as a means of payment. The origin or destination of crypto currencies can be disguised via a crypto-currency mixing service. Via this online service, crypto currencies can be split up for a fee and recombined in a different composition. Such a mixing service can help increase the anonymity of the persons involved. In May 2019, the FIOD and the OM took one of the largest online mixers for crypto currencies offline based on the suspicion that the mixer was being used to conceal and launder criminal money flows.[120]

In 2018, FIU-the Netherlands received almost double the number of reports compared to 2017 regarding unusual transactions with the subject of 'virtual assets'.[121] FIU-the Netherlands provides information on typologies that could lead to transactions such as the buying and selling of crypto currencies being qualified as 'unusual'.[122] One of the indicators relates to the possible use of a mixer by the buyer and/or seller of these virtual means of payment.

119 According to Coinmarketcap, there were 5,093 different cryptocurrencies as of early February 2020 with a total market value of USD 266,558,777,427 (as on 5 February 2020, 4.00 p.m.) (https://coinmarketcap.com/charts/).

120 www.fiod.nl/fiod-en-om-halen-witwasmachine-voor-cryptovaluta-offline/.

121 FIU-the Netherlands (2019).

122 www.fiu-nederland.nl/nl/wetgeving/witwastypologieen/virtuele-betaalmiddelen.

Box 10 Case involving money laundering via crypto currencies

Case 1
At the end of 2019, the OM demanded a prison sentence for two people and a confiscation of hundreds of thousands of euros in illegal bitcoin exchanges. The persons are said to have been guilty of converting bitcoins into cash for two and half years. This concerned criminal money allegedly earned through drug trafficking and other criminal activities. A total of more than EUR 3.5 million was booked on the investigated bank accounts, all of which originated from bitcoin exchanges. One of the suspects appeared to have three regular customers, one of whom had been convicted of drug trafficking via the dark web and another had been arrested for drug dealing. According to the OM, the suspect must have been aware that his customers had earned the bitcoins through criminal activities. This suspicion is based on the fact that the bitcoin exchanger asked for a much higher commission from the suspect than that asked by regular exchangers. Moreover, if a legal bitcoin exchanger had been involved, the exchange could have taken place online and not, as it happened in this case, in a car park.*

Case 2
In 2018, the OM demanded a five-year prison sentence for a bitcoin trader who had exchanged about EUR 11.5 million in bitcoins over a period of two years. According to the OM, this money probably came from the illegal trade in drugs and other prohibited goods on the dark web. The suspect charged an unusually high commission for exchanging bitcoins. The OM believes that the high commission was the price customers had to pay in order to remain anonymous.**

* www.om.nl/actueel/nieuws/2019/10/08/om-eist-celstraffen-en-een-ton-ontneming-voor-illegale-bitcoin-wisselingen.

** www.om.nl/actueel/nieuws/2018/02/20/om-eist-5-jaar-tegen-witwassende-bitcoin-handelaar.

Money laundering via loan-back arrangements
In the case of money laundering via a loan-back arrangement, a criminal lends his or her own illegally obtained money to himself or herself, pretending that the money belongs to someone else. In this way, it looks like a legitimate loan agreement between two parties.[123] In his study, Soudijn gives the following concrete example of such a loan-back arrangement. Person A buys a house abroad for a large amount of money that Person A has borrowed from Person B. While it may appear to the civil-law notary or broker that Person A has taken out a regular mortgage, in reality he has transferred his criminally obtained funds to Person B (for example, a family member or friend) with the instruction to enter into a so-called private loan contract with Person A. Such loan-back arrangements become more complex in nature when large amounts are involved. In these cases, instead of using private persons as borrowers, financial institutions, companies, trust offices and foreign offshore companies are used.[124]

Box 11 Case involving money laundering via loan-back arrangements*

In 2018, the OM demanded that two men pay a total of more than EUR 8,500,000 to the State. It was alleged that they had earned this amount through participation in a criminal organisation that was involved in drug trafficking. Both suspects had been previously convicted for this in 2012 and 2017, respectively. A large number of national and international legal entities were registered in their name.

123 Soudijn (2017).

124 Soudijn (2017).

In addition, they made use of loan-back arrangements, where they bought real estate in the Netherlands with the help of a mortgage from an international legal entity within their own network. These arrangements disguised the fact that the money for these purchases was actually provided by them and this, according to the OM, had enabled them to continue laundering their criminal money for years.

* www.om.nl/actueel/nieuws/2018/04/18/om-eist-dat-twee-veroordeelde-mannen-ruim-8.500.000-betalen-aan-staat.

Money laundering via ABC transactions

In an ABC transaction, three or more parties sell real estate to each other within a short period of time where, with each sale, the price of the real estate increases. In this way, the parties try to create legal income via a false increase in value (or sometimes a reduction in value) that arises from the property being resold above (or below) the market price or via an incorrect value as a result of a false valuation.[125] In practice, ABC transactions are quite common in the real estate sector and usually do not involve any money laundering. ABC transactions may also have a legitimate purpose, for example, when a municipality sells land to a builder/property developer and the latter sells a building lot to a private individual. In some cases, the municipality may transfer its ownership directly to the private individual. But, as shown in the case described below, ABC transactions are susceptible to money laundering, partly because straw men may be used. The National Threat Assessment for Organised Crime (*Nationaal Dreigingsbeeld Georganiseerde Criminaliteit*) of 2017 also highlights this problem.[126]

Box 12 Case involving money laundering via ABC transactions*

In 2019, the OM demanded prison sentences and community service orders to be imposed on seven persons suspected of money laundering and fraud. According to the OM, the main suspect had made use of ABC structures. The main suspect instructed properties to be purchased by and in the name of straw men who often had financial problems and were looking for affordable housing through the main suspect. This is how the suspect tried to evade the attention of the Tax and Customs Administration and other authorities.

* www.om.nl/actueel/nieuws/2019/02/12/om-eist-in-hoger-beroep-tot-8-jaar-cel-voor-oplichting-en-hypotheekfraude-in-den-haag.

Money laundering via investment institutions/firms

Investment institutions are investment companies or funds that attract money from the public via the issue of participating interests (shares or right to hold participating interests) and then jointly invest these funds – i.e. for all the investors collectively – in financial and non-financial assets. This includes equity funds, bond funds, hedge funds and real estate funds. Investments firms are companies that are licensed by the AFM to provide investment services such as asset management.

Even though the first expert meeting did not refer to any concrete case of money laundering via investment institutions/firms and the nature and mechanisms of this money laundering method were not explained further, the experts agreed that this threat could have a major impact. In the interviews, it was emphasised that the risk associated with this money laundering threat is mainly associated with *unlicensed*

125 Soudijn (2017).

126 Boerman et al. (2017).

investment institutions/firms, and to a lesser extent, with licensed institutions and firms.

Money laundering via offshore companies
Criminals may launder illegally gained money in a concealed manner by making use of offshore companies outside the Netherlands. An offshore company is a company with share capital, governed by private law, incorporated under foreign law and with legal personality that is not allowed to develop or does not develop any economic activities within the field of jurisdiction in which the place of incorporation and/or registered office of the company is located, and of which the actual titleholder or holders resides or reside in a country other than where the company is established.[127] Van Koningsveld mentions some additional characteristics of offshore companies (which may not apply to every field of jurisdiction):

- The government in the country of incorporation does not levy direct tax (although the offshore company is obliged to pay a fixed annual amount to the government).
- The offshore company does not have its own physical office address, personnel, means of communication and such.
- The offshore company must have an agent in the country of establishment (registered agent) and office address (registered office).
- The offshore company is managed and administered by an employee of a local trust or law firm.
- In fact, these are often sole proprietorships with transactions taking place between affiliated companies within the same organisational structure.

Box 13 Cases involving money laundering via offshore companies*

In 2017, the FIOD and the British tax investigation service seized more than EUR 6 million as part of a joint investigation into suspected tax fraud and money laundering by a Dutch man and his British wife. It is suspected that the couple committed tax fraud through covert arrangements set up via their marketing company, where they allegedly used offshore bank accounts in the Netherlands, Germany and Austria to launder the criminal assets earned by them.

* www.fiod.nl/gezamenlijk-onderzoek-fiod-en-britse-hmrc-naar-verhuld-vermogen-in-buitenland/.

According to Van Koningsveld, the term 'offshore company' does not include public legal entities or any kind of foundation or trust. He also indicates that certain elements of an offshore company, such as a minimum level of filing obligations in public registers, can help increase the anonymity of the persons involved.[128]

Money laundering via structures by trust offices
A trust office is a legal entity, company or natural person engaged in providing trust services on a commercial/professional basis, either alone or in conjunction with other people, legal entities or companies.[129] As discussed earlier in Chapter 3, the services of a trust office may include serving as a director of a legal entity or company, providing a postal address, providing administrative services and offering to act as a conduit company.[130] Trust office services are characterised by a high risk

127 Van Koningsveld (2015).

128 Van Koningsveld (2015).

129 Article 1, Wtt 2018; See the References section for the formal titles and sources of the laws and regulations.

130 DNB (2019).

of money laundering. This risk arises from the nature of the services: this often involves services associated with tax-driven structures of legal entities which, partly due to their complexity, are susceptible to misuse. The structures of the legal entities, to which a trust office provides its services, may be used to conceal assets or the identity of the UBOs. In addition, these structures often go through various offshore jurisdictions in well-known tax havens including Anguilla, The Bahamas, Bermuda, Saint Kitts and Nevis, Seychelles, Cayman Islands and Panama.[131]

Chapter 3 indicated that there is a downward trend noticeable in the number of licensed trust offices in recent years. At the end of 2011, there were 310 trust offices in the Netherlands, which dropped to 170 by February 2020.[132] According to Holland Quaestor, the sector organisation for licensed trust offices in the Netherlands, there has also been a significant decrease in the total number of object companies served by the trust offices: in the period from June 2016 to December 2017, this decreased by 10%. Since 2013, there has also been a significant decrease in the services provided by trust offices to limited partnerships (CV, *commanditaire vennootschap*) that are part of complex international structures and that offer foreign UBOs the option of anonymity. In mid-2013, 75 trust offices provided services to 1,602 CVs; at the end of 2017, 62 trust offices provided services to 521 CVs.[133]

In the interviews, it was emphasised that the risk associated with this money laundering threat is mainly associated with *unlicensed* trust offices, and to a lesser extent, with licensed trust offices.

Box 14 Case involving money laundering via structures by trust offices

Case 1
An administrative fine of EUR 40,000 has been imposed on a trust office because it reported a share/depositary receipt transfer to FIU-the Netherlands four months after the transaction had taken place. The trust office should have reported this earlier, since it involved a transfer by a customer to another party, without any form of consideration, of EUR 8 million worth of real estate registered under a legal entity incorporated under the law of Seychelles.*

Case 2
In 2019, a trust office was accused by the OM of not reporting unusual transactions of a customer to FIU-the Netherlands on time. These transactions had been carried out by a subsidiary of a group of companies in Ukraine, active in the energy and raw materials sector. In 2013, the company acquired four other companies for a sum of more than EUR 200 million, which gave the acquiring company control over a major player in the Ukrainian energy and raw materials sector. The OM also accused the trust office of not having investigated these transactions in sufficient depth. For this, the trust office has accepted and settled a transaction offered to it by the OM in the form of a payment of EUR 350,000.**

* https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:CBB:2018:6.

** www.om.nl/actueel/nieuws/2019/09/03/trustkantoor-vistra-betaalt-35-ton-voor-niet-melden-ongebruikelijke-transacties.

131 For more about this, see Van Koningsveld (2016).

132 DNB, Trust Offices Register, see: www.dnb.nl/toezichtprofessioneel/openbaar-register/WTTTK/index.jsp?filter_value=&naam=Statutaire+naam+%2F+Handelsnaam.

133 https://hollandquaestor.nl/cijfers-en-trends-in-de-trustsector/.

Money laundering via legal entities

In addition to offshore companies and structures by trust offices, criminals may attempt to launder money by using various kinds of legal entities. Criminals may use intermediaries who set up legal entities for them, through which the identity of the legal entity's UBO – in this case, the criminal – can be disguised. The more legal entities a criminal uses, whether or not through intermediaries, the greater the complexity of the money laundering method. Criminals may also make payments or instruct payments to be made between the various legal entities, which again offers opportunities to use other types of money laundering methods. For example, money laundering may take place via over-invoicing/under-invoicing between different BVs that are, in fact, owned by the same criminal party.

Box 15 Case involving money laundering via legal entities*

The FIOD arrested three suspects as part of a criminal investigation into money laundering involving the purchase of a house of more than EUR 700,000 by a foundation. It is suspected that such an arrangement was chosen in order to cover up criminal money. One of the suspects is the director of the foundation that bought the house. He is the brother of another suspect who is believed to be the ultimate owner of the home. The house itself, as well as digital and paper documents and cash worth EUR 82,000, were seized.

* https://www.fiod.nl/3-aanhoudingen-witwasonderzoek-nieuwkuijk/.

Table 11 provides a schematic overview of some of the characteristics of a number of legal entities in the Netherlands.[134]

Table 11 Schematic overview of certain legal entities

Legal entity	Characteristics
Sole proprietorship (*Eenmanszaak*)	Establishment: form-free Capital requirement: none Management: owner
Private limited company (BV, *Besloten vennootschap*)	Incorporation: notarial deed Capital requirement: EUR 0.01 Management: management board
Public limited company (NV, *Naamloze vennootschap*)	Incorporation: notarial deed Capital requirement: €45,000 Management: management board
Partnership (*Maatschap*)	Incorporation: no prescribed form, preferably written/notarial contract Capital requirement: none Management: partners
Commercial partnership (VOF, *Vennootschap onder firma*)	Incorporation: no prescribed form, preferably written/notarial contract Capital requirement: none Management: partners
Limited partnership (CV, *Commanditaire vennootschap*)	Incorporation: no prescribed form, preferably written/notarial contract Capital requirement: none Management: managing partners
Foundation (*Stixhting*)	Incorporation: notarial deed Capital requirement: none Management: management board

Source: Chamber of Commerce (2020)

134 Chamber of Commerce (2020). See: www.kvk.nl/download/SchemaRechtsvormen_tcm109-389297.pdf.

The Chamber of Commerce distinguishes legal entities with legal personality such as BVs and foundations and legal entities without legal personality such as sole proprietorships and CVs.[135] Some legal entities are relatively easy to set up, especially when there is virtually no capital requirement as in the case of sole proprietorships, foundations, BVs and CVs. A notarial deed is also not required for certain legal entities; this is only required for the incorporation of BVs, NVs and foundations.

Box 16 Insight into unusual situations relating to legal entities

The use of structures involving legal entities is mentioned as one of the methods used in money laundering. Justis has provided certain tables containing data from the Commercial Register in order to offer quantitative insight into such types of structures, including the non-transparent structures of legal entities and changes in the management of legal entities. These tables reveal a number of unusual situations. It is possible that these relate to forms of money laundering that make use of structures involving legal entities. However, a direct link with money laundering cannot be established.

Data for the reference year 2017 are given below. Data for the reference year 2015 were also requested. The results are comparable for both years.

- In 2017, a total of 83,512 legal entities were incorporated in the Netherlands. Most of the incorporated legal entities are BVs, foundations and associations.
- In 2017, 87,100 natural persons were involved as directors in the incorporation a new legal entity. This concerned 77,294 unique natural persons, 193 of which were involved in the role of director in more than 50 legal entities in the period 2017-2019. Of these 193 natural persons, 13 were resident outside the Netherlands.
- In 2017, 39,169 legal entities were involved as directors in the incorporation of a new legal entity. This concerned 31,312 unique legal entities, 185 of which were involved in the role of director in more than 50 legal entities in the period 2017-2019. Of these 185 legal entities, 17 were registered as being established in the Netherlands, and for 168 of them, the country of establishment was unknown.
- Of the 87,100 non-unique natural persons who were involved as directors in the incorporation of a legal entity in 2017, 1,023 persons held this position for less than 30 days. Of these, 135 persons were resident outside the Netherlands.
- Of the 39,169 non-unique legal entities who were involved as directors in the incorporation of a legal entity in 2017, 596 held this position for less than 30 days. Of these, 21 were registered as being established in the Netherlands, and for 574 of them, the country of establishment was unknown.

Money laundering via trade-based structures involving goods and/or services

Trade-based structures involving goods and/or services are methods by which criminals can launder illegally obtained money via international or national trade. This money laundering method is also known as Trade-Based Money Laundering.

135 Sole proprietorships, VOFs, CVs and partnerships are legal entities without legal personality. Hence , these legal entities are not included in Book 2 of the Dutch Civil Code. However, Book 2 does include the legal entities with legal personality, i.e. BVs, NVs, associations, cooperatives and mutual insurance associations and foundations. Sources: Book 2, Dutch Civil Code and Chamber of Commerce. https://ondernemersplein.kvk.nl/overzicht-rechtsvorm/.

The FATF describes this method as a process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise the illicit origin of these proceeds. This can be done by misrepresenting the price and quantity or quality of imports or exports. According to the FATF, one of the basic techniques for this money laundering method is the over-invoicing and under-invoicing of goods or services.[136] In concrete terms, this method implies that two companies that work together (or are owned by the same person) send each other excessive invoices for the delivery of goods or services. For example, Company A invoices EUR 10,000 for the delivery of a particular product when, in fact, this product costs no more than EUR 50. Company B pays the invoice, thus using a large amount of criminal money for a legitimate purpose. Variants of this method, as also mentioned by the FATF, include the issue of multiple invoices for the same goods or services, overshipments or short shipments of goods or services and false descriptions of goods or services.

