

# **Financial Crime Threat Assessment of The Netherlands 2023-24**

Nederlandse Vereniging van Banken

March 2024

# Contents

---

1	Management summary	3
2	Introduction	4
3	Methodology Financial Crime Threat Assessment The Netherlands 2023-24	7
4	Profile Dutch financial crime landscape	10
5	Compiled list of Financial Crime threats in The Netherlands	13
6	Financial Crime Threat Assessment of The Netherlands 2023-24	15
7	Appendices	40



# 1. Management summary

In co-creation with the financial sector and public parties, NVB developed a Financial Crime Threat Assessment of The Netherlands 2023-24. This assessment provides an overview of current, relevant Financial Crime threats in The Netherlands.



## Context & scope

### Background

- The Dutch Banking Association (*hereinafter: NVB*) aims to fulfil the need for increased alignment and collaboration on Dutch-specific financial crime risks as actionable input for the individual risk management processes of banks (such as the Systematic Integrity Risk Assessment, *hereinafter SIRA*).

### Objective

- The Financial Crime Threat Assessment of The Netherlands 2023-24 provides an overview of current, relevant financial crime threats in The Netherlands.
- This initial assessment will be the starting point for the Financial Crime Threat Assessment for banks, which can be used as input for the individual risk management processes of financial crime of banks in The Netherlands.
- To contribute to gatekeeper effectiveness, the strategic objective of the Financial Crime Threat Assessment for banks is to engage in dialogue with the public sector regarding the extent to which banks are impacted by threats and whether these are identifiable by banks.



## Methodology

### Enriching publicly available information with expert input

- **Document review and expert opinions:** publicly available information was complemented with expert input (from public and private parties) during multiple deep dive sessions.
- **Overview of 88 NL financial crime threats:** all information was assessed by quantitative and qualitative analysis and led to a compiled list of 88 financial crime threats for The Netherlands.
- **20 threats selected:** 20 threats were selected for elaboration at this stage, based on relevance, volume, and extent.

### Limitations

- This document is based on existing, publicly available information and expert input. It has not been developed following a scientific approach, nor is it aiming for a scientific substantiation of results.
- This process aims to provide a thorough understanding of the financial crime landscape in The Netherlands. The defined situation is subject to continuous change and therefore serves as a snapshot of the current situation in Q4 2023.



## Results

### Selected threats

- The following financial crime threats are selected for elaboration in this assessment. A baseline description, modus operandi, extent of the threat in The Netherlands - linked to the characteristics of The Netherlands - are provided on:
  - Arms trafficking
  - Bribery
  - Concealment of beneficial ownership
  - Concealment of identity
  - Drugs economy
  - Environmental crime
  - Extremism
  - Fragmentation of payment landscape
  - Market facilitators
  - Modern slavery
  - Organised crime at transport hubs
  - Payment fraud
  - Public funding fraud
  - Sanctions evasion
  - State actors
  - Tax evasion
  - Terrorism financing
  - Trade-based money laundering
  - Underground banking
  - Value Added Taxes (*hereinafter: VAT*) fraud

*Note: This document is part I/III and is extended with a financial crime threat assessment for banks (II) and a risk scenario library, based on consolidated SIRA input (III).*

## 2. Introduction

The NVB developed a Financial Crime Threat Assessment of The Netherlands 2023-24 to have an overview of the current, relevant financial crime threats in The Netherlands

