



Wetenschappelijk Onderzoek- en
Datacentrum

Cahier 2024-1

Dutch National Risk Assessment on Money Laundering 2023

Summary

Cahier 2024-1

Dutch National Risk Assessment on Money Laundering 2023

Summary

H.C.J. van der Veen

L.F. Heuts

Cahier

De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het Wetenschappelijk Onderzoek- en Datacentrum is verricht. Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Justitie en Veiligheid weergeeft.

Summary

Dutch National Risk Assessment on Money Laundering 2023

Background of the study

The Dutch policy for the prevention and repression of money laundering is based on the recommendations of the Financial Action Task Force (FATF) and regulations of the European Union (EU). As a member of the FATF, the Netherlands is bound by the recommendations of this intergovernmental body aimed at taking preventive and repressive measures against money laundering and terrorist financing, measures with regard to national legal systems and international cooperation. For the EU member states, most of the FATF recommendations have been converted into several successive anti-money laundering directives. Based on these directives, the EU member states must implement a risk-oriented policy against money laundering and terrorist financing and establish a National Risk Assessment (NRA). For the Netherlands, the implementation of the NRA is laid down in the Money Laundering and Terrorist Financing Prevention Act (Wwft). Article 1f paragraph 1 of the Wwft states that the Ministers of Finance and Justice and Security jointly publish a report, to be updated every two years, of the identified, analysed and assessed national risks in the areas of money laundering and terrorist financing.

The Research and Data Center (WODC) carried out a third NRA on money laundering for the European Netherlands in the period June 2022 to December 2023.¹ The risk analysis carried out for the NRA covers the period January 2020 to June 2023. The NRA has a fivefold purpose:

- 1 identifying the money laundering threats with the greatest potential impact (i.e. the greatest money laundering threats);
- 2 determining the level of potential impact of the greatest money laundering threats;
- 3 determining the level of resilience of the policy instruments for the prevention and/or repression of the greatest money laundering threats;
- 4 providing insight into the nature and mechanisms of the greatest money laundering threats; and
- 5 determining the risk level of the greatest money laundering threats by comparing the potential impact of the threats and the resilience of the policy instruments.

Research methodology

The structure of the third NRA is – as in the previous NRAs – determined by the ISO 31000 framework for risk management. The research methodology used includes the following components:

¹ Since 2017, two previous NRAs in the field of money laundering have been carried out by the WODC for the European Netherlands. In addition, two NRAs on terrorist financing have since been carried out for the European Netherlands. Two NRAs have also been carried out for the Caribbean Netherlands since 2017, relating to both money laundering and terrorist financing. Parallel to the realisation of the third NRA on money laundering, the WODC conducted the third NRA on terrorist financing (for the European Netherlands).

- A context analysis outlining the specific characteristics of the Netherlands that may influence the prevalence of money laundering and its potential impact. These factors can play a role in determining the money laundering methods to be used. For this context analysis, a literature study was conducted and relevant quantitative data sources were consulted.
- For the purpose of an inventory of money laundering threats, recent reports (published since 2020) have been studied, including the European Supra National Risk Assessment (SNRA), and the so-called FANO survey² has been conducted among public and private parties with a task in the prevention and/or combat of money laundering.
- In the first expert meeting, representatives of expert organisations identified the money laundering threats which they view as the threats having the greatest potential impact.
- After the first expert meeting, in-depth interviews were conducted with representatives of expert organisations and other parties with a role in combating money laundering to further discuss the nature, mechanisms and cases of the threats on the provisional shortlist of the greatest money laundering threats.
- In the second expert meeting – based on the findings from the interviews – the shortlist of the greatest money laundering threats was adjusted and finally established, after which the experts estimated the potential impact of the threats using a Multi Criteria Analysis (MCA).
- In the third expert meeting, experts estimated the resilience of the total package of available policy instruments for each of the greatest money laundering threats.
- By comparing the estimated potential impact of the money laundering threats with the estimated resilience, insight was gained into the risk level of the 18 greatest money laundering threats.
- Data requests have been submitted to a number of public organisations for all 18 threats and as much available quantitative data as possible as well as recent cases have been included in the report.
- In the final phase of the study, validating interviews are conducted with seven experts working at five key organisations, with the main aim of determining the extent to which they recognize the risk level of the 18 greatest money laundering threats. In addition, the correlation has been determined for the eight threats with the same scope that are included in the list of greatest threats in both the third NRA on money laundering and the third NRA on terrorist financing.

Greatest money laundering threats

From a longlist of 50 money laundering threats, relating to placement, concealment, legitimisation or integration methods, money laundering experts identified in the first expert meeting the ten threats that, in their opinion, scored highest in terms of potential impact within the Dutch context. This led to a preliminary shortlist of 15 greatest money laundering threats, which was expanded to 18 threats in the second expert meeting. The NRA focuses on this final shortlist of 18 greatest money laundering threats, which are shown categorised in Table Sum1 because the greatest threats do not vary much in terms of potential impact.