Money laundering via trade-based structures involving services is said to occur when these structures relate to services rather than products, for example, advisory services that have not been provided or not been provided in full, for which the activities as entered in the records have not been performed or for which these activities have been performed by persons other than those entered in the records, and so on. The same money laundering methods can be used for money laundering via trade-based structures involving services or goods.

Box 17 Case involving money laundering via trade-based structures involving goods*

A criminal investigation has revealed a case involving the export of potatoes and onions to West Africa for which the payments were not settled via the bank but with cash. In the period from 2014 to early 2019, Dutch potato and onion traders probably accepted almost EUR 150 million in cash from underground bankers and money couriers. This money probably had a criminal origin. The investigated traders indicated that they had accepted amounts in cash due to the alleged absence of a properly functioning banking system with, for example, Mauritania. This money laundering method works as follows: a customer in, for example, Mauritania hands over money to an African broker who then contacts a fellow broker in the Netherlands. The broker in the Netherlands hands over the cash – presumably criminal in origin – to the Dutch agricultural companies. Banks accepted the cash deposits from the agricultural sector based on the declaration that potatoes or onions had been delivered in return for this money.

* www.om.nl/actueel/nieuws/2019/07/17/aardappel--en-uienhandel-vatbaar-voor-witwaspraktijken.

136 FATF (2006).

5 Resilience of the policy instruments

This chapter starts by describing the way in which the prevention and combat of money laundering is organised in the Netherlands. Subsequently, the available policy instruments for preventing and combating money laundering are discussed. The present NRA focuses on the policy instruments that were available until the end of 2019. The chapter concludes with a section discussing certain possibilities for strengthening the resilience of the policy instruments.

5.1 Organisation of anti-money laundering actions

In the Netherlands, many parties are involved in preventing and combating money laundering. The Ministry of Finance and the Ministry of Justice and Security are responsible for the prevention and suppression of money laundering and for managing this effort.

When it comes to preventing money laundering in the Netherlands, the Wwft (see Section 5.4 for more information) is of key importance. There are six supervisory authorities under the Wwft:[137]

- The AFM monitors investment firms, investment institutions and financial service providers insofar as they act as brokers in life insurance contracts.
- The BFT monitors civil-law notaries, junior civil-law notaries and assigned civil-law notaries, tax consultants, chartered accountants, accounting consultants as well as persons/institutions performing similar activities in a professional or commercial capacity such as administration offices, tax consultants and business consultants.
- The BTWwft monitors buyers and sellers of goods or intermediaries in the purchase and sale of goods, real estate agents and brokers, real estate appraisers, pawnshop operators and domicile-providers.
- The dean of the Bar Association in the various districts monitors lawyers who provide services under the Wwft, including advice on buying and selling companies, setting up and managing companies and legal entities and managing funds.
- DNB monitors financial institutions, including banks, insurers, payment institutions, electronic money institutions, exchange institutions and trust offices.
- Ksa monitors gambling casinos.

Pursuant to the Wwft, the aforementioned financial institutions and professionals have a duty to report unusual transactions to FIU-the Netherlands and are obliged to screen their customers (see Section 5.4 for more information). FIU-the Netherlands analyses the unusual transactions and may declare them to be suspicious, in which case they are forwarded to the various special investigative, intelligence and security services. According to FIU-the Netherlands, these suspicious transactions may serve various purposes: as cause to initiate an investigation, as a demonstrable reason for additional proof to be provided in the courtroom, as a guiding instrument in an investigation, as a source of analysis for conducting strategic investigations, and finally, for providing information about and an overview of regional and national crime.[138]

137 Slot & De Swart (2018).

138 FIU-the Netherlands (2019).

The financial and economic crime section of the regional police units, the FIOD and the National Investigation Service (*Dienst Landelijke Recherche*) play a key role in the criminal investigation of money laundering. Persons suspected of money laundering may be charged by the OM and subsequently brought to trial. The OM and the Central Fine Collection Agency (CJIB, *Centraal Justitieel Incassobureau*) play a role in the confiscation of criminal assets. The number of money laundering cases brought to court fluctuated annually between approximately 1100 and 1500 in the period 2010-2019.[139]

The KMar and Customs Service also fulfil an important task in preventing and combating money laundering. The KMar works closely with the FIOD at Schiphol; in case of suspicions related to money laundering, the KMar hands the matter over to FIOD. Customs Service provides information to FIU-the Netherlands about the cross-border transport of large quantities of liquid assets such as cash with a value of EUR 10,000 or more or unusual shipments of liquid assets such as gold and cheques.

Moreover, the sector/umbrella organisations of the aforementioned financial institutions and non-financial businesses and professions with a reporting obligation under the Wwft also play a role in the fight against money laundering. Examples include the Dutch Banking Association (NVB, *Nederlandse Vereniging van Banken*), Holland Quaestor (trust offices), Royal Dutch Association of Civil-Law Notaries (KNB, *Koninklijke Notariële Beroepsorganisatie)*, Netherlands Institute of Chartered Accountants (NBA, *Nederlandse Beroepsorganisatie van Accountant*s), Dutch Money Transfer Association (NVGTK, *Nederlandse Vereniging van Geldtransactiekantoren*) and Dutch Association of Real Estate Brokers and Valuers (NVM, *Nederlandse Vereniging van Makelaars en Taxateurs*). These organisations also inform their members about, for example, how they can comply with the Wwft and/or the cases involving money laundering methods encountered by their members.

Various partnerships have been set up between some of the above-mentioned parties for preventing and combating money laundering. During the third expert meeting, the experts identified these partnerships as part of the policy instruments for preventing and combating money laundering. Section 5.5 provides a brief explanation of the most important partnerships.

5.2 Available policy instruments

The available policy instruments for preventing and combating money laundering include all the relevant instruments based on municipal, national and international laws and regulations as well as regulations defined at sectoral and organisational levels. However, the term 'policy instrument' can be interpreted more broadly than just laws and regulations. Prior to the third expert meeting, a longlist of policy instruments (see Appendix 5) was sent to experts via an email survey and they were asked to add to this longlist any other policy instruments that they considered relevant. According to the experts, the guidelines, instructions and policy plans of organisations that play a role in preventing and/or combating money laundering can also be seen as policy instruments. Moreover, as indicated in the previous section, partnerships between organisations that play a role in increasing the integrity of the

139 Slot & De Swart (2018) and https://www.accountant.nl/nieuws/2020/2/explosie-aantal-witwaszaken-is-betrekkelijk/.

financial system and combating money laundering are also a kind of policy instrument, according to experts.

At the beginning of the third expert meeting, the findings of the email survey were discussed jointly. This discussion resulted in the following overview of policy instruments for preventing and combating money laundering (see Table 12). Each policy instrument is briefly explained in the following sections.

Table 12 Policy instruments for preventing and combating money laundering

International laws and regulations	National laws and regulations	Other policy instruments
FATF-recommendations EU Anti-Money Laundering Directive EU Regulation on Controls of Cash Wire Transfer Regulation 2	Money Laundering and Terrorist Financing Prevention Act Financial Supervision Act Penal Code Code of Criminal Procedure Trust and Company Service Providers (Supervision) Act 2018 Public Administration Probity Screening Act Legal Entities Supervision Act Commercial Register Act 2007 Tax legislation Economic Offences Act Right to report Tax and Customs Administration 2003	National partnerships International partnerships Sectoral and sector-oriented regulations and terms and conditions Guidelines and policy plans

An important side note regarding the above table is that the third expert meeting took place at the end of 2019. Experts based their assessment of the resilience of the policy instruments on the specific instruments that existed *at that time*. This means that they have not taken into account any laws and regulations and other policy instruments that have been or are intended to be introduced from the beginning of 2020. Hence, this NRA also focuses on the policy instruments that were available until the end of 2019. In the following sections (in particular, Section 5.6), some policy instruments that have been or will be introduced from 2020 are discussed in more detail.

5.3 International laws and regulations

FATF recommendations[140]

The Dutch policy for preventing and combating money laundering is based on the recommendations of the FATF. Members of the FATF, including the Netherlands, are bound by recommendations stipulating that the appropriate preventive and suppressive measures and measures to improve national legal systems and international cooperation must be taken. In addition, the FATF monitors the correct functioning and effective implementation of these regulations. In this context, the FATF periodically conducts a country evaluation to assess the country's level of compliance with

140 FATF (2012).

the recommendations. The next country evaluation for the Netherlands is expected to take place in 2021-2022.

EU Anti-Money Laundering Directive[141]
For EU Member States, the majority of the FATF's recommendations have been adopted as part of the amendment to the Fourth European Anti-Money Laundering Directive. This Directive establishes rules at the European level to prevent the use of the financial system for money laundering and terrorist financing. In the Netherlands, these rules for preventing the use of the financial system for money laundering and terrorist financing have been included in the Wwft (see Section 5.4). The Fourth Anti-Money Laundering Directive entered into effect in the Netherlands on 25 July 2018. The amendment of the Fourth Anti-Money Laundering Directive, also known as the Fifth European Anti-Money Laundering Directive, was adopted in the EU in mid-2018 and is currently being implemented in the Netherlands. The Implementation Bill was adopted in the Senate in April 2020 and entered into effect on 21 May 2020.

EU Regulation on Controls of Cash[142]
Since June 2007, rules governing the movement of cash in and out of EU territory have been laid down and are an integral part of the EU framework to prevent and combat money laundering and terrorist financing. The legislation requires all citizens who enter or leave the EU carrying cash of EUR 10,000 or more to declare this cash to the customs authorities. A revised new regulation with updated rules was adopted at the end of 2018 and will enter into force in June 2021.[143] In the new regulation, the definition of cash has been expanded to include not only banknotes but also other liquid assets such as cheques, travellers cheques, prepaid cards and gold. From June 2021 onwards, the regulation will also apply to cash transported in postal, freight or courier shipments.

Wire Transfer Regulation 2 (WTR 2)[144]
In effect since June 2017, the new WTR2 obliges all payment service providers and intermediary payment service providers to record information not just on the payer but also the beneficiary. Payment service providers must ensure that the transfer of funds always includes the payee's name and payment account number. In addition, the obligations under the previous WTR1 have been made stricter for payment products that can be used anonymously or that are not linked to persons.

141 See the list of References for the formal titles and sources of the laws and regulations.

142 See the list of References for the formal titles and sources of the laws and regulations.

143 www.consilium.europa.eu/nl/press/press-releases/2018/10/02/controls-on-cash-entering-and-leaving-the-eu-council-adopts-regulation/#.

144 See the list of References for the formal titles and sources of the laws and regulations.

5.4 National laws and regulations[145]

Money Laundering and Terrorist Financing Prevention Act (Wwft)[146]
The Wwft aims to prevent the use of the financial system for money laundering and terrorist financing by imposing a number of obligations on financial institutions and a large number of professional groups (Section 5.1 provides a brief overview of the type of institutions and professional groups). First of all, these parties are obliged to perform customer due diligence. These checks include identifying the customer and verifying the customer's identity, as well as identifying the customer's Ultimate Beneficial Owner (UBO) and taking reasonable measures to verify the UBO's identity. Secondly, these institutions are obliged to report unusual transactions to FIU-the Netherlands. Unusual transactions are reported based on objective and subjective indicators. An example of an objective indicator is 'money exchange transactions with a value of EUR 10,000 or more' and that of a subjective indicator is 'transactions where there is reason for an institution to assume that they may be related to money laundering or terrorist financing'. The Wwft prescribes a risk-based approach: in many cases, institutions must themselves assess the risk of a customer being involved in money laundering and adjust the strictness of their own measures accordingly. These measures may vary from a basic customer due diligence to a decision to not embark upon or even terminate a business relationship.

Financial Supervision Act (Wft)[147]
Since 1 January 2007, the supervision of the financial sector in the Netherlands is regulated by the Wft. Financial supervision guarantees the stability of financial systems, ensures that financial markets operate efficiently and protects consumers against the insolvency or unacceptable behaviour of financial institutions. DNB and the AFM perform the supervisory tasks under the Wft. DNB's task is to exercise 'prudential supervision'[148] with respect to financial companies and take decisions on the admission of these financial companies to the financial markets. The AFM's task is to exercise 'conduct supervision'[149] with respect to financial markets and take decisions on the admission of financial companies to these markets. The Wft stipulates that institutions must ensure that their business operations are ethical and controlled. In addition, the Wft provides for an assessment of the suitability and reliability of policymakers.

---

145 In addition to the national laws and regulations listed below, the experts referred to the Betting and Gaming Act (*Wet op de Kansspelen*) and the Remote Betting and Gaming Act (*Wet Kansspelen Op Afstand*), which is pending implementation. Since money laundering via gambling is not one of the money laundering methods identified as having the greatest potential impact, the Betting and Gaming Act has not been described here. The Dutch Civil Code, which was mentioned in the email survey, is also not going to be dealt with here because, as it appeared during the third expert meeting, the Dutch Civil Code can only be linked to a limited extent to the money laundering methods with the greatest potential impact that are the main focus of this NRA. However, the Dutch Civil Code is briefly discussed in Section 5.7 when discussing options for increasing the resilience of foundations against money laundering.

146 See the list of References for the formal titles and sources of the laws and regulations.

147 See the list of References for the formal titles and sources of the laws and regulations.

148 Prudential supervision focuses on the soundness of financial companies and contributing to the stability of the financial sector.

149 Conduct supervision focuses on orderly and transparent financial market processes, integrity in relationships between market parties and a scrupulous treatment of customers.

Penal Code (WvSr) and Code of Criminal Procedure (WvSv)[150]
The WvSr determines what is considered an offence and the penalties that may be imposed for this. The WvSv determines how criminal offences are to be prosecuted. Since 6 December 2001, money laundering is considered an independent criminal offence for which conviction for a basic offence, such as drug trafficking, is not necessary. The following forms of money laundering are included in the WvSr:

- There is a question of intentional money laundering if a person 'knows at the time of committing the act that the object he is hiding or concealing has originated from a crime' (Article 420a).
- Self-laundering only involves the acquisition or possession of objects that originate from crimes committed by the perpetrator (Article 420a.1).
- In habitual money laundering, a person is repeatedly guilty of intentional money laundering or money laundering in the exercise of his profession or business (Article 420b).
- In the case of culpable money laundering, it must be proven that a person had reasonable grounds to suspect that the object originated from criminal activities (Article 420c).
- Finally, there is also culpable money laundering that consists solely of acquiring or having in possession objects directly resulting from crimes committed by the perpetrator (Article 420c.1).

Trust and Company Service Providers (Supervision) Act 2018 (Wtt 2018)[151]
The Wtt 2018 entered into effect on 1 January 2019 and replaces the previous Trust Offices Supervision Act. The Wtt 2018 is primarily aimed at improving the integrity of the Dutch financial system. The Act lays down requirements for the management and organisation of trust offices and the customer due diligence conducted by trust offices. In addition, the Act provides a way to verify the suitability and reliability of policymakers at trust offices. Trust offices that meet the aforementioned requirements are eligible to receive a licence from DNB. It is prohibited to perform trust services in or for the Netherlands without possessing an appropriate licence for this.

Public Administration Probity Screening Act (Wet Bibob)[152]
The Wet Bibob is an instrument under administrative law that applies to certain permits, subsidies, invitations to tender and real estate transactions. Administrative authorities may refuse or withdraw a permit if there is a serious risk of the permit being used to commit crimes or to make use of money obtained from crime. The Wet Bibob is aimed at preventing the government from facilitating criminal activities and protecting the competitive position of bona fide entrepreneurs.

Legal Entities (Supervision) Act[153]
The purpose of the Legal Entities (Supervision) Act is to prevent and counter abuse by legal entities. This Act implements a system of continuous control over legal entities in the Netherlands. This includes an integrity assessment of the legal entity, directors and other persons and companies associated with the legal entity, which may result in the issuance of a risk report. In addition, supervisory, law enforcement and/or investigative bodies for legal entities may request that a network overview be performed. Such a network overview identifies the relevant relationships between the legal entity being investigated and other natural and legal entities

150 See the list of References for the formal titles and sources of the laws and regulations.

151 See the list of References for the formal titles and sources of the laws and regulations.

152 See the list of References for the formal titles and sources of the laws and regulations.

153 See the list of References for the formal titles and sources of the laws and regulations.

and/or companies. It also identifies any relevant bankruptcies and dissolutions. The task of supervision is carried out by the TRACK department of Justis, the screening authority of the Ministry of Justice and Security. This Act helps set up a systematic approach to financial and economic crime. By continuously monitoring legal entities for possible abuse, the supervisory, investigative and/or other law enforcement authorities have the opportunity to take more adequate actions.[154]

Commercial Register Act 2007[155]
The Commercial Register Act 2007, which entered into effect on 1 January 2008, contains provisions for mandatory registration in the Commercial Register of the Chamber of Commerce. This obligation applies to companies as well as to all other Dutch legal entities under private and public law, as well as their branches. The UBO Register is intended to become part of the Commercial Register, which means that it will also be managed by the Chamber of Commerce. The initially planned introduction of the UBO Register on 10 January 2020 has been postponed because the bill has not yet been adopted by the Senate. It is now planned to be introduced later in 2020 (see Section 5.6 for more information about the UBO Register).

Tax legislation
Tax legislation can help in preventing and suppressing money laundering. Tax fraud, a basic money laundering offence, can be countered through tax legislation. The Tax and Customs Administration also checks for unexplained assets based on the tax legislation.