### Background

- ▶ The fight against financial crime by banks in The Netherlands took a notable shift in 2023 with the ‘risk-based roundtables’, initiated by the Dutch Central Bank (*hereinafter: DNB*). These roundtables have led to more discussion and dialogue within the sector on applying a risk-based approach in fulfilling the gatekeeper role of the banks. This has resulted in documentation (industry baselines) aimed at enhancing the proportionality and risk relevancy of activities that banks perform as gatekeeper within the financial sector. The roundtables and industry baselines demonstrated a promise of a collective achievement in further refining the risk-based approach in a public-private partnership.
- ▶ Therefore, the NVB aims to fulfil the need of banks for more concrete guidelines and collaboration on risks as input for the individual risk management processes of banks in The Netherlands. This will allow banks to effectively and efficiently implement Anti-Money Laundering (*hereinafter: AML*) and/or Combating Financing of Terrorism (*hereinafter: CFT*) controls to collectively disrupt illegal financial flows. More concrete guidelines will lead to targeted deployment of capabilities and capacity where needed most and reduce undesirable consequences where these could, and therefore should, be avoided. Sectoral expertise is essential to further align on high-risk financial crime threats for banks, which necessitate (additional) adequate measures, as well as identifying low-risk areas to effectively manage targeted risks. This can potentially assist banks to select certain threats, thereby allocate their capacity in a most effective manner, which ultimately contributes to their societal role in combating crime.
- ▶ Therefore, NVB and five participating banks have decided to develop a joint Financial Crime Threat Assessment for banks. In order to create this Financial Crime Threat Assessment for banks, it was essential to start with researching, collecting and summarizing relevant available sources of information in a Financial Crime Threat Assessment of The Netherlands 2023-24.
- ▶ In fulfilling their gatekeeper role, banks acknowledge the often complex task of identifying the underlying modus operandi from financial crime related transactions. Given this challenge, unusual transactions that are identified, are being reported to the FIU. By participating in this initiative, banks anticipate that their risk management processes may potentially improve, thereby enhancing their capability to effectively report unusual transactions. Consequently, this approach serves to strengthen the sector’s AML/CFT controls, to support banks in exploring the possibilities to identify threats and underscores the importance of the gatekeeping role of banks for society.

## 2. Introduction

In scope are financial crime threats for financial institutions which are subject to the Wwft and the Sanctions Law

### Strategic objective

- ▶ The Financial Crime Threat Assessment of The Netherlands 2023-24 should be seen as an overview of the current, relevant financial crime threats in The Netherlands and will be input for the Financial Crime Threat Assessment for banks.
- ▶ The strategic objective of the Financial Crime Threat Assessment for banks is to engage in dialogue with the public sector regarding the extent to which banks are impacted by threats and whether these threats are identifiable by banks.
- ▶ The outcome of the Financial Crime Threat Assessment for banks should provide actionable information to banks as input for their individual risk management processes and will point them to the threats where more focus could be required.
- ▶ This document is part I/III and is extended with a financial crime threat assessment for banks (II) and a risk scenario library, based on consolidated SIRA input (III). The purpose of this document is to provide information for banks in their role as gatekeeper and as input for their individual risk management processes, such as risk assessments. This document cannot be used for other purposes.

### Scope

- ▶ Financial crime refers to illegal acts committed by an individual or a group of individuals to obtain a financial or professional advantage (Definition Europol, EMPACT 2022+).
- ▶ In scope of this Financial Crime Threat Assessment of The Netherlands 2023-24 are all financial crime threats for financial institutions which are subject to the Wet ter voorkoming van witwassen en financieren van terrorisme (*hereinafter: Wwft*) and the Sanctions Law.
- ▶ In terms of geographical scope, it has been agreed that the assessment focuses on threats manifesting in The Netherlands, which implies that these threats can also carry an international aspect.
- ▶ The scope includes threats that apply to both natural persons and business entities.

# 2. Introduction

This document contains the methodology, an overview of the Dutch financial crime landscape, a compiled list of financial crime threats in The Netherlands, the Financial Crime Threat Assessment of The Netherlands 2023-24 and appendices



### Chapter 3.

#### Methodology of the Financial Crime Threat Assessment of The Netherlands 2023-24

This section details the methodology and definitions used in the Financial Crime Threat Assessment of The Netherlands 2023-24. It explains the steps undertaken during the process, elaborates on the definitions applied, and discusses the limitations of this approach.



### Chapter 4.

#### Dutch financial crime landscape

This section contains a detailed analysis of characteristics of The Netherlands as a country which are relevant for the financial crime threat landscape. It outlines 18 distinct characteristics grouped into 7 overarching features.



### Chapter 5.

#### Compiled list of financial crime threats in The Netherlands

This section contains a comprehensive list of 88 potential threats, ascertained from publicly available sources and expert input gathered through workshops with both private and public parties.