² In this online survey, respondents were asked to indicate in a longlist of threats whether they have experience with facts/cases of the threats from their own work and to what extent they consider the prevalence of the threats to be plausible or not based on of the information available at their organisation. FANO stands for Facts/case, Probable, Implausible and Unknown.

Table Sum1 Potential impact of 18 greatest money laundering threats (n=9)

Threat	Potential impact (on a scale of 0-100)
Score category '60 or more'	
Money laundering via professional service providers	67
Money laundering via wire transfers at licensed banks	60
Money laundering via trade-based constructions involving goods or services	60
Score category '55 to 59'	
Money laundering via private real estate	58
Money laundering via the purchase/sale, rental or lease of high-value products	58
Money laundering via commercial real estate	58
Money laundering via cash transactions/deposits at licensed banks	58
Money laundering via the physical movement of large amounts of cash and/or high-value products in the Netherlands or to/from abroad	57
Money laundering via less transparent Dutch legal entities	57
Money laundering via criminal underground banking or hawala banking	57
Money laundering via Payment Service Providers	56
Score category '50 to 54'	
Money laundering via providers of financial crypto services	54
Money laundering via straw men, front men or money mules	53
Money laundering via easily accessible ways to open a foreign bank account	52
Money laundering via foreign (offshore) structures	51
Money laundering via foreign bank account	51
Score category 'Less than 50'	
Money laundering via licensed money transfer organisations	49
Money laundering via splitting up trust office services	48

The threat 'money laundering via professional service providers' received by far the highest score of the 18 greatest money laundering threats, namely a potential impact score of 67 on a scale of 0 to 100. Lowest in this list of the greatest money laundering threats is 'money laundering via licensed money transfer organisations' and 'money laundering via splitting up trust office services' (in both cases a score of slightly lower than 50). The table above makes it clear that the potential impact of the vast majority of the 18 greatest money laundering threats does not differ greatly from each other (after all, the scores are often between 50 and 60).

The money laundering threats are aimed at placing criminal cash in the legal money circuit, integrating criminal money into the financial system, concealing the manner in which the criminal money is placed or integrated and/or the identity of the criminal who places or integrates the money, and/or giving the criminal money an appearance of legitimacy. These threats can – in various combinations of two or more threats – form a money laundering construction. A money laundering construction can be quite

simple in nature (for example, the use of a money mule who moves large amounts of cash abroad), but can also be very complex in nature (for example, the purchase of private real estate by a straw man involving both offshore structures and less transparent Dutch legal entities).

A previous study shows that in 2014, drugs and fraud together were responsible for more than 90 percent of the money laundering needs in the Netherlands. The fact that drugs and fraud appear to be the most important preceding form of crime is supported by data from the Annual Review of the Financial Intelligence Unit of the Netherlands (FIU-the Netherlands): most suspicious transaction reports relate to these two forms of crime. In general, it can also be stated that drug crime involves more use of cash than financial fraud. This may indicate that money laundering threats in which cash is placed or moved in the legal circuit mainly involve drug money.

Resilience of the policy instruments

The available policy instruments to prevent and combat money laundering include all relevant instruments arising from international and national legislation and regulations, legislation and regulations at a municipal level, sectoral and industry-oriented regulations, and regulations at an organisational level. This NRA also views partnerships between public and/or private organisations and guidelines, guidances and policy plans of organisations that play a role in the prevention and/or combat of money laundering as a policy instrument. Table Sum2 provides an overview of the policy instruments that were available until June 2023 - the month in which the third expert meeting took place - to prevent and combat money laundering.

Table Sum2 Policy instruments to prevent and combat money laundering

International laws and regulations	National laws and regulations	Other policy instruments
<ul style="list-style-type: none"> • FATF recommendations • EU anti-money laundering directives • European regulation on declaration of liquid assets • Wire Transfer Regulation 2 	<ul style="list-style-type: none"> • Money Laundering and Terrorist Financing Prevention Act³ • Financial Supervision Act • Penal Code • Code of Criminal Procedure • Sanctions Act 1977 • Trust and Company Service Providers (Supervision) Act 2018 • General Customs Act • Legal Entities Supervision Act • Trade Register Act 2007 (including UBO-registers) • Tax legislation • Economic Offenses Act • Public Administration Probity Screening Act 	<ul style="list-style-type: none"> • National partnerships • International partnerships • Sectoral regulations and conditions • Guidelines, guidances and policy plans

³ In the Netherlands, the Money Laundering and Terrorist Financing Prevention Act (Wwft) requires a large number of institutions to report Unusual Transactions to the Financial Intelligence Unit - the Netherlands.