Economic Offences Act (WED)[156]
The Economic Offences Act (WED, *Wet op de economische delicten*) is a framework act that defines all types of economic offences. Certain infringements of the Wwft, Wft, Wtt 2018 and Commercial Register Act 2007 are also classified as economic offences.

Tax and Customs Administration's right to report unusual transaction (2003)[157]
Since 2003, government institutions such as the Tax and Customs Administration and Customs Service are authorised to report unusual transactions to FIU-the Netherlands (at the time still referred to as the Office for the Reporting of Unusual Transactions (*Meldpunt Ongebruikelijke Transacties*)).

5.5 Other policy instruments

National partnerships
Various partnerships have been established to prevent and combat money laundering. During the third expert meeting, the experts identified these partnerships as part of the policy instruments for preventing and combating money laundering. The Money Laundering Action Plan (*Plan van aanpak witwassen*) of June 2019 also devotes extensive attention to these partnerships.[158] By intensifying the cooperation and exchange of information between public parties and between private and public

154 Justis (2017).
155 See the list of References for the formal titles and sources of the laws and regulations.
156 See the list of References for the formal titles and sources of the laws and regulations.
157 Tax and Customs Administration (2004).
158 Ministers of Finance and of Justice and Security (2019).

parties, the aim is to increase the effectiveness of both the gatekeeper function performed by the institutions falling under the supervision of the Wwft as well as that of the actual supervision itself. The Money Laundering Action Plan refers to a large number of initiatives. Below is a brief explanation of the most important partnerships:

- *Financial Expertise Centre (FEC)*: The FEC is a partnership of the AFM, DNB, OM, Netherlands Police, FIU-the Netherlands, FIOD and Tax and Customs Administration. The common goal of the FEC is to strengthen the integrity of the financial sector by exchanging information and sharing insights, knowledge and skills. Partnerships have also been formed between the FEC and banks, including the FEC-PPP and the Pilot Serious Crime Taskforce.
- *Anti-Money Laundering Centre (AMLC):* the AMLC, founded by the FIOD, is a platform that allows parties involved in the fight against money laundering to share knowledge and experiences and collaborate operationally. This takes place at three levels, i.e. through the implementation of concrete projects, the sharing and acquisition of knowledge and expertise and the collection and analysis of data.
- *Information Exchange on Criminal and Unexplained Wealth (iCOV)*: iCOV is a partnership between the Tax and Customs Administration, Customs Service, Netherlands Police, OM, FIOD, Netherlands Police Internal Investigations Department, FIU-the Netherlands, special investigative bodies of the Human Environment and Transport Inspectorate (*Inspectie Leefomgeving en Transport*), the Dutch Food and Consumer Product Safety Authority (*Nederlandse Voedsel- en Warenautoriteit*) and the Inspectorate SZW (*Inspectie SZW*). In addition, the CJIB, DNB, AFM and Dutch Media Authority (*Commissariaat voor de Media*) are also part of this cooperation. iCOV provides data intelligence products to member organisations. In addition, iCOV develops risk indicators and identifies patterns with the aim of exposing money laundering and fraudulent structures.
- *Regional Information and Expertise Centres (RIEC):* 10 RIECs have been set up in the Netherlands with the objective of combating organised, subversive crime. These organisations connect the information, expertise and strengths of various government bodies such as municipal and provincial authorities as well as the OM, Netherlands Police, Tax and Customs Administration, Tax and Customs Administration/Benefits, Customs Service, FIOD, Social Affairs and Employment Inspectorate (*Inspectie Sociale Zaken en Werkgelegenheid*), KMar and Immigration and Naturalization Service (IND, *Immigratie- en Naturalisatiedienst*). The National Information and Expertise Centre (LIEC, *Landelijk Informatie en Expertise Centrum*) plays a supporting and facilitating role.
- *Integrated Asset Recovery Teams:* in the context of the Integrated Asset Recovery Teams (*Integrale Afpakteams*), the police may seek out cooperation with parties such as the OM, FIOD, Tax and Customs Authorities and municipalities. By bundling their joint knowledge, the Integrated Asset Recovery Teams try to recover money and assets of criminal origin via criminal, tax and administrative means.
- The *Committee for the Reporting of Unusual Transactions* (*Commissie Meldplicht van ongebruikelijke transacties*) meets twice a year. Sector/umbrella organisations of institutions with a reporting obligation, Wwft supervisory authorities, the OM and FIU-the Netherlands carry out discussions with representatives of the Ministry of Finance and the Ministry of Justice and Security on national policy developments for the prevention and suppression of money laundering and terrorist financing, the design and implementation of the reporting obligation and determination of the indicators used for assessing whether a transaction should be regarded as an unusual transaction.

International partnerships
The existing international partnerships are also discussed in the Money Laundering Action Plan.[159] FIU-the Netherlands, investigative services and the OM have frequent contact with foreign partners involved in dealing with money laundering or related fields such as the fight against subversive crime. Information sharing with foreign partners takes place via, for example, the channels of the Egmont Group and FIU.net, Interpol, Europol, Eurojust and the Camden Asset Recovery Inter-agency Network (CARIN). Joint initiatives with foreign partners are carried out within the European Multidisciplinary Platform Against Criminal Threats (EMPACT), the Anti-Money Laundering Operational Network (AMON) and the Joint Chiefs of Global Tax Enforcement (J5) platform, and its international system for data matching, the Financial Criminal Investigation Network (FCInet).

In addition, there is international cooperation in the field of European and other international legal assistance systems. Multilateral and bilateral contacts are also maintained with various countries. Liaison officers from the police and KMar as well as liaison magistrates of the OM have been placed in various countries with the task of promoting cooperation in Dutch criminal investigations, for example, by providing guidance for the implementation of Dutch legal assistance requests. Finally, supervisory authorities such as DNB and the AFM actively participate in international partnerships such as the European Supervisory Authority Anti-Money Laundering Committee (as of 1 January 2020, this is called the AMLSC), the International Association of Insurance Supervisors and the Basel Committee on Banking Supervision.

Sectoral regulations and conditions
Sectors may also have regulations and conditions that play a role in preventing and combating money laundering via their sector. For example, the general banking terms and conditions of Dutch banks define the rules of conduct between banks and their customers. All banks that are affiliated with the NVB use the same general banking terms and conditions. If necessary, banks may refuse customers on this basis. The financial sector in the Netherlands has yet another instrument that may play a role in the prevention and/or suppression of money laundering, i.e. the External Referral Application (EVA, *Externe Verwijzingsapplicatie*) which is the joint fraud prevention system of the NVB and the Dutch Finance Houses' Association (VFN, *Vereniging van financieringsondernemingen in Nederland*). The EVA Register links the fraud registers of the affiliated organisations and the information contained in it may be shared between banks that are members of the NVB.

Guidelines, instructions and policy plans
Another type of policy instrument mentioned in the email survey and the third expert meeting are the guidelines and instructions drawn up by the FATF, Wwft supervisory authorities and sector or professional organisations. Indicators and typologies relating to money laundering methods developed by the FATF, the Wolfsberg Group[160] and FIU-the Netherlands are also considered to be policy instruments by experts. Finally, experts also see government policy plans as an instrument for combating money laundering, for example, the aforementioned Money Laundering Action Plan of June 2019 as well as the Security Agenda 2019-2022 that sets out the national policy objectives regarding the performance of police duties.

159 Ministers of Finance and of Justice and Security (2019).

160 The Wolfsberg Group is a non-governmental organisation of 13 globally operating banks that develops standards for the financial sector regarding the policy for combating money laundering and terrorist financing.

In addition, initiatives such as the FEC Academy and similar seminars have been developed to ensure that knowledge about money laundering and how to counter it remains up-to-date. Finally, there are also publications, such as those issued by FIU-Netherlands, the FEC and the AMLC, that are aimed at improving the level of awareness and provision of information.

5.6 Possibilities for improving resilience

The so-called AIU principle (AIO, *Anoniem, Internationaal en Ongereguleerd*) applies to many of the greatest money laundering threats. This AIU principle had been identified earlier in the first Dutch NRA.
It refers to money laundering methods that contain one or more of the following three components:

- Anonymous: the money laundering method conceals the identity of the criminal involved in money laundering.
- International: the money laundering method has an international character and is deployed via or from abroad.
- Unregulated: the money laundering method relates to or is applied in an unregulated sector.

For money laundering methods where the AIU principle plays a large role, the resilience of the policy instruments is relatively low (also see Chapter 6). In order to strengthen the resilience of these policy instruments, efforts should be made to reduce the possibilities for the AIU components to occur. The Money Laundering Action Plan of June 2019 contains various types of measures through which the government aims to further improve the prevention and suppression of money laundering from 2020 onwards. Many of these measures are expected to help, to a greater or lesser extent, in avoiding the AIU components of the greatest money laundering threats identified in this NRA.

Anonymous
The UBO Register will be implemented in 2020 to reduce the degree of anonymity with which money laundering methods can be applied. The UBOs of companies and other legal entities will be recorded in this Register. The UBO Register will be included as part of the Commercial Register of the Chamber of Commerce. The obligation to register the UBO applies to a large number of the legal entities in the Commercial Register. This includes BVs, public limited companies (NV, *naamloze vennootschap)*, foundations, associations, cooperatives, CVs, *commanditaire vennootschap*) and commercial partnerships (VOF, *vennootschap onder firma*). However, the obligation does not apply to owners' associations. A UBO register for trusts and similar legal constructs will also be introduced. The intention is to ensure that the UBOs of the legal construct are registered for all trusts and similar legal constructs (1) of which the director resides or is established in the Netherlands or (2) of which the director resides or is established outside the EU and where this director enters into a business relationship or acquires real estate in the Netherlands on behalf of the trust or similar legal construct.[161] The draft of this Implementation Act was presented for consultation on 17 April 2020.

161 Ministers of Finance and of Justice and Security (2019).

International[162]
Many of the identified money laundering methods are characterised by a strong international component. Examples of this are money laundering via trade-based structures involving services, money laundering via trade-based structures involving goods and money laundering via offshore companies. To effectively prevent and suppress the predominantly international money-laundering methods, close international collaboration and data sharing is required between supervisory, investigative and enforcement bodies. However, such collaborative efforts are often not easy to realise in practice due to differences in money laundering definitions and judicial systems. As mentioned earlier in Section 5.5, FIU-the Netherlands, investigative services and the OM frequently contact each other, share information and jointly develop initiatives with foreign partners in order to tackle money laundering.

Unregulated[163]
Some of the money laundering methods relate to or are applied in unregulated sectors. Examples of this include the threats of money laundering via underground banking and money laundering via crypto currencies. The level of resilience to the latter threat is expected to increase from 2020 onwards. Once the Amendment to the Fourth Anti-Money Laundering Directive Implementation Act enters into effect in 2020, virtual asset service providers must comply with the requirements of the Wwft, and just like other institutions with a reporting obligation under the Wwft, they must carry out a customer due diligence and report any unusual transactions to FIU-the Netherlands. In addition, there are requirements with regard to the formation of the company: virtual asset service providers must organise their processes so that they can adequately apply the aforementioned requirements to existing and new customers.[164]

The Money Laundering Action Plan refers to various options for the further regulation of virtual asset service providers. It states that the exchange of two (or more) cryptocurrencies (crypto-to-crypto) and financial service providers that issue new cryptocurrencies or offer services for an Initial Coin Offering (ICO) should be monitored. An ICO is a form of crowdfunding to raise capital, often using crypto currencies.[165]

It is possible that the tightening of policy measures may lead to a shift towards illegality or to sectors that are not yet regulated. To better understand one of the ways in which this possible waterbed effect could manifest itself, the Letter to Parliament concerning the progress of the Money Laundering Action Plan announced that an investigation will be initiated into illegal forms of trust services.[166]

162 Ministers of Finance and of Justice and Security (2019).

163 Ministers of Finance and of Justice and Security (2019).

164 www.toezicht.dnb.nl/2/50-237939.jsp.

165 The AFM describes ICOs as a way for companies – usually startups – to finance the development of certain services. By using blockchain technology, the provider issues digital tokens during an ICO. ICOs are an inherently cross-border activity: in principle, anyone with internet access and a digital wallet can buy the tokens. The offered tokens may sometimes be purchased in euros or dollars, but more often they are purchased with known cryptocurrencies such as Bitcoin or Ethereum. https://www.afm.nl/nl-nl/professionals/onderwerpen/ico.

166 Ministry of Finance and Ministry of Justice and Security (2020).

Policy instruments to be used from 2020 onwards[167]
A part of the Money Laundering Action Plan is aimed at making the activities of foundations more transparent. This would help prevent the financial and economic misuse of such foundations. Examples of this misuse include cases in which malicious parties use the legal form of a foundation as a vehicle for committing tax fraud, bankruptcy fraud or other kinds of fraud for money laundering or for developing other criminal activities. Pursuant to the Dutch Civil Code, foundations are currently obliged to draw up a balance sheet and statement of income and expenditure. The draft bill on the transparency of civil society organisations proposes changes to the Dutch Civil Code, whereby all foundations will be obliged to file these internal financial documents with the Chamber of Commerce.[168]

With respect to money laundering threats in which cash plays or may play a role, there are some plans that could further strengthen the resilience of the policy instruments. Work is currently underway on The Money Laundering Action Plan Bill (*Wet plan van aanpak witwassen*), which was presented for consultation in December 2019. This bill introduces a prohibition in the Netherlands on cash payments of EUR 3,000 and above that will apply to professional/commercial buyers or sellers of goods (traders). This prohibition replaces the current obligations under the Wwft applicable to cash payments for amounts of EUR 10,000 or more for professional/commercial buyers or sellers of goods. In addition, the Dutch government is committed to discontinuing the use of the EUR 500 banknote. Via the ECB, DNB is calling for an end date on which the EUR 500 banknote will be permanently withdrawn from circulation. In addition, the government will discuss in the National Forum on the Payment System (*Maatschappelijk Overleg Betalingsverkeer*) how the acceptance of the EUR 500 banknote can be limited as long as it remains in circulation.[169] From June 2021 onwards, Customs Service is expected to play a greater role with respect to money laundering via the physical movement of cash. Currently, this organisation is only authorised to carry out checks if cash crosses an EU external border. The General Customs Act (Algemene Douanewet) was amended in 2020, giving Customs Service a legal basis for monitoring intra-EU and inland traffic. This means that, in the case of third-country traffic, Customs Service may carry out checks not only for cash but also for other valuable goods such as jewellery, expensive watches, precious stones and antiques as well as for documents containing evidence of assets.

With respect to the money laundering threats relating to offshore companies and structures by trust offices, a bill was presented for consultation on 9 April 2020 containing three prohibitions for trust offices: (1) a general prohibition on the provision of conduit companies, (2) a prohibition on providing services to clients, object companies or UBOs of clients or object companies that are established or have their registered office in a third high-risk country and (3) a prohibition on providing services to clients, object companies or UBOs of clients or object companies that are established or have their registered office in a country that is on the list of non-cooperative countries for tax purposes.

167 The present NRA focuses on the period up to 2019. Hence, the policy instruments and other initiatives presented below have not been taken into account when determining the resilience of the policy instruments. See Section 6.2

168 Ministers of Finance and of Justice and Security (2019).

169 Ministers of Finance and of Justice and Security (2019).

Another development that may help strengthen the resilience of the policy instruments is the proposed closer cooperation between five Dutch banks. In September 2019, it was announced that ABN-AMRO, ING, Rabobank, Triodos Bank and De Volksbank want to set up an organisation to monitor payment transactions: 'Transaction Monitoring Netherlands' (*Transactie Monitoring Nederland*). The banks will investigate whether this is feasible and how the technical and legal problems can be solved. They are working closely with the government on this matter. The Money Laundering Action Plan Bill (see above) outlines legislative measures that will make this initiative possible. The intention is for other banks to join this initiative later.[170]

Further improvement opportunities
In addition to the aforementioned plans, the third expert meeting also discussed other ways of further improving the prevention and combating of money laundering. The main opportunity for improvement relates to information sharing between the parties involved in preventing and/or combating money laundering. Although it is currently possible to exchange a certain amount of information based on existing legislation such as the Police Data Act (*Wet Politiegegevens*) and via specific partnerships such as the FEC, this process of sharing information between public parties can be further improved. The Data Processing by Partnerships Act (*Wet gegevensverwerking door samenwerkingsverbanden*) – if adopted by the Senate in the future – may help in bringing this about. The Money Laundering Action Plan Bill (see above) also contains legislation introducing greater possibilities for exchanging transaction data between Wwft institutions.

In addition to an improved sharing of information at a national level, experts indicated that it is also important to further improve this at an international level. During the study, there were signs of initiatives are being developed in this field as well, for example, the strengthening of the position of the European Banking Authority (EBA) and the establishment of the European Financial and Economic Crime Centre (EFECC) within Europol. Considering that many of the greatest money laundering threats identified in this NRA have or may have an international component, it is very important to retain the focus on this aspect.

170 www.nvb.nl/nieuws/nederlandse-banken-bundelen-krachten-tegen-witwassen/.

6 Greatest money laundering risks in the Netherlands

This chapter describes the results of the second and third expert meetings. In the second expert meeting, experts assessed the potential impact of the greatest money laundering threats based on a Multi-criteria Analysis (MCA). The results of this assessment are explained in Section 6.1. In the third expert meeting, experts assessed the resilience of the available policy instruments (see Chapter 5) for the 15 greatest money laundering threats (see Chapter 4) or the extent to which these instruments counteract the potential impact of the money laundering threats. The results of this assessment are explained in Section 6.2. The final section brings together the expert assessments of the potential impact and resilience. The result is a list of the 15 greatest money laundering risks in the Netherlands, ranked by the level of their RPI (Residual Potential Impact).