### Chapter 6.

#### Financial Crime Threat Assessment of The Netherlands 2023-24

This section contains 20 financial crime threats, selected by the experts. Each threat is complemented with a description, the characteristics aligned with The Netherlands, and the general modus operandi. This information should be understood as a broad description of the financial crime threats in The Netherlands.



### Chapter 7.

#### Appendices

The appendix includes an overview of the sources used for identifying threats and elaborating them.



# 3. Methodology of the Financial Crime Threat Assessment of The Netherlands 2023-24



# 3. Methodology Financial Crime Threat Assessment of The Netherlands 2023-24

This assessment is documented based on publicly available information, complemented with expert input during workshops with public and private parties. This led to 20 threats to elaborate extensively on in this assessment

- This assessment is documented based on publicly available information, complemented with expert input during workshops with public and private parties.
- The selected publicly available information is based on industry practices of financial crime related institutions (e.g. Europol, FATF and EBA), open-source intelligence and expert input. The total overview of sources can be found in appendix I and II.
- Two types of experts were involved in the workshops: banking experts (Core Team, including five participating banks, NVB and public sector experts. The participating banks experts are delegates from: Rabobank, ING, ABN AMRO, de Volksbank and Triodos. The public sector experts involve experts from the Financial Intelligence Unit (*hereinafter: FIU*), Fiscal Intelligence and Investigation Service (*hereinafter: FIOD*) and The Netherlands Police (*hereinafter: Police*).
- The workshops were characterised by a constructive and productive exchange of information, with valuable interaction and the consolidation of results. This approach, involving public sector- and banking experts collaborating in workshops, has proven to be a useful method. We would like to express our appreciation to all parties involved who have invested their time and effort into this collaboration.
- The publicly available information and expert input was recorded in a database on which quantitative analysis and qualitative analysis took place in Q4 2023 to assess and cluster the threats, this led to a compiled list of 88 threats (see chapter 5).
- Each expert group was asked to select a Top 10 of most important threats to discuss in further detail. Result of this exercise is a selection of 20 threats to elaborate extensively on in this assessment. Additionally, 11 clusters of threats were assembled to cover the complete results of the desk research and workshops (see chapter 6).
- Based on desk research and expert input, the threats were linked to the characteristics of The Netherlands to describe the country's vulnerabilities. Additionally, the extent of the threat in The Netherlands is included to provide information for further selection of threats.
- It should be noted that threats that have been deep dived during workshops for the Financial Crime Threat Assessment for banks present a more detailed level of modus operandi due to the extensive expert input.



# 3. Methodology Financial Crime Threat Assessment of The Netherlands 2023-24

A common understanding of the following definitions within this Financial Crime Threat Assessment of The Netherlands 2023-24 is essential: threat, risk, scenario and modus operandi

## Limitations

- This document has not been developed using a scientific approach, nor is it aiming for a scientific substantiation of results; it is built on existing, publicly available information and expert input. It should not be seen as stand-alone guidance to prioritise threats within a bank.
- This process aims to provide a thorough understanding of the financial crime landscape in The Netherlands. However, the defined situation is subject to continuous change and therefore serves as a snapshot of the current situation in Q4 2023.
- At the start of this assessment, it had become clear that the nature of the various threats is different; modus operandi, predicate offences, risk indicators etc. became part of the compiled list of financial crime threats in The Netherlands. Therefore, the list consisted of threats with different abstraction levels. However, the project group decided that despite these differences and the resulting difficulties of comparison, the compiled list of threats is a comprehensive initial representation of the current financial crime threats in The Netherlands.
- The threats in this assessment are selected by the involved private and public parties' experts based on their experience and subject matter knowledge. The selection of threats included in this assessment is based on the current relevance of the threats in Q4 2023. The characteristics and modus operandi of the threats outlined in this document are therefore not exhaustive, but a reflection of the desk research and expert input in Q4 2023.