For the 18 greatest threats, in the third expert meeting money laundering experts assessed the extent to which the total package of existing policy instruments counters the potential impact of the threats. The results of the expert meeting are shown categorised in table Sum3. In their assessment of the resilience of the policy instruments, experts based their assessment on the policy instruments that had been implemented at that time (June 2023).

For two money laundering threats, the experts judge that the resilience of the policy instruments counters the potential impact by 60% or more, namely 'money laundering via cash transactions/deposits at licensed banks' (score 64) and 'money laundering via wire transfers at licensed banks' (score 60). The four money laundering threats with the lowest resilience score all have an international character: money laundering via foreign bank account (score 31), via foreign (offshore) structures (score 26), via criminal underground banking or hawala banking (score 26) and via easily accessible ways to open a foreign bank account (score 20). The low scores therefore mean that the total package of policy instruments – according to experts – only counteract these money laundering threats to a relatively limited extent. Table Sum3 shows that the resilience of the policy instruments can differ greatly between the 18 greatest money laundering threats (the scores are between 20 and 64).

Despite the mitigating effect of the available instruments on the 18 greatest money laundering threats, the threats can still have a greater or lesser degree of impact. The mitigating effect is related to the extent to which the AIO principle⁴ applies to the money laundering threats. With most money laundering methods one or more of the three AIO components apply. The more the AIO elements apply to money laundering threats, the lower the resilience of the policy instruments for preventing and repressing the threats.

⁴ AIO stands for 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).

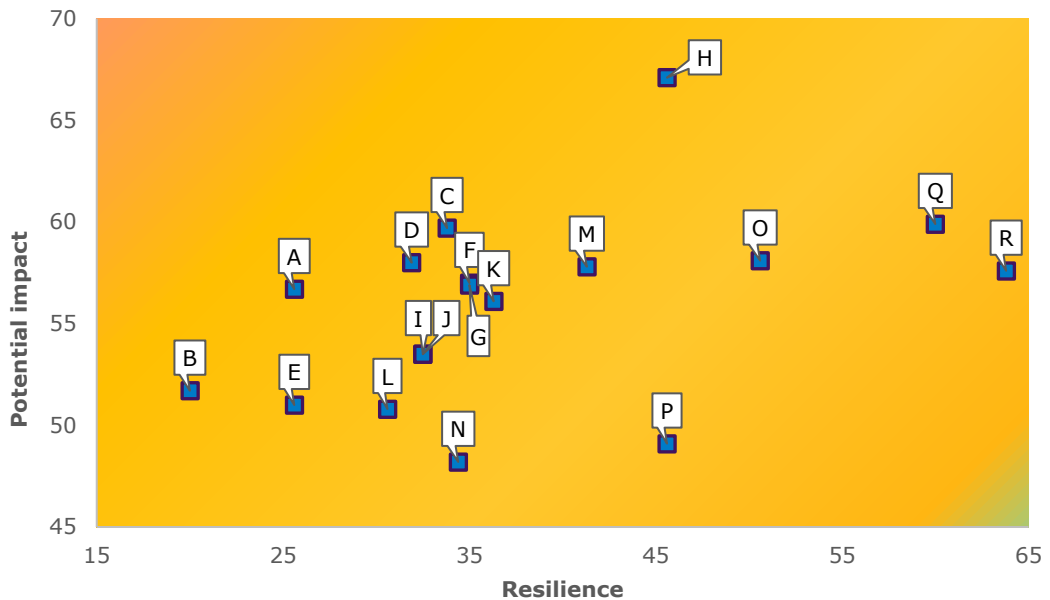
Table Sum3 Resilience of policy instruments per greatest money laundering threat (n=9)

Threat	Resilience (on a scale of 0-100)
Score category '60 or more'	
Money laundering via cash transactions/deposits at licensed banks	64
Money laundering via wire transfers at licensed banks	60
Score category '50 to 59'	
Money laundering via private real estate	51
Score category '40 to 49'	
Money laundering via professional service providers	46
Money laundering via licensed money transfer organisations	46
Money laundering via commercial real estate	41
Score category '30 to 39'	
Money laundering via Payment Service Providers	36
Money laundering via the physical movement of large amounts of cash and/or high-value products in the Netherlands or to/from abroad	35
Money laundering via less transparent Dutch legal entities	35
Money laundering via splitting up trust office services	34
Money laundering via trade-based constructions involving goods or services	34
Money laundering via providers of financial crypto services	33
Money laundering via straw men, front men or money mules	33
Money laundering via the purchase/sale, rental or lease of high-value products	32
Money laundering via foreign bank account	31
Score category '20 to 29'	
Money laundering via foreign (offshore) structures	26
Money laundering via criminal underground banking or hawala banking	26
Money laundering via easily accessible ways to open a foreign bank account	20

Risk level of greatest money laundering threats

In Figure Sum1, a heat map compares the expert estimates of the potential impact and resilience of the policy instruments for the 18 greatest money laundering threats. The highest risks are threats with a high potential impact and low resilience of the available policy instruments. This heatmap can be seen as a summary of the third NRA on money laundering. However, it must be taken into account that the heatmap only shows the greatest money laundering threats and that the other threats from the longlist, that are also part of the NRA, are seen by the experts as moderate risks.