6.1 Assessment of the potential impact of the greatest money laundering threats

After the final list of the 15 greatest money laundering threats had been determined in the second expert meeting, the experts assessed the potential impact of these threats using an MCA. As a first step in the MCA, the experts were asked to assign a weight to the various criteria used in the MCA. This process gave a clear indication of which criteria were considered more or less important by the experts in determining the potential impact of the threats (see Table 13). According to the experts, the deterioration in the stability of the financial system and the undermining of authority and legal order are the two most important criteria (score of 8) for measuring the potential impact of the money laundering threats. Reduction of subjective/objective security is the least important criterion (score of 6). The criterion weights are rounded off to the nearest integer because the MCA software uses criterion weights expressed in integers.[171] The criterion weights were determined over two rounds; the first estimate was followed by a plenary discussion, after which the experts made the final estimate for the criteria weights in the second round.

Table 13 Weights assigned to MCA criteria

Criteria:	Average score (On a scale of 0 to 10)
Deterioration in the stability of the financial system	8
Undermining of authority and the legal order	8
Damage to the regular economy	7
Disruption of the social order	7
Damage to the image of the Netherlands abroad	7
Reduction of subjective/objective security	6

Subsequently, for each threat and criterion, the experts assessed the possible consequences of the money laundering threats based on the six criteria (on a scale of 0 to 100). However, the experts were requested to refrain from making an assessment if they felt they were not qualified to do so for one or more of the threats. An

171 The MCA module included in the standard GDR software provided by Spilter was used.

initial round of assessment was followed by a detailed plenary discussion of the results. After this, as part of the second round of assessment, the experts were given the opportunity to adjust the earlier assessment based on any new insights possibly gained after the plenary discussion. The results of the second and final assessment of the potential impact are displayed in Table 14.

The table shows that the scores for the potential impact of most of the 15 greatest money laundering threats are fairly close together, with an outlier at the upper end and one at the lower end. The money laundering threat with the greatest potential impact (score of 66 out of 100) is money laundering via wire transfers by licensed banks. Money laundering via physical movement of cash scores lowest in terms of potential impact (score of 40 out of 100). The other 13 money laundering threats have a potential impact ranging from 49 to 57.

Table 14 Potential impact of the greatest money laundering threats

Threats	Average potential impact (On a scale of 0 to 100)	Number of experts
Money laundering via wire transfers by licensed banks	66.1	15
Money laundering via structures by trust offices	57.2	15
Money laundering via offshore companies	57.2	15
Money laundering via legal entities	56.7	15
Money laundering via dealers of high-value services/goods	55.8	14
Money laundering via trade-based structures involving services	55.2	14
Money laundering via the use of intermediaries	54.0	13
Money laundering via investment institutions/firms	54.0	14
Money laundering via trade-based structures involving goods	53.0	15
Money laundering via ABC transactions	52.7	15
Money laundering via loan-back arrangements	51.5	15
Money laundering via fictitious company turnover	51.2	15
Money laundering via crypto currencies	50.6	15
Money laundering via underground banking, including via unlicensed payment service providers	48.9	14
Money laundering via physical movement of cash	39.6	15

6.2 Assessment of the resilience of the available policy instruments

In the third expert meeting, the 15 participating experts were asked to assess the extent to which they felt that the total set of existing policy instruments are capable of countering the potential impact of the 15 greatest money laundering threats. A score from 0 to 100 could be assigned to each money laundering threat, where the higher the score, the higher the resilience. However, the experts were specifically requested to refrain from making an assessment of the resilience if they felt they were unable to properly assess the resilience of the policy instruments for countering the money laundering threats, because, for example, they did not have an adequate overview of the potential impact of the threat or if they considered themselves to be insufficiently informed about the scope and/or implementation of the policy instruments.

An initial round of assessment was followed by a detailed plenary discussion of the results. Subsequently, as part of the second round of assessment, the experts were given the opportunity to adjust the earlier assessment based on any new insights

that may have arisen after the plenary discussion. The results of the second and final assessment of the resilience are displayed in Table 15. The table shows that the experts did make use of the option to not assess the resilience for 11 of the 15 greatest money laundering threats. For the threat of money laundering via investment institutions/firms, 11 of the experts present made an assessment of the resilience and four experts refrained from doing so.

Table 15 Resilience of total set of policy instruments per money laundering threat

Threats	Average resilience (On a scale of 0 to 100)	Number of experts
Money laundering via wire transfers by licensed banks	64.1	15
Money laundering via structures by trust offices	51.6	15
Money laundering via investment institutions/firms	51.4	11
Money laundering via fictitious company turnover	48.1	14
Money laundering via legal entities	44.4	14
Money laundering via ABC transactions	44.1	14
Money laundering via the use of intermediaries	43.6	14
Money laundering via loan-back arrangements	43.3	12
Money laundering via dealers of high-value services/goods	34.6	14
Money laundering via trade-based structures involving goods	33.4	15
Money laundering via offshore companies	32.5	13
Money laundering via physical movement of cash	29.9	14
Money laundering via trade-based structures involving services	27.7	13
Money laundering via crypto currencies	20.1	14
Money laundering via underground banking, including via unlicensed payment service providers	18.9	15
Average for the 15 greatest money laundering threats	39.1	

For one of the money laundering threats, i.e. money laundering via wire transfers by licensed banks, the resilience score was above 60 (score of 64.1). According to experts, this means that the total set of policy instruments available have a relatively significant mitigating effect as far as this money laundering threat is concerned. This score implies that almost 64.1% of the estimated potential impact of this money laundering threat is countered.

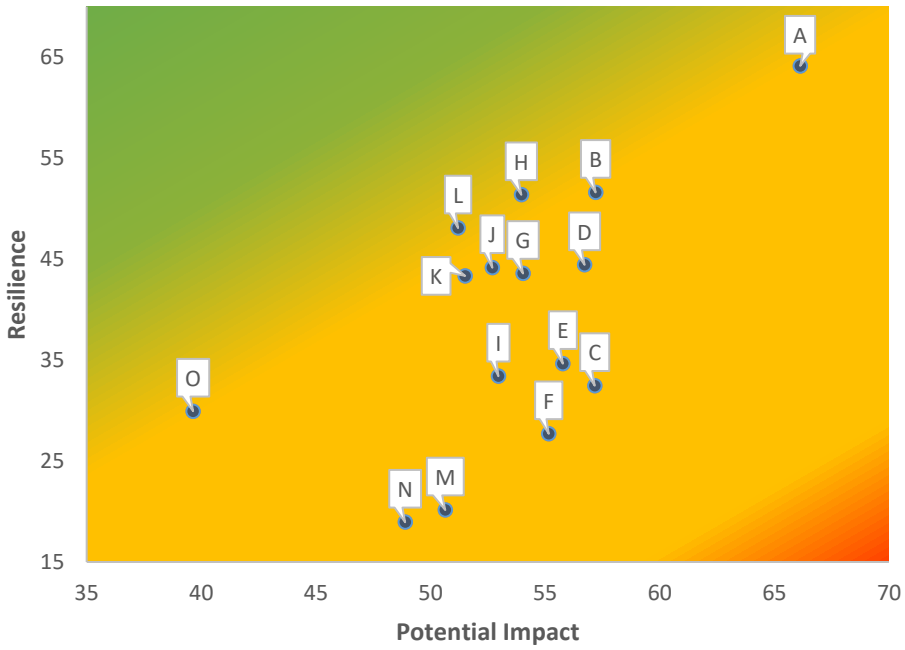
Other money laundering threats for which the available policy instruments offer a relatively high level of resilience are, according to experts, money laundering via structures by trust offices (score of 51.6) and money laundering via investment institutions/firms (score of 51.4). An important note in this respect is that the experts have estimated the resilience to these two threats as being high, because they have based their assessment on *licensed* institutions *established in the Netherlands*. Hence, the resilience against money laundering via structures involving offshore companies (established abroad) is scored much lower (score of 32.5).

The resilience of the policy instruments is relatively low for two of the money laundering threats, i.e. money laundering via crypto currencies (score of 20.1) and money laundering via underground banking including unlicensed payment service providers (score of 18.9). This means that, according to experts, the total range of policy instruments available until 2019 are only able to counteract this money laundering threat to a relatively limited extent.

6.3 Greatest money laundering risks in the Netherlands

Figure 2 brings together the expert assessments of the potential impact (second expert meeting) and resilience (third expert meeting) for the 15 money laundering threats. Threats with a high potential impact and low resilience are considered high-risk. The figure shows that this high-risk combination does not occur for the 15 money laundering threats focused on in this NRA.

Figure 2 Potential impact compared to resilience for the 15 greatest money laundering threats



A Wire transfers by licensed banks
B Structures by trust offices
C Offshore companies
D Legal entities
E Dealers of high-value services/goods
F Trade-based structures involving services
G Use of intermediaries
H Investment institutions/firms
I Trade-based structures involving goods
J ABC transactions
K Loan-back arrangements
L Fictitious company turnover
M Crypto currencies
N Underground banking including unlicensed payment service providers
O Physical movement of cash

Figure 2 shows that many of these money laundering threats are similar to one another in terms of potential impact and resilience. However, this is not the case for money laundering via wire transfers by licensed banks because this has a relatively high potential impact and the resilience is also relatively high. According to the experts, this means that this threat may have very harmful consequences, but the policy instruments are able to counter the impact of this threat to a relatively large extent. Money laundering via physical movement of cash also falls outside the point cloud in which the other threats are positioned. In fact, this money laundering threat has been assigned a low score by the experts, both in terms of potential impact and resilience: experts believe that this money laundering threat – in comparison with the other threats – may have less harmful consequences and that the policy instruments can only counteract this threat to a limited extent. The highest

risks, however, can be linked to the money laundering threats positioned in the lowermost right-hand corner of Figure 2.

But Figure 2 does not provide a clear answer about the extent to which the available policy instruments are able to counteract the potential impact of the 15 money laundering threats assessed in this NRA. To gain more insight into this, a subsequent step of the analysis assessed the residual potential impact of each threat after taking into account the mitigating effect – or in other words, the resilience – of the policy instruments. The result of this is the final list of the 15 greatest money laundering risks in the Netherlands, ranked by the potential impact that remains after taking into account the mitigating effect of the policy instruments. In this NRA, this is referred to as the residual potential impact (RPI).[172] The magnitude of the RPI determines the scope of the money laundering risk. The results of this analysis are shown in Table 16:

Table 16 The 15 greatest money laundering risks in the Netherlands

Risks	Residual Potential Impact (RPI) (scale from 0-100)
Money laundering via crypto currencies Money laundering via trade-based constructions involving services Money laundering via underground banking, including unlicensed payment service providers Money laundering via offshore companies Money laundering via dealers of high value services/goods	36 to 40
Money laundering via trade-based constructions involving goods Money laundering via legal entities Money laundering via the use of intermediaries	31 to 35
Money laundering via ABC transactions Money laundering via loan back constructions Money laundering via the physical movement of cash Money laundering via structures by trust offices Money laundering via fictitious company turnover Money laundering via investment institutions/companies	26 to 30
Money laundering via wire transfers by licensed banks	21 to 25

The RPI scores for the 15 money laundering risks range from 24 to 40 (on a scale of 0 to 100). This means that the RPI scores are not very high. Since these scores do not differ widely from one another and are based on the inherently and partly subjective expert assessments, they have been presented in a clustered form in Table 16.[173] Of the 15 money laundering risks, five risks fall into the highest RPI score category of 36 to 40 in this NRA. This includes money laundering via crypto currencies, via trade-based structures involving services, via underground banking including unlicensed payment service providers, via offshore companies and via dealers of high-value services/goods. These risks also appeared in the bottom right quadrant in Figure 2. The lowest RPI score is for money laundering via wire transfers by licensed banks. This can be traced back to the relatively high resilience score for this money laundering risk.

172 Residual Potential Impact (RPI) = (Potential Impact*(100 – Resilience))/100.

173 The overview with the exact RPI scores is included in Appendix 6.

Comparison with results from the first Money Laundering NRA

The main differences and similarities are as follows:

- One difference is that the money laundering risks in this second NRA are specified in greater detail than in the first NRA. This means that the potential impact has been estimated for a larger number of money laundering threats in the present NRA (for 15 threats instead of 10 threats[174]) and the wording of approximately the same money laundering threats differs, to a greater or lesser extent, in the two NRAs.
- As far as the identified money laundering risks are concerned, the differences between the first and second NRA are limited. In both this NRA and the first NRA, the potential impact of money laundering via licensed banks was estimated as being the highest. Furthermore, money laundering via trust offices, offshore companies, trade-based structures involving services, trade-based structures involving goods, crypto currencies, physical movement of cash, underground banking and investment and/or investment structures have emerged as the greatest money laundering risks in both NRAs, albeit with somewhat different wording.
- Three money laundering risks from the first NRA that appear not to have been included in the second NRA have in fact been designated as part of the greatest money laundering risks but under a different name. This refers to the following money laundering risks from the first NRA:
  - *Money laundering via payment service provider*s: in the second NRA, this risk is reflected in the specific description of the risk of money laundering via underground banking including unlicensed payment service providers. The risk of money laundering via licensed payment service providers has not been classified as a serious money laundering threat in this second NRA.
  - *Money laundering constructions to conceal actual value*: this generally worded overarching risk category relates to many of the money laundering risks identified in the second NRA. It refers to the money laundering risks involving the use of specific structures to disguise funds obtained via crime such as the setting up of trade-based structures involving goods or services, structures by trust offices, ABC transactions and loan-back arrangements and fictitious company turnover.
  - *Money laundering via tax-driven/complex corporate structures:* this type of risk is reflected in the present NRA in three specific risks: money laundering via structures by trust offices, via offshore companies and via legal entities.

174 In the first NRA, these threats had been identified as risks in the analysis phase itself. Due to a more accurate application of the risk equation, the term 'risk' in this second NRA is only used when all elements of the risk equation have been taken into account. In this second NRA, the risks are no longer an intermediate step in the analysis, but the final result.

7 Conclusions

This final chapter begins by describing the key results of this second Money Laundering NRA. The focus is on providing an answer to the research questions. Subsequently, the NRA is evaluated based on the growth model of the NRA methodology, with an explanation of the strengths of and areas for improvement in the research methodology used. Finally, the chapter lists some of the lessons learned, which may be useful in giving shape to the next NRA.

7.1 Answers to the research questions

Research Question 1: What are the context-related factors that may influence the prevalence of money laundering in the Netherlands?
For this second NRA, a context analysis has been carried out to examine the characteristics of the Netherlands that may influence the prevalence of money laundering in our country. The geographic, demographic, socio-cultural, economic and criminological characteristics of the Netherlands have been examined.

The Netherlands is characterised by an open, trade-oriented economy, a large and internationally oriented financial sector and is fiscally attractive for large foreign companies. The country is one of the most competitive economies in the world, boasts an airport and port that are among the largest in the world and it is one of the largest exporters in the world. The Dutch economy can be described as a service economy. All these characteristics make the Netherlands attractive to criminals for laundering their criminally obtained money. Compared to other European countries, the Netherlands is characterised by relatively few cash payments and a high degree of digitalisation. These factors may influence the money laundering methods used by criminals. A socio-cultural factor typical to the Netherlands is its culture of tolerance where, particularly, the tolerance towards soft drugs may contribute to the occurrence of drug-related crime and the laundering of the proceeds thereof. In keeping with the culture of the Polder Model, it is customary for Dutch organisations to seek consensus and cooperation with other organisations. In this sense, the Netherlands can be distinguished from many other countries by the relatively high prevalence and wide variety of partnerships that have been established to prevent and combat money laundering. This includes public-public, public-private and private-private partnerships.

Research Question 2: What can be said about the nature, mechanisms and potential impact of the greatest money laundering threats and the types of crime that may precede these threats?
The 15 money laundering threats with the greatest potential impact as assessed by experts in this field are categorised and displayed in Table 17. The scope of the potential impact of the threats is determined by performing an MCA. Experts arrived at quantitative estimates that ultimately determined the scope of the potential impact based on the following six criteria: deterioration in the stability of the financial system, undermining of authority and legal order, damage to the regular economy, disruption of social order, damage to the international reputation of the Netherlands and reduction of subjective/objective security.
According to experts, the money laundering threat with the greatest potential impact is that of money laundering via wire transfers by licensed banks. Money laun-

dering via the physical movement of cash scores the lowest in terms of potential impact. Most of the money laundering threats have a potential impact ranging from 50 to 59 on a scale of 100.

Table 17 The 15 greatest money laundering threats*

Threats	Potential impact level (scale from 0-100)
Money laundering via wire transfers by licensed banks	60 to 69
Money laundering via structures by trust offices Money laundering via offshore companies Money laundering via legal entities Money laundering via dealers of high value services/goods Money laundering via trade-based constructions involving services Money laundering via the use of intermediaries Money laundering via investment institutions/companies Money laundering via trade-based constructions involving goods Money laundering via ABC transactions Money laundering via loan back constructions Money laundering via fictitious company turnover Money laundering via crypto currencies	50 to 59
Money laundering via underground banking, including unlicensed payment service providers Money laundering via the physical movement of cash	40 to 49

* The table with the exact impact scores can be found in Appendix 6.