## Definitions in the Financial Crime Threat Assessment of The Netherlands 2023-24

- Threat is a potential danger, hazard, or harm that can exploit vulnerabilities and negatively impact a system, organisation, or individual. It represents a source of potential damage or loss.
- Risk refers to the likelihood of a threat exploiting vulnerabilities and the resulting impact it may have. It involves assessing the potential consequences of a threat and the likelihood of it occurring.
- Scenario is a detailed description of a possible sequence of events, often related to a specific threat or risk. Scenarios help in understanding and preparing for potential situations and are used in various risk assessments.
- Modus operandi is a Latin term that translates to "mode of operation". In the context of criminal activities, it refers to the specific methods, techniques, or procedures that individuals or groups use to carry out their illegal actions.

# 4. Profile Dutch financial crime landscape

Relevant financial crime characteristics of The Netherlands



## 4. Profile Dutch financial crime landscape

Seven overarching features describe the characteristics of The Netherlands: international trade centre, geographic location, international financial hub, technology & digital environment, social & cultural environment, political environment and maturity of industries

To develop the Financial Crime Threat Assessment of The Netherlands 2023-24, it was crucial to establish a thorough and accurate profile of The Netherlands as a country. This profile serves as a foundational element in gaining an understanding of The Netherlands, both as an individual entity and as a participant in the global financial ecosystem.

Distinct characteristics of The Netherlands that shape its financial crime threat landscape are outlined in the National Risk Assessment Witwassen 2019 (*hereinafter: NRA*). This comprehensive document is a product of the Scientific Research and Data Center (*hereinafter: WODC*). The WODC's NRA provides an in-depth review of the features unique to the country.

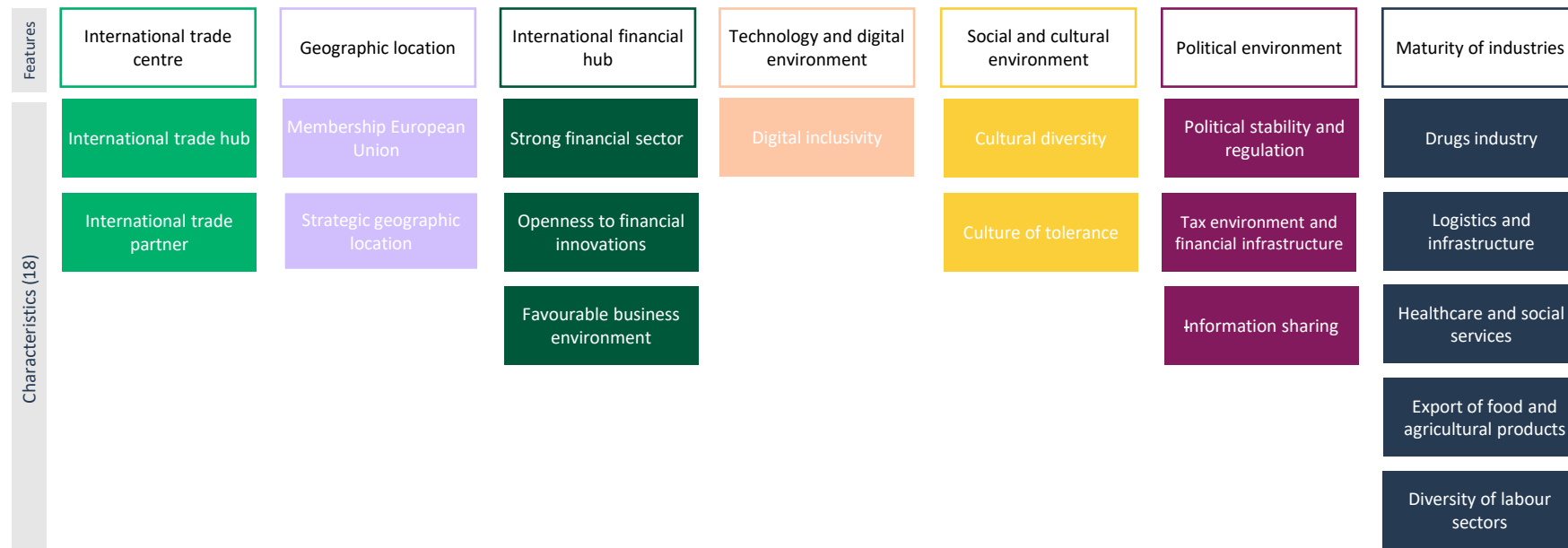
Therefore, using the NRA as a basis, 18 characteristics of the Dutch financial crime landscape were identified. These characteristics have been clustered into 7 overarching features to create a comprehensive profile of The Netherlands:

- **International trade centre** - The Netherlands, with one of the highest gross domestic product (GDP) and competitive economies, serves as an international trade centre, making it a critical component of the Dutch financial crime landscape. This robust trade environment can attract financial crime due to the high volume of trade and widespread international ties.
- **Geographic location** - The Netherlands' strategic geographic location, bordered by the EU, with easy access to Schengen zone countries and the Caribbean, as well as its extensive sea and river transport hubs, makes it a hotspot in the financial crime landscape. These characteristics facilitate easier movement of goods and funds, which can be exploited for illicit activities.
- **International financial hub** - As an international financial hub, The Netherlands hosts numerous internationally active banks that drive the rapid adoption of new payment methods, contributing to its financial crime landscape. This ever-evolving financial environment can potentially be exploited for illicit activities due to the speed and global reach of transactions.
- **Technology and digital environment** - The Netherlands' advanced technology and digital environment, highlighted by its status as the country with the highest number of households with internet access, makes it an influential part of the Dutch financial crime landscape. This high level of digital connectivity can be exploited for a.o. cybercrimes and online financial fraud.
- **Social and cultural environment** - In The Netherlands, a social and cultural environment marked by polarisation, tolerance, and consensus-based decision-making could inadvertently complicate preventing financial crimes by providing cover for illicit activities.
- **Political environment** - The Dutch political environment, marked by consensus-based decision-making, fiscal attractiveness and a reliable judicial system, contributes to the financial crime landscape. Additionally, the Dutch tax environment includes certain legal provisions and tax regulations, such as bilateral international tax agreements which are unique for The Netherlands.
- **Maturity of industries** - The maturity of Dutch industries, including dominant production, import, and export sectors, is a key feature of the country's financial crime landscape. These well-established industries provide significant financial flows that could be attractive for criminals, and targeted for illicit activities such as money laundering or fraud.

# 4. Dutch financial crime landscape

Relevant characteristics of The Netherlands regarding financial crime

The 20 threats described in this Financial Crime Assessment of The Netherlands (chapter 6) are linked to the following 18 characteristics of the Dutch financial crime landscape:



# 5. Compiled list of Financial Crime threats in The Netherlands



# 5. Compiled list of financial crime threats in The Netherlands

Quantitative and qualitative analysis of information from desk research and expert input during workshops led to an initial compiled list of 88 financial crime threats, presented in clusters based on how close they are associated with each other

This list is a comprehensive initial representation of the current financial crime threats in The Netherlands and therefore not exhaustive (please find additional information in chapter 3. Methodology)