Figure Sum1 Heatmap third NRA: potential impact compared to resilience to the greatest money laundering threats^a



A	Criminal underground banking or hawala banking	J	Straw men, front men or money mules
B	Easily accessible ways to open a foreign bank account	K	Payment Service Providers
C	Trade-based constructions with goods or services	L	Foreign bank account
D	Purchase/sale, rental or lease of high-value products	M	Commercial real estate
E	Foreign (offshore) structures	N	Splitting up trust office services
F	Physical movement of large amounts of cash and/or high-value products	O	Private real estate
G	Less transparent Dutch legal entities	P	Licensed money transfer organisations
H	Professional service providers	Q	Wire transfers at licensed banks
I	Financial crypto service providers	R	Cash transactions/deposits at licensed banks

^a To illustrate the differences as clearly as possible, the figure shown is a cut-out from a figure with axes ranging from 0 to 100, where the colors run from top left: red (highest potential impact and lowest resilience) to bottom right: green (lowest potential impact and highest resilience). The figure with the axes ranging from 0 to 100 can be found in Appendix 8.

The figure shows that the risk level of the 18 greatest money laundering threats does not differ significantly from each other. This applies in particular to the potential impact scores, which range from 48 to 67. The resilience to the threats shows a greater spread. All threats are in the orange area in the figure. Of all these high-risk money laundering threats, the following five threats have the highest risk level (shown at the top left of the figure):

- *Money laundering via criminal underground banking or hawala banking (A in Figure Sum1)*. This money laundering threat has such a high risk level mainly due to a low estimated resilience. According to the AIO principle the threat offers opportunities to transfer money anonymously, has an international character and is often deployed via and/or abroad, and concerns an unregulated 'sector'. Furthermore,

this money laundering method is relatively easily accessible to criminals who want to launder their illegally obtained money.

- *Money laundering via easily accessible ways to open a foreign bank account (B)* . With this money laundering threat, the high risk level is mainly caused by a very low estimated resilience. This is related to the fact that some digital foreign bank accounts can be opened relatively easily by criminals – with, depending on the country, possibly less strict money laundering regulations and supervision with regard to financial service providers – and that there are currently no policy instruments to counter this. Once the criminal has a foreign bank account, he or she can conduct transactions to, through or from this account, which are hard to monitor by Dutch banks and are less transparent to investigative authorities, which therefore have a less good information position.
- *Money laundering via trade-based constructions involving goods or services (C)*. With this money laundering threat, the high level of risk is related to the fact that the various methods that fall under Trade-Based Money Laundering (TBML) and Service-Based Money Laundering (SBML) are non-transparent in nature and that they often have an international character. This money laundering threat is therefore less insightful for Dutch investigative authorities.
- *Money laundering via the purchase/sale, rent/rental or lease of high-value products (D)*. The high risk level of this money laundering threat is caused by the fact that it offers many different ways to place or integrate criminal cash into the legal money circuit (for the benefit of one's own use of the high-value products). The fact that the rental and so-called operational lease of high-value products, as is often the case with leasing cars, do not fall under the Wwft and the supervision by the Wwft Monitoring Office (BTWwft) also contributes to the high risk level of the threat.
- *Money laundering via professional service providers (H)*. With this money laundering threat, the high risk level is caused by the very high estimated potential impact of the threat. This high estimate is because professional service providers play a pivotal role in many money laundering methods. Their conscious or unconscious involvement makes it possible, for example, to purchase a home with criminal money or to set up a foundation.

Of the 18 greatest money laundering threats, the least high risk level lies with the three money laundering threats located furthest at the (bottom) right of the figure: 'money laundering via licensed money transfer organisations' (P), 'money laundering via wire transfers at licensed banks' (Q) and 'money laundering via cash transactions/deposits at licensed banks' (R). Although these threats still involve a significant level of risk, their risk level is estimated to be relatively the lowest. This is mainly due to the highly estimated resilience, which can be related to the improvement of customer due diligence and transaction monitoring by both licensed banks and licensed money transfer organisations in recent years.

Het Wetenschappelijk Onderzoek-
en Datacentrum (WODC) is het
kennisinstituut voor de rechtsstaat.
Het WODC doet zelf onafhankelijk
wetenschappelijk onderzoek of laat
dit doen door erkende instituten en
universiteiten, ter ondersteuning
van beleid en uitvoering.

Meer informatie:

www.wodc.nl