A multitude of methods – whether or not used in combination with one another – may be used to launder criminal money. These money laundering methods may occur at different stages of the money laundering process. The FATF distinguishes three phases, i.e. the placement, layering and integration phases. Chapter 4 of this report examines the nature and mechanisms of the threat for each identified money laundering threat. Cases have been included for the vast majority of threats to illustrate and explain the way in which money laundering threats may occur. Some identified money laundering threats involve methods that are quite simple in nature, while others involve methods of a very complex nature. Some money laundering methods may be part of other methods and many of the greatest money laundering threats may be used in combination with one another.

With respect to the criminal activity that precedes money laundering, a study into the nature and extent of criminal expenditures shows that drugs and financial fraud are jointly responsible for more than 90% of the money laundering needs of criminals in the Netherlands, where the amount for fraud is estimated as being approximately three times as high as that for drug-related crimes.

Based on the in-depth interviews and expert meetings, it does not appear that certain money laundering methods are related to certain types of crime. However, compared to financial fraud, drug-related crime involves a greater use of cash, which influences whether or not it is necessary to place the criminal money in the financial system which, in turn, has consequences for the types of money laundering methods used by a criminal.

Research Question 3: What are the money laundering threats that have not yet been identified in the Netherlands, but could become relevant in the future?

The FLUU survey, the three expert meetings and the in-depth interviews with experts focused on the currently prevalent money laundering threats. Although the survey inquired about money laundering threats that were missing from the survey and the interviews asked about future threats, the experts were unable to identify any future threats. However, the nature of one of the 15 greatest money laundering threats identified, i.e. money laundering via investment institutions/firms, does involve a 'future' element. In the opinion of the experts, although this threat currently exists, there is still too little experience and information available to indicate how and on what scale money laundering via investment institutions/firms is currently taking place. This is why this NRA does not include a case description of money laundering via investment institutions/firms. In a validating interview, it was noted that the greatest risk is expected to involve unlicensed and/or investment institutions/firms not established in the Netherlands.

Research Question 4: What policy instruments are available in the Netherlands for preventing and combating the greatest money laundering threats?

The available policy instruments for preventing and combating money laundering include all the relevant instruments based on municipal, national and international laws and regulations as well as regulations outlined at sectoral and organisational levels. In this NRA, however, the term 'policy instrument' refers to more than just laws and regulations. According to the experts, the guidelines, instructions and policy plans of organisations that play a role in preventing and combating money laundering may also be seen as policy instruments. In addition, partnerships between organisations with a role in preventing and/or combating money laundering are also seen by experts as a policy instrument.

Table 18 Policy instruments for preventing and combating money laundering

International laws and regulations	National laws and regulations	Other policy instruments
FATF-recommendations	Money Laundering and Terrorist Financing Prevention Act	National partnerships
EU Anti-Money Laundering Directive	Financial Supervision Act	International partnerships
EU Regulation on Controls of Cash	Penal Code	Sectoral and sector-oriented regulations and terms and conditions
Wire Transfer Regulation 2	Code of Criminal Procedure	Guidelines and policy plans
	Trust and Company Service Providers (Supervision) Act 2018	
	Public Administration Probity Screening Act	
	Legal Entities Supervision Act	
	Commercial Register Act 2007	
	Tax legislation	
	Economic Offences Act	
	Right to report Tax and Customs Administration 2003	

Table 18 provides an overview of the policy instruments that were available in 2019 to prevent and combat money laundering. These policy instruments are explained in

greater detail in Chapter 5. It is important to note that the overview in this table relates to the situation at the end of 2019. Experts have based their assessment of the resilience of the policy instruments on the specific instruments that existed *at that time*. This means that they have not taken into account any laws and regulations and other policy instruments that have been or are intended to be introduced from the beginning of 2020.

Research Question 5: What can be said about the resilience of the available policy instruments for preventing and combating the greatest money laundering threats?

Money laundering experts have assessed the extent to which the total set of existing policy instruments counteracts the potential impact of the 15 greatest money laundering threats. The results of the expert meeting are categorised and displayed in Table 19.

Table 19 Resilience of total set of policy instruments per money laundering threat*

Threats	Resilience level (scale from 0-100)
Money laundering via wire transfers by licensed banks	60 to 69
Money laundering via structures by trust offices Money laundering via investment institutions/companies	50 to 59
Money laundering via fictitious company turnover Money laundering via legal entities Money laundering via ABC transactions Money laundering via the use of intermediaries Money laundering via loan back constructions	40 to 49
Money laundering via dealers of high value services/goods Money laundering via trade-based constructions involving goods Money laundering via offshore companies Money laundering via the physical movement of cash	30 to 39
Money laundering via trade-based constructions involving services Money laundering via crypto currencies	20 to 29
Money laundering via underground banking, including unlicensed payment service providers	10 to 19

* The table with the exact resilience scores can be found in Appendix 6.

The resilience score was above 60% for one money laundering threat, i.e. money laundering via wire transfers by licensed banks. According to experts, this means that the total set of available policy instruments are able to counter more than 60% of this money laundering threat. The other money laundering threats for which the available policy instruments offer a relatively high level of resilience are, according to experts, money laundering via structures by trust offices and money laundering via investment institutions/firms. An important note in this respect is that the experts have estimated the resilience to these two threats as being high because they have based their assessment on licensed institutions established in the Netherlands.

Although the available instruments clearly have a mitigating effect on the 15 greatest money laundering threats focused on in this NRA, these threats may still have a certain amount of impact, to a greater or lesser extent. The mitigating effect of the policy instruments depends on the extent to which the AIU principle, as introduced earlier in the first NRA, is applicable to the money laundering threats. Under the AIU principle, one or more of the following three components are applicable to most of the money laundering methods: anonymous (the method conceals the identity of

the criminal involved in money laundering), international (the method has an international character and is applied via or from abroad), and unregulated (the method relates to or is applied in an unregulated sector). The greater the applicability of the AIU elements to the money laundering threats, the lower the resilience of the policy instruments for the prevention and suppression of the threats. For such money laundering threats, the chance of apprehending the criminal involved in money laundering activities is therefore relatively low.

To effectively prevent and combat the predominantly international money-laundering risks, close international collaboration and data sharing is required between supervisory, investigative and law enforcement authorities. However, such collaborative efforts are often not easy to realise in practice due to differences in money laundering definitions, enforcement practices and judicial systems. With regard to the money laundering threats at financial institutions and service providers that operate without a licence – for example, the threat of underground banking – the available policy instruments are, according to the experts, limited in terms of capacity and not adequately implemented to effectively counter the risks. Finally, there appears to be a relatively low level of resilience with respect to methods that increase the anonymity of transactions such as money laundering via crypto currencies, underground banking and the physical movement of cash.

Research Question 6: What money laundering threats are considered by experts as the greatest money laundering risks?
By comparing the estimated potential impact of the greatest money laundering threats with the estimated resilience, the WODC gained a better understanding of the greatest money laundering risks in the Netherlands, ranked by their RPI.

Table 20 Residual Potential Impact (RPI) of the 15 greatest money laundering risks*

Risks	Residual Potential Impact (RPI) (scale from 0-100)
Money laundering via crypto currencies	36 to 40
Money laundering via trade-based constructions involving services	
Money laundering via underground banking, including unlicensed payment service providers	
Money laundering via offshore companies	
Money laundering via dealers of high value services/goods	
Money laundering via trade-based constructions involving goods	31 to 35
Money laundering via legal entities	
Money laundering via the use of intermediaries	
Money laundering via ABC transactions	26 to 30
Money laundering via loan back constructions	
Money laundering via the physical movement of cash	
Money laundering via structures by trust offices	
Money laundering via fictitious company turnover	
Money laundering via investment institutions/companies	
Money laundering via wire transfers by licensed banks	21 to 25

* The table showing the exact RPI scores can be found in Appendix 6.

Five of the 15 money laundering risks fall in the highest RPI score category of 36 to 40 on a scale that, in theory, can go up to 100. Money laundering via wire transfers by licensed banks has the lowest RPI score, as a result of the relatively high resilience score for this risk. From this, it can be concluded that the impact of the money

laundering threats is levelled off to a considerable extent by the available policy instruments.

Research Question 7: To what extent can the data available within expert organisations be used for a quantitative data analysis of the identified risks?
This second NRA has made an initial attempt to collect – via iCOV – quantitative data for three of the identified money laundering threats, i.e. money laundering via ABC transactions, money laundering via loan-back arrangements and money laundering via legal entities. Via iCOV, data can be combined from various data sources that are relevant for understanding money laundering threats, in order to collectively analyse these data. Due to operational problems, it was ultimately not possible to gain access to these data within the time frame of the NRA. When it became clear that the iCOV process would not lead to the collection of the intended quantitative data, contact was made with Justis and in collaboration with Justis, quantitative data were collected that was presumed to offer some insight into money laundering via legal entities. The quantitative data analysis has provided limited insight into a number of unusual situations concerning legal entities that may relate to money laundering. However, it can be concluded that the data on legal entities available to the NRA cannot be used to establish a direct relationship with money laundering since the data files supplied by Justis could only consist of aggregated information from the Commercial Register of the Chamber of Commerce. Within the conditions applicable to the use of the Justis data, it was not possible for the NRA to link to other data sources that might have enriched the information obtained from the Justis data, such as sources containing data on judicial records and transactions declared suspicious by FIU-the Netherlands.

Research Question 8: What further data do we need for gaining a better insight into the identified risks?
The analysis of the data files supplied by Justis illustrates the limitations of requesting data sets separately from different data source holders. For complex assessment questions such as the need to provide insight into the money laundering risks, there is a need to combine data from different perspectives. For example, a more direct link with money laundering could potentially have been established for the risk of money laundering via legal entities, if a link could be established between, on the one hand, the legal entities, and on the other hand, the involvement of the directors of these legal entities in financial and economic crime, or with the help of data from the Commercial Register combined with data on transactions declared suspicious by FIU-the Netherlands and other criminal information. However, without further criminal investigation, it will remain very difficult to link the data to money laundering with sufficient confidence.

Research Question 9: What lessons have been learned that could be applied to future NRAs?
The following sections of this chapter answer this research question in detail. Firstly, the strengths and areas for improvement of the research methodology used in this NRA are explained. This is followed by a description of some of the lessons learned, which can be taken into account when implementing a subsequent NRA.

7.2 Evaluation of the second NRA

Chapter 2 includes an extensive description of how this second NRA was performed. The selected approach builds on the experiences gained from the first NRA and fits

within the chosen growth model for methodology development of the Dutch NRAs. In order to learn from the experiences gained, an attempt has been made to report as transparently as possible and a self-evaluation, as described in this section, has been carried out.

As in the first NRA, the research approach is structured based on the ISO 31000 risk management framework. In short, the research methodology involved the following steps:

- A context analysis outlining the specific characteristics of the Netherlands that may influence the prevalence of money laundering. A literature study was conducted for the purpose of this context analysis.
- In order to prepare an inventory of the threats in the field of money laundering, a literature study was carried out and the FLUU Survey was conducted among money laundering experts.
- Subsequently, at the first expert meeting, experts identified the money laundering threats they felt had the greatest potential impact.
- In the period after the first expert meeting, the nature and mechanisms of the greatest money laundering threats identified were more closely examined via in-depth interviews with experts.
- In the second expert meeting, experts assessed the potential impact of the 15 greatest money laundering threats that have been specified in detail based on an MCA.
- Thereafter, a survey was conducted among the experts to gain more knowledge of the policy instruments available for the prevention and suppression of money laundering.
- In the third expert meeting, experts assessed the resilience of the available policy instruments designed to prevent or suppress the 15 greatest money laundering threats. By comparing the estimated potential impact of the greatest money laundering threats with the estimated resilience, the WODC gained a better understanding of the greatest money laundering risks in the Netherlands, ranked by their RPI (Residual Potential Impact).
- Finally, in the last phase of the study, validating interviews were conducted with six key experts, the primary objective of which was to determine to what extent they agreed with the ranking of the identified money laundering risks (according to the RPI score, see Table 20) and how they thought these risks could be further countered.

In addition to the above-mentioned mainly qualitative research methods, a quantitative data analysis was carried out in cooperation with Justis for the risk of money laundering via legal entities. An attempt was made to obtain a clearer picture of a non-transparent 'stacking' of legal entities and changes in the management of legal entities.

Strengths of this second NRA

There are a number of strengths to be noted with regard to the implementation of this second NRA, some of which were also mentioned earlier in the first Money Laundering NRA of 2017. These are briefly repeated below:

- *Close involvement of the sector:* all organisations that play a role in the prevention and/or suppression of money laundering in any way were involved in the assessment at some point.
- *Transparent description of the applied methodology*: the applied methodology, including the method of data collection and the MCA used, has been described in a transparent manner with a view to the growth model of the NRA (learning from

experiences) and further refinement of the applied methodology. The aim is to maximise the reproducibility of the research.

- *Significant added value of the GDR*: the GDR (Group Decision Room) is time-efficient compared to a regular meeting and creates the opportunity to understand the results in greater depth through plenary discussions. The use of the GDR (by alternating group discussions with entering assessments on a laptop) ensures that the experts participate actively throughout the meeting. In addition, the GDR simplifies the process of data collection. Finally, the GDR ensures that the numerical scores assigned by all the experts present at the meeting are included, which means that all relevant perspectives are also taken into account in the final risk assessment. All relevant perspectives are represented here.
- *Structuring effect of the MCA:* the MCA was conducted within the GDR environment and helped to make the meeting more structured, contributed to the data collection process and ensured the transparency of the results and the process by which they had been achieved. The MCA uses predefined criteria, on the basis of which the experts assessed the potential impact of the greatest money laundering threats. This created fewer opportunities for the experts to allow personal interests to play a role in their assessment of the severity of the money laundering threats.
- *Delphi method important for risk identification*: the Delphi method was used to identify the greatest money laundering threats, determine the potential impact of the threats and assess the resilience of the policy instruments. Over two rounds and an intervening group discussion, experts were able to indicate their choices or estimates. Following the group discussion, experts adjusted their initial assessments so that the money laundering threats that remained outside the list of greatest money laundering threats after the first round of identification could still be included on this list.
- *Validation of NRA results.* six key experts were interviewed in the final phase of the NRA. The validation confirmed that the ranking of the 15 greatest money laundering risks was widely recognised.

Another strength of this second NRA can be attributed to a lesson learned from the first NRA conducted in 2017:

- *More attention to substantiation and detail:* Another lesson learned from the first NRA was that the second NRA (and subsequent NRAs) should pay more attention to substantiating and gaining a deeper understanding of the greatest money laundering threats identified by experts. This second NRA has devoted more attention in various ways to further substantiating and gaining a deeper understanding of the research findings:
  - *FLUU Survey*: in the FLUU Survey, experts were asked to indicate, on the longlist of threats sent to them, whether they are aware of facts or cases relating to the threats and to what extent they consider the prevalence of the threats likely or not based on the information available within their organisation. The survey provided insight into whether or not expert organisations were familiar with the offences or cases relating to the threats in the longlist, which helped provide more clarity about the organisations that should be invited to the expert meetings.
  - *Three expert meetings instead of two:* thanks to this, there was a greater opportunity for plenary discussions on the longlist of threats and relevant cases. At the first expert meeting, the entire longlist of money laundering threats as well as the threats added to the list based based on the FLUU Survey were discussed extensively with all the participating experts. This resulted in a few adjustments to the longlist of threats (merging of multiple threats, splitting of a

single threat into multiple threats and a more precise formulation). When discussing each threat, participants were requested to discuss the cases known to them. More time was also provided during the second expert meeting to substantiate and discuss the views of the participants.
  - *In-depth interviews:* After the first expert meeting, in-depth interviews were held with representatives of the expert organisations in order to gain more insight into the greatest money laundering threats identified at the meeting. These interviews inquired about the nature and mechanisms of the threats and about concrete cases involving these threats. The results were discussed at the beginning of the second expert meeting, which led to a further refinement and expansion of the list of greatest money laundering threats.
  - *Cases included in reports:* besides paying attention to the cases discussed in the expert meetings and the in-depth interviews, other cases involving money laundering threats were also collected and reported via desk research.
  - *Policy instruments survey:* prior to the third expert meeting, a longlist of policy instruments was sent to the experts via an email survey. They were asked to indicate how they thought the policy instruments contributed to the prevention and/or suppression of money laundering. They were also asked about existing policy instruments that were missing from the longlist sent to them and about other policy instruments that did not yet exist but which they felt might contribute significantly to the prevention and/or suppression of money laundering. The findings of the email survey formed the input for the third expert meeting. The plenary discussion of the various policy instruments resulted in an overview of the existing policy instruments that experts believe could make an important contribution to the prevention and suppression of the greatest money laundering threats.
- *Data-oriented NRA:* in the NRA, due attention has been paid to making the study more data-oriented. Although it must be noted that the contribution of the quantitative part is limited in this NRA, the exercise has yielded useful experiences and insights that can be used in a subsequent NRA. The exercise carried out using the Justis data has shown that unlinked data supplied by the individual organisations involved in preventing or combating money laundering do not provide sufficiently effective information that can serve as a basis for a risk assessment. Hence, it is necessary to look for a body that can bring together data from the relevant organisations and analyse these data items in relation to one another. This was also the reason for involving iCOV in the NRA. During the research process, it was seen that the infrastructure for data collection via iCOV was not yet organised such that the NRA could make use of it in this edition. For this reason, this strength has also generated an important point for consideration in a subsequent NRA (see below).

Points to consider in this second NRA

As in the case of the first NRA, there are certain points that must be taken into consideration when evaluating the results of the NRA. These points are largely inherent to the selected approach. In selecting the applied research methodology, an attempt has been made to carefully balance both the advantages and disadvantages that may be associated with these research tools.

- One of the lessons learned from the first NRA was that more attention needed to be paid to how the quantitative data analyses were performed. As a first step towards this, the intention was to perform a quantitative data analysis in the NRA for the risks of money laundering via legal entities, money laundering via ABC transactions and money laundering via loan-back arrangements. To this end, as mentioned above, cooperation was initially sought with iCOV because it has

access to a large number of data sources.[175] Unfortunately, the necessary declarations of consent from the various data source holders could not be obtained within the assessment time frame. When it became clear that this would not be achieved in time, the WODC sought out Justis, the screening authority of the Ministry of Justice and Security. A quantitative data analysis was carried out for the risk of money laundering via legal entities via Justis and with the help of data from the Commercial Register of the Chamber of Commerce, based on the presumption that these data would help in further clarifying the risk. However, the analysis showed that no direct relationship with money laundering could be established based on such a data analysis without a link to other data sources, for example, sources containing data on transactions declared suspicious by FIU-the Netherlands and other criminal or tax information. The analyses only provide limited insight into a number of allegedly unusual situations.

- The NRA is primarily based on the opinions and assessments of representatives of various investigative, law enforcement and supervisory authorities, and umbrella/sector organisations of entities with a reporting obligation. Although the chosen research approach has tried to optimise the conditions for reliable data collection, it cannot be entirely ruled out that subjective elements have also played a role in identifying the greatest money laundering threats, estimating their potential impact and assessing the resilience of the policy instruments and that these tasks may have been performed partly based on perceptions/personal opinions.
- During the expert meetings, there was an impression that the experts present did not have an equal level of knowledge and experience; not all experts were equal in expertise on all the topics discussed and not all assessments could be satisfactorily substantiated to the same extent. Although the FLUU Survey has provided insight into the knowledge available in expert organisations, this assessment tool has not been able to entirely avoid the aforementioned bottleneck. The difference in knowledge level may also relate to the fact that the participants at expert meetings are involved in different ways in the prevention and suppression of money laundering. Since each expert has his or her own field of knowledge and specific experiences, the participants had a lot of knowledge about some threats and less knowledge about others. In a general sense, the knowledge level of the participants at the expert meetings also seemed to differ. No corrections, for example, by applying a weight, have been made for these differences. After all, there are no objective grounds for determining such a weight. Moreover, there was not a single participant at the expert meetings who had knowledge of the entire field and a complete overview of all threats in the field of money laundering and/or the resilience of the policy instruments.
- Despite their knowledge of certain parts of the field, it was difficult for some experts to make a proper quantitative assessment of the criteria for determining the potential impact of the greatest money laundering threats and the resilience of the policy instruments. To reduce this risk, experts were asked to refrain from making a quantitative assessment if they felt that they did not have the necessary knowledge to arrive at a proper assessment, and they did make use of this option. In the second expert meeting, there were at least two experts who did not score the criteria for determining potential impact (in the second round of assessment) for five of the money laundering threats. One of the experts did not score the potential impact of any of the money laundering threats. In the third expert meeting, there was at least one expert who did not score the criteria for deter-

175 Via iCOV, it is possible to access data from the Tax and Customs Administration, Netherlands Police, OM, FIOD, Netherlands Police Internal Investigations Department (*Rijksrecherche*), FIU-the Netherlands, Chamber of Commerce, Netherlands' Cadastre, Land Registry and Mapping Agency (*Kadaster*) and DNB.

mining resilience (in the second round of assessment) for eleven of the money laundering threats. Four experts did not assign a score for one of the money laundering threats.
- Finally, it was difficult to bring all the relevant expert organisations together for each expert meeting. In some cases, experts had signed up to attend but had to cancel at the last minute, which meant that their organisation was no longer represented at the expert meeting in question.

7.3 Lessons for the next NRA

This section sets out a number of lessons that should be taken into account when carrying out subsequent NRAs.

- *Improvement of the FLUU Survey*: Although the FLUU Survey clearly added value to this second NRA, the survey itself could be designed better. It is advisable to ask the representatives of the organisations more explicitly about their *own* practical knowledge concerning the prevalence of the money laundering threats on the longlist. Some of the respondents may have completed the survey in another manner: they indicated that they are aware of certain threats, while they have likely only heard of this information from other organisations or from other sources. A further improvement of the FLUU Survey will provide useful leads for determining the invitation policy for the expert meetings. Moreover, a more precisely worded FLUU Survey could provide a starting point for assigning weights to the expert assessments, for example, when performing the MCA or determining the resilience of the policy instruments.
- *Greater involvement of experts in determining MCA criteria:* earlier in this chapter, the close involvement of the experts in the field was mentioned as a strength of the second NRA. However, experts were not involved in one part of the research: the formulation and determination of the MCA criteria based on which experts have assessed the potential impact of the greatest money laundering threats. These MCA criteria have been determined in consultation with the Scientific Advisory Committee based on a literature study. For a subsequent NRA, involving experts to a greater extent in determining the MCA criteria could be considered. This may allow the list of MCA criteria to be further refined.
- In this second NRA, experts were requested to make a quantitative assessment of the potential impact of the greatest money laundering threats and the resilience of the policy instruments. This involves making a quantitative assessment of two of the three elements in the risk equation based on which the risks are determined. For the vulnerabilities element in the risk equation, no separate quantitative assessment was made for the influence of the reasonably fixed context-related characteristics on the money laundering risks. Experts have been asked to take into account the Dutch context within which the money laundering threats may arise when assessing the potential impact. However, in a subsequent NRA, it may be decided to ask experts to also make a quantitative assessment for the vulnerabilities element. This could be done, for example, on the basis of an MCA, where the various general characteristics of the Netherlands dealt with in the context analysis can be used as the MCA criteria.
- *Quantitative data analysis:* in this second NRA due attention has been paid on performing a quantitative data analysis in collaboration with iCOV and Justis. The quantitative data analysis has provided insight into a number of unusual situations relating to legal entities. As previously reported, it was not possible to establish a direct relationship with money laundering based on these data. Even if additional data sources are included in the analysis in a subsequent NRA, these

are not expected to provide insight into the prevalence of the money laundering risk in question. In fact, a definite relationship with money laundering cannot be established without further criminal investigation. A complicating factor in carrying out a more data-based NRA is the wide divergence in the nature of the money laundering risks and the required data sources. For example, the money laundering risk of crypto currencies requires different data sources than the risks relating to the physical movement of cash, wire transfers by licensed banks and underground banking. The NRA involves a complex analysis encompassing all the risks, in which the various data sources must be linked to one another. For this, the data sources must meet certain quality requirements in terms of completeness, reliability, validity and mutual compatibility. At present, there is insufficient knowledge and insight about the extent to which these quality requirements can be met. In addition, the actual process of performing a quantitative data analysis has shown that obtaining consent for the use of the data is no easy task. Each data owner must be precisely informed about what data is being requested for what purpose. In doing so, a trade-off must be made between the desired and available data required for reliably identifying the risks. Finally, data source holders must grant permission for the use of their data for the purpose of the NRA. All data source holders must grant permission for this separately. Although discussions were held with iCOV in the initial phase of the NRA process, this proved to be too time-intensive to be completed within the scope of this NRA. In order to streamline the data collection process and include a meaningful data analysis in a subsequent NRA, it is recommended that a separate exploratory study be carried out prior to the upcoming NRA. Such a study could examine how the available data sources can be made compatible, suitable and available for a meaningful data analysis in a subsequent NRA. Experience gained during this NRA has shown that it is difficult to carry out the NRA and this exploratory study at the same time. It must be concluded at present that data analyses are not yet suitable as an alternative to a high-quality NRA and therefore offer only limited added value for such a study.

References

Belastingdienst (2004). *Jaarverslag Belastingdienst 2003.*

Besamusca, E., & Verheul, J. (2010). Introduction. In E. Besamusca & J. Verheul (red.), *Discovering the Dutch: On culture and society of the Netherlands*. Amsterdam: Amsterdam University Press.

Blouin, J, Robinson, L. (2019). Double counting accounting: How much profit of multinational enterprises is really in tax havens? *SSRN*, (versie van 21 mei 2020). http://dx.doi.org/10.2139/ssrn.3491451.

Boerman, F., Grapendaal, M., Nieuwenhuis, F., & Stoffers, E. (2017). *Nationaal dreigingsbeeld 2017 georganiseerde criminaliteit.* Zoetermeer: Dienst Landelijke Organisatieinformatie Nationale Politie.

CBS (2010). *Minder traditionele criminaliteit, meer cybercrime.* www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime.

CBS (2017). *Belang dienstensector sinds 1969 sterk toegenomen.* www.cbs.nl/nl-nl/nieuws/2017/27/belang-dienstensector-sinds-1969-sterk-toegenomen.

CBS (2019a). *Nederland Handelsland 2019*.

CBS (2019b). *De effectieve vennootschapsbelastingdruk, 2006-2017.* www.cbs.nl/nl-nl/maatwerk/2019/43/de-effectieve-vennootschapsbelastingdruk-2006-2017.

Central Bank of Cyprus en FIU-Cyprus (2018). *National Assessment of Money Laundering and Terrorist Financing Risks.* Cyprus: CBC/MOKAS.

CPB (2019). *Risicorapportage Financiële markten 2019*.

Department of State. Bureau for International Narcotics and Law Enforcement Affairs (2019a). *2016 International Narcotics Control Strategy Report Volume I: Drug and chemical control.* United States Department of State.

Department of State. Bureau for International Narcotics and Law Enforcement Affairs (2019b). *2016 International Narcotics Control Strategy Report Volume II: Money laundering and financial crimes.* United States Department of State.

DNB (2015). *DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act: Preventing the misuse of the financial system for money laundering and terrorist financing purposes and controlling integrity risks*.

DNB/Betaalvereniging Nederland (2019). *Betalen aan de kassa 2018.*

DNB (2019). *Wat is een trustdienst?* Factsheet 2 januari 2019. Referentie 01277 www.toezicht.dnb.nl/2/50-226561.jsp.

Duyne, P. van, Harvey, J., Gelemerova, L. (2018). *The critical handbook of money laundering: Policy, analysis and myths.* Londen: Palgrave Macmillan.

ECB (2017). *The use of cash by households in the euro area.*

Europese Commissie (2019a). *Supranational risk assessment of the money laundering and terrorist financing risks affecting the EU*. Brussel: Europese Commissie.

Europese Commissie (2019b). *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.* Brussel: Europese Commissie.

Europol (2019). *Internet Organised Crime Threat Assessment (IOCTA).*

EMCDDA (2019). *Europees Drugsrapport 2019: Trends en ontwikkelingen*. Luxemburg: Bureau voor publicaties van de Europese Unie.

FATF (2006). *Trade Based Money Laundering.*

FATF (2012). *International standards on combating money laundering and the financing of terrorism & proliferation: The FATF Recommendations*. Parijs: FATF.
FATF (2013). *Guidance national money laundering and terrorist financing risk assessment*. Parijs: FATF.
Financial Intelligence Unit – New Zealand Police (2019). *National Money Laundering and Terrorism Financing Risk Assessment.* Wellington: FIU.
FIU-Nederland (2019). *Jaarverslag 2018.* Zoetermeer: FIU-Nederland
Hamilton, A., & Hammer, C. (2018). *Can we measure the power of the grabbing hand? A comparative analysis of different indicators of corruption.* Washington (DC): World Bank Group. Policy Research Working Paper 8299.
Hong Kong Special Administrative Region Government (2018). *Hong Kong Money Laundering And Terrorist Financing Risk Assessment Report.* Hong Kong: HKSAR Government.
ISO 31000:2009 (2009a). *Risk management: Principles and guidelines.* Genève: International Organization for Standardization.
ISO/IEC 31010:2009 (2009b). *Risk management: Risk assessment techniques.* Genève: International Organization for Standardization.
Janský, P. (2019). *Effective tax rates of multinational enterprises in the EU.* A report commissioned by the Greens/EFA group in the European Parliament.
Justis (2017). *De Wet controle op rechtspersonen: Een continue controle op rechtspersonen.* Den Haag: Justis.
Kerste, M., Baarsma, B., Weda, J., Rosenboom, N., Rougoor, W., & Risseeuw, P. (2013). *Uit de schaduw van het bankwezen: Feiten en cijfers over bijzondere financiële instellingen en het schaduwbankwezen*. Amsterdam: SEO Economisch Onderzoek.
KLPD (2008). *Witwassen. Verslag van een onderzoek voor het Nationaal dreigingsbeeld 2008.* Zoetermeer: KLPD.
Koningsveld, J. van (2013). Money laundering – 'You don't see it until you understand it': rethinking the stages of the money laundering process to make enforcement more effective. In B. Unger & D. van der Linde (red.), *Research handbook on money laundering* (pp. 435-451). Cheltenham: Edward Elgar.
Koningsveld, T.J. van (2015). De offshore vennootschap: Het ideale verhullingsinstrument voor de witwasser? *Justitiële verkenningen, 41*(1), 54-68.
Koningsveld, J. van (2016). Compliance & offshorewereld: 'Je ziet het pas als je het doorhebt'. De risico's van transacties met offshore-vennootschappen. *De Compliance Officer*, maart 2016, 18-21.
Kroon, M. (1992). *Effects of accountability on groupthink and intergroup relations: Laboratory and field studies*. Proefschrift Rijksuniversiteit Utrecht. Amsterdam: Thesis Publishers.
Kruisbergen, E.W., Bunt, H.G. van de, Kleemans, E.R., Kouwenberg, R.F., Huisman, K., Meerts, C.A., & Jong, D. de (2012). *Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit.* Den Haag: Boom Lemma. Onderzoek en beleid 306.
Lees, F.P. (1980). *Loss Prevention in the Process Industries.* London: Butterworth-Heinemann.
Le Gouvernement du Grand-Duché de Luxembourg – Ministère des Finances (2018). *National risk assessment of money laundering and terrorist financing.*
Lejour, A. (2020). *De last van onbelaste winsten: Belastingontwijking in en door Nederland.* Oratie Tilburg University, 7 februari 2020.
Mijnhardt, W. (2010). A tradition of tolerance, In E. Besamusca & J. Verheul (red.), *Discovering the Dutch: On culture and society of the Netherlands.* Amsterdam: Amsterdam University Press.

Ministerie van Infrastructuur en Milieu (2015). *Ons Water in Nederland: Nieuw Nationaal Waterplan 2016-2021.* Den Haag: Ministerie van Infrastructuur en Milieu.
Ministers van Financiën en Justitie en Veiligheid (2019). *Plan van aanpak witwassen*. *Juni 2019*.
Ministeries van Financiën en Justitie en Veiligheid (2020). *Voortgang plan van aanpak witwassen.* Kamerbrief 14 januari 2020.
National Commissioner of the Icelandic Police (2019). *National Risk Assessment Money Laundering and Terrorist Financing 2019.* Reykjavik: NCIP.
Organisatie voor Economische Samenwerking en Ontwikkeling (2019). *Corporate Tax Statistics* (eerste druk). Parijs: OESO.
Rijksoverheid (2019). *Miljoenennota 2020.*
Rooijendijk, L. (2019). Troika Laundromat: Nederlandse banken betrokken bij Russische witwasoperatie. *Transparancy International Nederland,* 5 maart 2019.
Slot, B., & Swart, L. de (2018). *Monitor anti-witwasbeleid 2014-2016.* Rotterdam: Ecorys.
Soudijn, M., & Akse, Th. (2012). *Witwassen Criminaliteitsbeeldanalyse 2012.* Driebergen: KLPD.
Soudijn, M. (2017). *Witwassen. Criminaliteitsbeeldanalyse 2016*.
The Swedish Companies Registration Office, the Swedish National Council for Crime Prevention, the Swedish Economic Crime Authority, the Swedish Estate Agents Inspectorate, Swedish Financial Supervisory Authority, the Swedish Enforcement Authority, the County Administrative Board of Skåne, the County Administrative Board of Stockholm, the County Administrative Board of Västra Götaland, the Swedish Police Authority, the Swedish Inspectorate of Auditors, the Swedish Tax Agency, the Swedish Gambling Authority, the Swedish Bar Association, the Swedish Security Service, Swedish Customs, and the Swedish Prosecution Authority (2019). *National Risk Assessment of Money Laundering and Terrorist Financing in Sweden 2019.*
Unger, B., Ferwerda, J., Trouw, J., Nelen, H., & Ritzen, L. (2010). *Detecting criminal investments in the Dutch real estate sector*. Studie voor de ministeries van Financiën, Justitie en BZK.
Unger, B., Ferwerda, J., Koetsier, I., Gjoleka, B., Saase, A. van, Slot, B., & Swart, L. de (2018). *Aard en omvang van criminele bestedingen: Eindrapportage.* Utrecht/Rotterdam: Universiteit Utrecht, Ecorys, Vrije Universiteit Amsterdam.
US Department of the Treasury – Office of Terrorist Financing and Financial Crimes (2018). *National Money Laundering Risk Assessment 2018*. Washington (DC): US Department of the Treasury.
Veen, H.C.J. van der, & Ferwerda, J. (2016). *Verkenning methoden en data National Risk Assessment Witwassen en Terrorismefinanciering*. Den Haag: WODC. Cahier 2016-12.
Veen, H.C.J. van der, & Heuts, L.F. (2017a). *National Risk Assessment Witwassen*. Den Haag: WODC. Cahier 2017-13.
Veen, H.C.J. van der, & Heuts, L.F. (2017b). *National Risk Assessment Terrorismefinanciering*. Den Haag: WODC. Cahier 2017-14.
Veen, H.C.J. van der, & Heuts, L.F. (2018). *National Risk Assessment Witwassen en Terrorismefinanciering Bonaire, Sint Eustatius en Saba*. Den Haag: WODC. Cahier 2018-17.
World Economic Forum (2019). *Global Competitiveness Report 2019*. Genève: World Economic Forum.
World Trade Organization (2019). *World trade Statistical Review 2019.* Genève: World Trade Organization.

Zanden, J.L. van (2010). The Economy of the Polder. In E. Besamusca & J. Verheul (red.), *Discovering the Dutch: On culture and society of the Netherlands*. Amsterdam: Amsterdam University Press.

Websites

https://www.accountant.nl/nieuws/2020/2/explosie-aantal-witwaszaken-is-betrekkelijk/
https://aci.aero/news/2019/03/13/preliminary-world-airport-traffic-rankings-released/.
https://coinmarketcap.com/charts/
https://ec.europa.eu/eurostat/web/population-demography-migration-projections/data/main-tables
https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals/nl#Internettoegang.
https://hollandquaestor.nl.
https://icov.nl/.
https://lloydslist.maritimeintelligence.informa.com/one-hundred-container-ports-2019/.
https://ondernemersplein.kvk.nl/overzicht-rechtsvormen/
https://opendata.cbs.nl/statline/#/CBS/nl/.
https://statistiek.dnb.nl/downloads/index.aspx#/?kindofproduct=mainproduct.
https://stats.oecd.org/index.aspx?DataSetCode=PDB_LV#.
https://wetten.overheid.nl/BWBR0014656/2018-05-01.
www.amsadvocaten.nl/woordenboek/ondernemingsrecht/trust/.
www.banken.nl/bankensector/bankensector-nederland.
www.banken.nl/nieuws/21731/ranglijst-grootste-nederlandse-banken-2019.
www.cia.gov/library/publications/the-world-factbook/geos/nl.html.
www.ebf.eu/the-netherlands/.
www.europa-nu.nl/id/vh1alz099lwi/schengen_en_visabeleid.
www.europa-nu.nl/id/vh7dosyo6lu1/europese_economische_ruimte_eer.
www.fatf-gafi.org.
www.fatf-gafi.org/faq/moneylaundering/.
www.fec-partners.nl.
www.fiod.nl/3-aanhoudingen-witwasonderzoek-nieuwkuijk/.
www.cbs.nl/nl-nl/dossier/dossier-asiel-migratie-en-integratie/hoeveel-mensen-met-een-migratieachtergrond-wonen-in-nederland-
www.cbs.nl/nl-nl/nieuws/2018/50/80-procent-inkomende-investeringen-direct-doorgesluisd.
www.cbs.nl/nl-nl/nieuws/2019/45/hoogste-exportverdiensten-dankzij-machines.
www.cbs.nl/nl-nl/visualisaties/dashboard-arbeidsmarkt/banen-werkgelegenheid/toelichtingen/werkgelegenheidsstructuur.
www.cn.dnb.nl/nl/toezicht/toezicht_geldtransactiekantoren/markttoegang#geldtransactiekantoor.
www.consilium.europa.eu/nl/press/press-releases/2018/10/02/controls-on-cash-entering-and-leaving-the-eu-council-adopts-regulation/#.
www.dnb.nl/toezichtprofessioneel/openbaar-register/WTTTK/index.jsp?filter_value=&naam=Statutaire+naam+%2F+Handelsnaam.
www.emcdda.europa.eu/system/files/publications/11347/netherlands-cdr-2019.pdf.
www.kvk.nl/download/SchemaRechtsvormen_tcm109-389297.pdf.
www.nrc.nl/nieuws/2019/01/21/nederland-is-een-fiscaal-paradijs-a3651183.
www.nvb.nl/nieuws/nederlandse-banken-bundelen-krachten-tegen-witwassen/.

www.rand.org/topics/delphi-method.html.
www.weforum.org/agenda/2019/11/netherlands-dutch-farming-agriculture-sustainable/.
www.toezicht.dnb.nl/2/50-226561.jsp.
www.toezicht.dnb.nl/2/50-237939.jsp.
www.topsectoren.nl/.
www.transparency.org/cpi2018.
www.weforum.org/agenda/2019/11/netherlands-dutch-farming-agriculture-sustainable

Cases

https://magazines.openbaarministerie.nl/inzicht/2019/03/ondergronds-bankieren.
https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHAMS:2015:3979.
Trouw, 5 maart 2019: 'De Russische witwasmachine loopt ook door Nederland'.
www.fiod.nl/fiod-en-om-halen-witwasmachine-voor-cryptovaluta-offline/.
www.fiod.nl/gezamenlijk-onderzoek-fiod-en-britse-hmrc-naar-verhuld-vermogen-in-buitenland/.
www.fiod.nl/3-aanhoudingen-witwasonderzoek-nieuwkuijk/.
www.fiu-nederland.nl/nl/wetgeving/witwastypologieen/virtuele-betaalmiddelen.
www.om.nl/actueel/nieuws/2018/09/04/ing-betaalt-775-miljoen-vanwege-ernstige-nalatigheden-bij-voorkomen-witwassen
www.om.nl/actueel/nieuws/2020/01/16/katvangers-inzetten-om-42-miljoen-euro-te-verhullen.
www.om.nl/actueel/nieuws/2018/02/08/celstraf-en-werkstraffen-geeist-voor-witwassen-met-horlogehandel.
www.om.nl/actueel/nieuws/2019/10/08/om-eist-celstraffen-en-een-ton-ontneming-voor-illegale-bitcoin-wisselingen.
www.om.nl/actueel/nieuws/2018/02/20/om-eist-5-jaar-tegen-witwassende-bitcoin-handelaar.
www.om.nl/actueel/nieuws/2018/04/18/om-eist-dat-twee-veroordeelde-mannen-ruim-8.500.000-betalen-aan-staat.
www.om.nl/actueel/nieuws/2019/02/12/om-eist-in-hoger-beroep-tot-8-jaar-cel-voor-oplichting-en-hypotheekfraude-in-den-haag.
www.om.nl/actueel/nieuws/2019/09/03/trustkantoor-vistra-betaalt-35-ton-voor-niet-melden-ongebruikelijke-transacties.
www.om.nl/actueel/nieuws/2019/09/13/administratie-geld-valse-merktelefoons-in-beslag-bij-grootschalige-zoekingen-bedrijventerrein.
www.om.nl/actueel/nieuws/2019/07/17/aardappel--en-uienhandel-vatbaar-voor-witwaspraktijken.
www.recht.nl/rechtspraak/uitspraak/?ecli=ECLI:NL:RBOVE:2018:421.

Sources for international laws and regulations

Title	Abbreviation	References
Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU	Fourth EU Anti-Money Laundering Directive	OJEU 2018, L 156/43
Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006	Wire Transfer Regulation 2 (WTR2)	OJEU 2015, L 141/1
Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls of cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005	European Cash Control Regulation	OJEU 2018, L 284/6

Sources for national laws and regulations

Title	Abbreviation	Source*
Money Laundering and Terrorist Financing Prevention Act	Wwft	Bulletin of Acts and Decrees 2019, 342
Financial Supervision Act	Wft	Bulletin of Acts and Decrees 2020, 19
Penal Code	WvSr	Bulletin of Acts and Decrees 2019, 507
Code of Criminal Procedure	WvSv	Bulletin of Acts and Decrees 2019, 507
Trust and Company Service Providers (Supervision) Act 2018	Wtt 2018	Bulletin of Acts and Decrees 2018, 464
Public Administration Probity Screening Act	Wet Bibob	Bulletin of Acts and Decrees 2018, 248
Legal Entities (Supervision) Act	-	Bulletin of Acts and Decrees 2018, 312
Commercial Register Act 2007	-	Bulletin of Acts and Decrees 2019, 450
Economic Offences Act	WED	Bulletin of Acts and Decrees 2020, 93

* The source relates to the entry into effect of the most recent amendment of the Act in question.

Appendix 1 Composition of the Scientific Advisory Committee

Chair

Prof W.F.M. Bams	Maastricht University, School of Business and Economics

Members

J. van der Knoop Phd	Decision Support
T.J. van Koningsveld Phd	Offshore Kenniscentrum
C.S. van Nassau MSc	Research and Documentation Centre
D. Weggemans MSc	Leiden University, Institute for Security and Global Affairs
M. Wesseling Phd	WES Consulting
Z. Zuidema LLM MA	Ministry of Justice and Security, Law Enforcement and Crime Fighting Department

Appendix 2 List of interviewed experts

To preserve the anonymity of the respondents, this list only indicates the names of the organisations where the respondents were employed. The table shows how many employees were interviewed in each organisation.

Table B2.1 Exploratory interviews for the quantitative data analysis

Organisation	Number of interviewees
Dutch Authority for the Financial Markets	1 employee
Financial Supervision Office	2 employees
Wwft Monitoring Office	2 employees
De Nederlandsche Bank	3 employees
Customs Service	2 employees
Financial Intelligence Unit – the Netherlands	2 employees
Netherlands Gambling Authority	2 employees
iCOV	3 employees
Public Prosecution Service	2 employees

Table B2.2 In-depth interviews

Organisation	Number of interviewees
ABN-AMRO	4 employees
Anti-Money Laundering Centre	2 employees
Dutch Authority for the Financial Markets	3 employees
Tax and Customs Administration	2 employees
Financial Supervision Office	2 employees
Wwft Monitoring Office	2 employees
Corpag (on behalf of Holland Quaestor)	1 employee
De Nederlandsche Bank	2 employees
Customs Service	1 employee
Europol	2 employees
Financial Expertise Centre (FEC)	2 employees
Financial Intelligence Unit – the Netherlands	2 employees
ING	2 employees
Justis, Ministry of Justice and Security	2 employees
Chamber of Commerce	1 employee
Royal Dutch Association of Civil-Law Notaries	2 employees
Netherlands Police	1 employee
Dutch Association of Real Estate Brokers and Valuers	2 employees
Public Prosecution Service	1 employee
Rabobank	1 employee
De Volksbank	2 employees

Table B2.3 Validating interviews

Organisation	Number of interviewees
Anti-Money Laundering Centre	1 employee
Financial Intelligence Unit – the Netherlands	2 employees
ING	2 employees
Ministry of Finance	2 employees
Ministry of Justice and Security	2 employees
Public Prosecution Service	1 employee

Appendix 3 List of participants at the expert meetings

To preserve the anonymity of the participants, this list gives only the names of the organisations in which the participants were employed. In most cases, the same representative of an organisation participated in the three expert meetings. But since this was not always the case, a distinction has been made between 'Employee I' and 'Employee II'.

Table B3.1 Participants at the three expert meetings

Organisation	First expert meeting	Second expert meeting	Third expert meeting
Anti-Money Laundering Centre	Employee I	Employee I	Employee I
Dutch Authority for the Financial Markets	Employee I	Employee I	Employee I
Financial Supervision Office	Employee I	Employee I	Employee I
Wwft Monitoring Office	Employee I	Employee I	Employee I
Corpag (on behalf of Holland Quaestor)	Employee I	*Did not participate, although invited*	Employee I
De Nederlandsche Bank	Employee I	Employee II	Employee II
Customs Service	Employee I	Employee I	Employee II
Financial Intelligence Unit – the Netherlands	Employee I	*Did not participate, although invited*	Employee I
ING	Employee I	Employee I	*Did not participate, although invited*
Netherlands Gambling Authority	Employee I	Employee II	Employee II
Royal Netherlands Military and Border Police	Employee I	Employee I	Employee I
Royal Dutch Association of Civil-Law Notaries	Employee I	Employee I	Employee I
Netherlands Police	Employee I	Employee II	Employee II
Netherlands Institute of Chartered Accountants	Employee I	Employee I	Employee I
Netherlands Bar Association	Employee I	Employee I	*Did not participate, although invited*
Dutch Money Transfer Association	Employee I	Employee I	*Did not participate, although invited*
Dutch Association of Real Estate Brokers and Valuers	Employee I	Employee I	Employee I
Public Prosecution Service	Employee I	Employee I	Employee II

Appendix 4 Money laundering threats in FLUU Survey

The text and tables below were sent to expert organisations via email.

Longlist of money laundering threats
Via this email survey, we want to find out whether your organisation is aware of the offences or cases relating to the threats and to what extent your organisation considers the prevalence of the threats likely or not (based on the information available within your organisation). This will be done based on the so-called FLUU system. You are requested to indicate one of the following letters for the money laundering threats on the longlist:

- *An 'F' if, according to you, this threat is present and one or more offences or cases relating to the threat are known to your organisation*
- *An 'L' if, according to you, it is likely that this threat is present but no factual offences or cases are known to your organisation*
- *A 'U' if, according to you, it is unlikely that the threat is present, based on the information available to your organisation*
- *A 'U' if it is unknown to you whether or not the threat is present because your organisation has no information regarding this*

Please mark the appropriate box (F, L, U, U) in the table to indicate your choice (for example, with a cross). You need to do this for each threat in the table. If you do not do this for a specific threat, we will interpret this as a 'U' (Unknown) during the analysis.

Placement channels (incl. selection of placement methods)	F	L	U	U
1. Licensed banks: wire transfers	…	…	…	…
2. Licensed banks: cash transactions/deposits	…	…	…	…
3. Unlicensed banks (underground banking): wire transfers	…	…	…	…
4. Unlicensed banks (underground banking): cash transactions/deposits	…	…	…	…
5. Licensed payment service providers: wire transfers	…	…	…	…
6. Licensed payment service providers: cash transactions/deposits	…	…	…	…
7. Unlicensed payment service providers: wire transfers	…	…	…	…
8. Unlicensed payment service providers: cash transactions/deposits	…	…	…	…
9. Trust offices	…	…	…	…
10. Accountants	…	…	…	…
11. Civil-law notaries	…	…	…	…
12. Lawyers	…	…	…	…
13. Insurers	…	…	…	…
14. Estate agents	…	…	…	…
15. Gambling (casinos, online gambling and/or lotteries)	…	…	…	…
16. Dealers of high-value goods (cars, jewellery, art, etc.)	…	…	…	…
17. Investment firms/institutions	…	…	…	…
18. Tax consultants	…	…	…	…

Other placement methods	F	L	U	U
19. Crypto currencies	…	…	…	…
20. Payment cards (prepaid cards, telephone cards, etc.)	…	…	…	…

Concealment methods	F	L	U	U
21. Investment schemes (including loan-back arrangements and ABC transactions)	…	…	…	…
22. Complex legal entities and structures (including offshore companies, trust schemes and legal entities such as foundations)	…	…	…	…
23. Trade-based structures (including legitimation of value transfer via commercial transactions and over-invoicing/under-invoicing)	…	…	…	…
24. Corporate structures (including the incorporation of one's own company and holding participating interests in other companies)	…	…	…	…
25. Use of straw men	…	…	…	…

Channels and/or methods not mentioned (to be filled in by respondent, max. 3)	F	L	U	U
…	…	…	…	…
…	…	…	…	…
…	…	…	…	…

Appendix 5 Email survey on policy instruments

How do the existing policy instruments contribute to preventing/combating money laundering?	No or limited contribution	Reasonable contribution	Significant contribution	Unable to estimate extent of contribution	Unfamiliar with policy instrument
EU Anti-Money Laundering Directive	…	…	…	…	…
European Cash Control Regulation	…	…	…	…	…
Wire Transfer Regulation 2	…	…	…	…	…
Money Laundering and Terrorist Financing Prevention Act	…	…	…	…	…
Financial Supervision Act	…	…	…	…	…
Trust and Company Service Providers (Supervision) Act 2018	…	…	…	…	…
Legal Entities (Supervision) Act	…	…	…	…	…
Penal Code	…	…	…	…	…
Code of Criminal Procedure	…	…	…	…	…
Civil Code	…	…	…	…	…
Commercial Register Act 2007	…	…	…	…	…
Telecom Act	…	…	…	…	…
Tax legislation	…	…	…	…	…
Social legislation	…	…	…	…	…
Sectoral regulations	…	…	…	…	…
Public Administration Probity Screening Act	…	…	…	…	…
General banking terms and conditions	…	…	…	…	…
Incident referral protocol (EVA Register)	…	…	…	…	…

What are the policy instruments that are missing from the above list? How do they contribute to preventing/combating money laundering?	No or limited contribution	Reasonable contribution	Significant contribution	Unable to estimate contribution
1…	…	…	…	…
2…	…	…	…	…
3…	…	…	…	…
4…	…	…	…	…
5…	…	…	…	…

What policy instruments that do not currently exist could make a major contribution to prevent/combating money laundering? Please explain your answer.
1…
2…
3…

Appendix 6 Results of the expert meetings

First expert meeting

Table B6.1 Threats with the greatest potential impact (based on the first round of identification)

Threats	Number of experts
Complex legal entities and structures (including offshore companies, trust schemes and legal entities such as foundations)	16
Trust offices	15
Licensed banks: wire transfers	13
Underground banking/physical movement of money	10
Use of straw men	10
Trade-based structures (including the legitimation of value transfers via commercial transactions and over-invoicing/under-invoicing)	10
Investment schemes (including loan-back arrangements and ABC transactions)	10
Dealers of high-value goods (cars, jewellery, art, etc.) and other dealers	9
Corporate structures (including the incorporation of one's own company and holding participating interests in other companies)	8
Unlicensed payment service providers: cash transactions/deposits	8
Correspondent banking en intermediary banking	7
Crypto currencies	7
Licensed banks: cash transactions/deposits	7
Licensed banks: cash transactions/deposits	7
Licensed payment service providers: cash transactions/deposits	6
Licensed payment service providers: wire transfers	6
Unlicensed payment service providers: wire transfers	5
Investment firms/institutions	4
Civil-law notaries	4
Unlicensed banks: wire transfers	4
Payment cards (prepaid cards, telephone cards, etc.)	3
Lawyers	3
Gambling (casinos, online gambling and/or lotteries)	2
Estate agents	2
Accountants	2
Currency exchange	1
Tax consultants	1
Insurers	0

Table B6.2 The 10 threats with the greatest potential impact (based on the second and final round of identification)

Threats	Number of experts
Complex legal entities and structures (including offshore companies, trust schemes and legal entities such as foundations)	18
Trade-based structures (including the legitimation of value transfers via commercial transactions and over-invoicing/under-invoicing)	16
Use of straw men	16
Correspondent banking en intermediary banking	15
Investment schemes (including loan-back arrangements and ABC transactions)	15
Crypto currencies	14
Dealers of high-value goods (cars, jewellery, art, etc.) and other dealers	13
Underground banking/physical movement of money	13
Corporate structures (including the incorporation of one's own company and holding participating interests in other companies).	12
Licensed banks: wire transfers	12

Second expert meeting

Table B6.3 Average potential impact per money laundering threat* (based on the first round of assessment)

Threats	Level of potential impact (Scale of 0-100)							Number of experts
	A	B	C	D	E	F	Total	
Money laundering via wire transfers by licensed banks	73.0	63.0	65.7	71.0	46.7	75.3	66.5	15
Money laundering via structures by trust offices	63.2	57.1	56.4	65.4	35.4	79.3	60.2	14
Money laundering via offshore companies	56.7	59.7	54.7	65.0	35.3	78.0	58.9	15
Money laundering via dealers of high-value services/goods	58.9	63.6	63.6	64.3	46.4	52.5	58.6	14
Money laundering via legal entities	57.0	63.3	54.3	63.0	46.3	61.0	57.9	15
Money laundering via services	56.8	60.0	55.4	61.8	43.2	61.8	56.9	14
Money laundering via the use of intermediaries	51.5	55.0	56.2	66.5	47.7	56.9	56.0	13
Money laundering via investment institutions/firms	59.6	57.5	54.6	56.4	42.5	62.1	55.9	14
Money laundering via goods	52.0	61.0	57.0	59.3	43.0	60.0	55.7	15
Money laundering via ABC transactions	54.7	58.0	54.0	62.0	42.3	54.4	54.7	15
Money laundering via loan-back arrangements	58.3	57.7	55.7	55.7	38.3	53.7	53.7	15
Money laundering via crypto currencies	55.4	51.8	53.6	53.2	46.8	53.2	52.5	14
Money laundering via fictitious company turnover	50.3	55.7	53.3	59.0	43.3	47.0	51.8	15
Money laundering via underground banking	47.9	47.9	49.6	58.2	44.6	52.5	50.4	14
Money laundering via physical movement of cash	39.6	39.6	42.5	49.3	43.2	44.3	43.2	14

* Here, A to F stands for the MCA criteria. A: Deterioration in the stability of the financial system, B: Damage to the regular economy, C: Disruption of the social order, D: Undermining of authority and the legal order, E: Reduction of subjective/objective security, F: Damage to the image of the Netherlands abroad

Table B6.4 Average potential impact per money laundering threat* (based on the second and final round of assessment)

Threats	Level of potential impact (Scale of 0-100)							Number of experts
	A	B	C	D	E	F	Total	
Money laundering via wire transfers by licensed banks	73.0	62.9	65.2	70.3	45.7	75.2	66.1	15
Money laundering via structures by trust offices	56.7	55.5	52.8	63.0	34.3	76.9	57.2	15
Money laundering via offshore companies	54.7	59.2	53.5	62.3	33.3	76.2	57.2	15
Money laundering via legal entities	55.7	62.2	53.1	62.3	44.0	60.5	56.7	15
Money laundering via dealers of high-value services/goods	55.0	60.6	59.8	62.5	43.2	50.9	55.8	14
Money laundering via services	54.6	58.8	54.1	59.3	41.1	60.6	55.2	14
Money laundering via the use of intermediaries	49.6	54.5	51.3	65.8	46.9	54.1	54.0	13
Money laundering via investment institutions/firms	56.8	55.6	52.6	55.0	40.4	60.9	54.0	14
Money laundering via goods	50.0	58.9	53.8	56.7	38.0	58.2	53.0	15
Money laundering via ABC transactions	52.3	56.5	51.1	60.7	39.3	53.2	53.0	15
Money laundering via loan-back arrangements	54.0	55.9	52.1	54.7	37.0	52.5	51.5	15
Money laundering via fictitious company turnover	51.7	55.5	52.5	58.7	40.3	45.9	51.2	15
Money laundering via crypto currencies	49.7	51.5	49.8	54.0	46.0	51.9	50.6	15
Money laundering via underground banking	46.4	44.9	49.1	56.8	44.3	50.5	48.9	14
Money laundering via physical movement of cash	36.7	34.9	40.1	46.3	38.7	40.5	39.6	15

* Here, A to F stands for the MCA criteria. A: Deterioration in the stability of the financial system, B: Damage to the regular economy, C: Disruption of the social order, D: Undermining of authority and the legal order, E: Reduction of subjective/objective security, F: Damage to the image of the Netherlands abroad

Third expert meeting

Table B6.5 Resilience of total set of policy instruments per money laundering threat (based on the first round of assessment)

Threats	Level of resilience (On a scale of 0 to 100)	Distribution	Number of Experts
Money laundering via wire transfers by licensed banks	62.5	19.5	15
Money laundering via structures by trust offices	57.4	21.3	15
Money laundering via ABC transactions	56.9	20.4	14
Money laundering via the use of intermediaries	50.8	19.2	14
Money laundering via investment institutions/firms	49.5	21.3	10
Money laundering via fictitious company turnover	49.3	19.2	13
Money laundering via legal entities	48.5	19.2	14
Money laundering via loan-back arrangements	43.8	20.9	12
Money laundering via services	38.8	24.1	11
Money laundering via dealers of high-value services/goods	38.6	22.1	14
Money laundering via physical movement of cash	37.3	18.1	13
Money laundering via offshore companies	37.0	19.9	13
Money laundering via goods	35.1	23.2	14
Money laundering via underground banking	24.9	18.2	14
Money laundering via crypto currencies	23.9	18.4	14
Average for the 15 greatest money laundering threats	43.8	23.3	

Table B6.6 Resilience of total set of policy instruments per money laundering threat (based on the second and final round of assessment)

Threats	Level of resilience (On a scale of 0 to 100)	Distribution	Number of Experts
Money laundering via wire transfers by licensed banks	64.1	16.5	15
Money laundering via structures by trust offices	51.6	20.6	15
Money laundering via investment institutions/firms	51.4	17.1	11
Money laundering via fictitious company turnover	48.1	17.3	14
Money laundering via legal entities	44.4	18.0	14
Money laundering via ABC transactions	44.1	16.2	14
Money laundering via loan-back arrangements	43.3	21.6	12
Money laundering via the use of intermediaries	43.6	17.2	14
Money laundering via dealers of high-value services/goods	34.6	17.8	14
Money laundering via goods	33.4	17.5	15
Money laundering via offshore companies	32.5	15.3	13
Money laundering via physical movement of cash	29.9	12.0	14
Money laundering via services	27.7	16.2	13
Money laundering via crypto currencies	20.1	11.8	14
Money laundering via underground banking	18.9	9.8	15
Average for the 15 greatest money laundering threats	39.1	20.6	

Table B6.7 Residual Potential Impact of the greatest money laundering risks in the Netherlands

Risks	Residual Potential Impact (On a scale of 0 to 100)
Money laundering via crypto currencies	40.4
Money laundering via services	39.9
Money laundering via underground banking	39.6
Money laundering via offshore companies	38.6
Money laundering via dealers of high-value services/goods	36.5
Money laundering via goods	35.3
Money laundering via legal entities	31.5
Money laundering via the use of intermediaries	30.5
Money laundering via ABC transactions	29.4
Money laundering via loan-back arrangements	29.2
Money laundering via physical movement of cash	27.8
Money laundering via structures by trust offices	27.7
Money laundering via fictitious company turnover	26.6
Money laundering via investment institutions/firms	26.2
Money laundering via wire transfers by licensed banks	23.7

Appendix 7 Quantitative data analysis

Collaboration with iCOV

iCOV is a partnership that produces reports or develops other information products solely for the benefit of the cooperating government partners. This means that iCOV operates in an entirely demand-driven manner. The collaborating partners prepare data for their own use or for use by the partners and give instructions for the preparation of reports under strict legal conditions. The legal basis of iCOV lies in the specific laws and regulations applicable to each party in the partnership.

In addition to processing personal data for the preparation of an iCOV product, such data are also processed within the partnership in the context of R&D activities. Various forms of research take place as part of these R&D activities, both scientific research as well as research with a view to the development of new products or the further development of existing products. For example, it may need to be investigated whether a particular result from scientific research can be included in an iCOV product. Scientific research at iCOV must be compatible with its objectives. The R&D objectives are set out in the iCOV Research and Development Data Processing Protocol 2018 (*Protocol gegevensverwerking iCOV Research and Development 2018*) that is published in the Government Gazette.[176]

In view of the social importance of gaining a proper understanding of the risks in the field of money laundering, iCOV has decided to enter into cooperation with the WODC in the context of a quantitative data analysis for the Money Laundering NRA. The scope of the study is in line with the objectives of iCOV. It has been agreed that the WODC bears ultimate responsibility for the project and the content of the results and conclusions. iCOV plays a facilitating role in requesting, compiling and preparing the data needed by the WODC for answering their research questions. Datasets are delivered anonymously for further analysis.

Research structure
At the first expert meeting for this NRA, representatives of the expert organisations identified the money laundering threats with the greatest potential impact. After the expert meeting, in-depth interviews were held with experts to discuss the precise nature and mechanisms of the identified threats, which resulted in a more detailed description of the threats. After consultation between iCOV and the WODC about the identified money laundering threats, it emerged that the specific threats of money laundering via ABC transactions, money laundering via loan-back arrangements and money laundering via legal entities were best suited for a quantitative data analysis, given the available data sources. The assumption was that it would be possible to provide some insight into the prevalence of the aforementioned money laundering threats by compiling and analysing a number of data files concerning these threats based on the data available at iCOV. The key question in the quantitative data analysis for the threats is: how do you prove that the threat is related to money laundering? For this, each construct was first elaborated in greater detail:

176 See: https://zoek.officielebekendmakingen.nl/stcrt-2019-11305.pdf.

Money laundering via ABC transactions involving real estate
An ABC transaction is a series of two or more transactions within a certain period of time with unexplained differences in value. Usually a period of 186 days is set as a maximum because of the exemption from transfer tax. Since the value differences cannot be properly traced from the land registry data, all transactions corresponding to this period are designated as ABC transactions. An ABC transaction may be used by traders to inflate prices in order to launder money. Slum landlords make use of the ABC transaction to conceal profits made from the sale of real estate. However, it should be noted that ABC transactions are not used exclusively for real estate money laundering. ABC transactions are not considered illegal as long as the transactions are transparent and in line with the law. Properties are bundled and sold together (one sale price) in order to disguise and drive up the price for an individual piece of property. These are known as 'baskets of properties'.[177]

An ABC transaction may be used to disguise the origin of criminal assets and legitimise the means by which the money was earned. But an ABC transaction in itself need not be suspicious or have anything to do with money laundering. What makes an ABC transaction potentially suspicious?
- Concealment of the identity of natural persons through the use of legal entities.
- Concealment of the selling price through the use of baskets of properties.
- Earlier involvement in financial and economic crime.

Money laundering via legal entities and malicious foundations
The concealment of liability and assets via structures of legal entities is often referred to in the relevant literature as a method used for money laundering. This was also often mentioned in the in-depth interviews. In this respect, any information contained in the data sources can be accessed via iCOV. Foreign legal entities such as offshore companies do not appear in iCOV data. However, it is possible to examine legal entities that are directors of another legal entity, even if this director is established abroad. What makes the use of legal entities potentially suspicious?
- Concealment of liability and assets through the use of non-transparent structures involving legal entities.
- Changes in the management board of legal entities.
- Earlier involvement in financial and economic crime.

Money laundering via loan-back arrangements involving real estate
The loan-back arrangement is a loan to yourself, usually by using a network of legal entities, so that the origin of the loan and the actual UBO are disguised.[178] A loan-back arrangement has the following features:
- A person lends his black money to himself.
- For this, he uses a network of legal entities.
- He is actually doing transactions with himsel.f
- He is also giving himself a mortgage.
- The legal entities make use of unregistered shareholders or bearer shares, an option that is available to NVs in the Netherlands.
- Foreign trusts and company service providers (offshore companies) are used.
- The mortgagee is a foreign legal entity.
- The legal entity is a non-business party.
- The legal entity is an unauthorised mortgage lender, according to DNB.
- The mortgagee is a company with unregistered shareholders.

177 Unger et al. (2010).

178 Unger et al. (2010).

The available data makes it possible to verify only a part of the total scenario:
- The mortgagee is an unauthorised legal entity.
- Country of establishment of the mortgagee.
- Indication of low income (on reference date).

To translate the above into measurable characteristics, iCOV, in consultation with the WODC, has developed a provisional structure for the data files to be provided. The structures started by taking a broad look at the scope of a characteristic, i.e. they looked at the entire source (the entire population) and then broke down these characteristics further based on elements of concealment and earlier involvement in financial and economic crime. All the characteristics are not equally distinctive in nature. If a certain combination of characteristics indicative of money laundering occurs proportionately as often in the entire population as in the research group (composed based on the distinguishing characteristics), it means that this set of characteristics may not be distinctive enough. In-depth interviews with experts showed that the age of natural persons could be a distinguishing characteristic. This is why, where possible, natural persons have been broken down into age categories.

Despite the fact that only three money laundering risks were supposed to be considered, the concrete translation, via characteristics and indicators, into quantitative standards resulted in a large-scale request for data. Based on the data available at the WODC and iCOV, an attempt was made to select the most promising money laundering risks for determining the quantitative substantiation. Subsequently, when developing the structures of the data sets to be analysed, an attempt was made to determine only the indicators possibly associated with the risks. For the three money laundering risks, a draft set of characteristics corresponding to the risks was formulated. Characteristics that can be derived from the data were translated into measurable constructs. The expected significance of these constructs cannot be determined in advance due to insufficient insight into the prevalence figures. Moreover, it was not always possible to substantiate the choice of parameters with insights from literature or from practice. This is inherent to the exploratory nature of the quantitative data analysis. The guiding principle was to substantiate, link with relevant literature and practical experience where possible, and use no more data than necessary.

The planned quantitative data analysis was expected to be emphatically exploratory in nature. Before performing the analysis, it is not clear to what extent the data allows one to look ahead and establish links in a way that produces reliable results. iCOV guarantees reliability through meaningful links, a substantiation of the structure of the data file and development of the search query. In order to compile the data files, choices have to be made regarding a considerable number of parameters such as research period/reference date, categories for classifying the indicators, type of legal entity and age category of the natural person. These choices were made prior to the study as much as possible, which means that they were made without insight into quantitative criteria. The resulting data files were intended to be delivered by iCOV in the form of tables with aggregated, and therefore anonymous, figures. Further analyses of the files would be carried out on location at iCOV by the WODC.

Collaboration with Justis

In addition to iCOV, organisations with a public-law task in the field of fraud prevention may also contact Justis' TRACK department for information in connection with a criminal, administrative or tax investigation of a legal or natural person.[179] As part of its task relating to the supervision of legal entities, TRACK provides information from the Commercial Register of the Chamber of Commerce. For individual risk reports or for identifying the networks surrounding a specific legal person, TRACK may also add criminal and tax data to the data from the Chamber of Commerce. The legal basis for this is laid down in the Legal Entities (Supervision) Act and the Legal Entities (Supervision) Decree. However, these do not contain any provisions for more large-scale processing of criminal and tax data for operational purposes or scientific research. Hence, these data are not available for the quantitative research performed as part of the NRA. Neither does TRACK have access to data from the Netherlands' Cadastre, Land Registry and Mapping Agency (*Kadaster*). This means that only data from the Commercial Register can be used for compiling the aggregated data sets as described in our research proposal.

After an exploratory interview with Justis employees, and once the Minister of Justice and Security had granted its permission for the provision of data in the form of aggregated tables, the WODC initiated discussions with TRACK data specialists. The purpose of this discussion was to determine the money laundering risks included in the research proposal for which quantitative inputs could be provided via TRACK. This revealed that the available data from the Chamber of Commerce could be used for quantifying context-related information, concealment elements and the prevalence of specific and possibly suspicious circumstances relating to money laundering for the risk of money laundering via legal entities. The following characteristics were specifically examined:

- Number of legal persons incorporated in 2015 and 2017 broken down by type of legal entity.
- Number of directors of the incorporated legal entities, broken down into natural and non-natural persons and further broken down by country of residence/business location.
- Number of directors involved in multiple establishments in the periods 2015-2019 and 2017-2019 broken down into natural and non-natural persons and further broken down by country of residence/business location.
- Number of establishments per director in the period 2015-2019 and 2017-2019 broken down into natural and non-natural persons.

179 For more information about the differences between investigations for operational purposes at iCOV and at Justis/TRACK, see https://www.justis.nl/binaries/WEB_122911_FS_Track_ICOV_tcm34-415584.pdf.