- |  |   |  |  |
|--|---|--|--|
| <ul style="list-style-type: none"><li><input type="checkbox"/> Alternative value transfer commodities (e.g. oil, gold and grain)</li><li><input type="checkbox"/> Bribery and corruption*</li><li><input type="checkbox"/> At sea- and airports / customs work</li><li><input type="checkbox"/> Conflict of interest</li><li><input type="checkbox"/> Cash-intensive businesses</li><li><input type="checkbox"/> Gambling services</li><li><input type="checkbox"/> Money service business</li><li><input type="checkbox"/> NPOs and NGOs</li><li><input type="checkbox"/> Automotive industry (car sales, export/import, carwash)</li><li><input type="checkbox"/> Jewelry store</li><li><input type="checkbox"/> Retail (designer products)</li><li><input type="checkbox"/> Sex workers</li><li><input type="checkbox"/> High value goods (including art)</li><li><input type="checkbox"/> Concealment of beneficial ownership*</li><li><input type="checkbox"/> Offshore companies</li><li><input type="checkbox"/> Service provider companies</li><li><input type="checkbox"/> Trust offices</li><li><input type="checkbox"/> Shell companies</li><li><input type="checkbox"/> Concealment of identity*</li><li><input type="checkbox"/> Cybercrime</li><li><input type="checkbox"/> Ransomware</li><li><input type="checkbox"/> Identity theft</li></ul> | <ul style="list-style-type: none"><li><input type="checkbox"/> Hacktivism</li><li><input type="checkbox"/> Darknet</li><li><input type="checkbox"/> Business e-mail compromise</li><li><input type="checkbox"/> Cyber-attacks</li><li><input type="checkbox"/> Spread of misinformation and propaganda</li><li><input type="checkbox"/> Theft (digital technologies)</li><li><input type="checkbox"/> Child pornography</li><li><input type="checkbox"/> Environmental crime*</li><li><input type="checkbox"/> Manure fraud</li><li><input type="checkbox"/> Soil, water or air pollution</li><li><input type="checkbox"/> Oil fraud</li><li><input type="checkbox"/> Substances of very high concern</li><li><input type="checkbox"/> Waste crimes</li><li><input type="checkbox"/> Trade in illegal plant protection products</li><li><input type="checkbox"/> Product quality fraud</li><li><input type="checkbox"/> Greenwashing</li><li><input type="checkbox"/> Fragmentation of payment landscape*</li><li><input type="checkbox"/> Payment service providers</li><li><input type="checkbox"/> Virtual IBANs</li><li><input type="checkbox"/> Money transfers</li><li><input type="checkbox"/> Virtual asset solutions (crypto / NFTs)</li><li><input type="checkbox"/> Fraud</li><li><input type="checkbox"/> Subsidy / public funding fraud*</li><li><input type="checkbox"/> Investment fraud</li><li><input type="checkbox"/> Systematic fraud</li></ul> | <ul style="list-style-type: none"><li><input type="checkbox"/> Payment fraud*</li><li><input type="checkbox"/> Bankruptcy fraud</li><li><input type="checkbox"/> Emission rights fraud</li><li><input type="checkbox"/> High-risk industries</li><li><input type="checkbox"/> Real estate</li><li><input type="checkbox"/> Professional services</li><li><input type="checkbox"/> Online marketplaces</li><li><input type="checkbox"/> Illegal smuggling and trade</li><li><input type="checkbox"/> Arms trafficking*</li><li><input type="checkbox"/> Human trafficking / smuggling</li><li><input type="checkbox"/> Counterfeit goods</li><li><input type="checkbox"/> Endangered plant species and wildlife</li><li><input type="checkbox"/> Drugs economy*</li><li><input type="checkbox"/> Cash smuggling</li><li><input type="checkbox"/> Market facilitators (other gatekeepers)*</li><li><input type="checkbox"/> Modern slavery*</li><li><input type="checkbox"/> Human exploitation</li><li><input type="checkbox"/> Money laundering</li><li><input type="checkbox"/> Trade-based money laundering*</li><li><input type="checkbox"/> Service-based money laundering</li><li><input type="checkbox"/> Trade in cash</li><li><input type="checkbox"/> Money mules</li></ul> | <ul style="list-style-type: none"><li><input type="checkbox"/> Non-compliance with regulations</li><li><input type="checkbox"/> Organised crime</li><li><input type="checkbox"/> In sea- and airports (transport hubs)*</li><li><input type="checkbox"/> The crime-as-a-service business</li><li><input type="checkbox"/> Currency counterfeiting</li><li><input type="checkbox"/> Threats to national security</li><li><input type="checkbox"/> Infiltration of legitimate supply chains</li><li><input type="checkbox"/> Sanction evasion*</li><li><input type="checkbox"/> State actors*</li><li><input type="checkbox"/> Tax evasion*</li><li><input type="checkbox"/> Free trade zones</li><li><input type="checkbox"/> Dividend stripping</li><li><input type="checkbox"/> Conduit companies</li><li><input type="checkbox"/> VAT fraud*</li><li><input type="checkbox"/> Terrorism financing*</li><li><input type="checkbox"/> Extremism* (combined with subversive crime)</li><li><input type="checkbox"/> Trading without permits (e.g. asset management)</li><li><input type="checkbox"/> Underground banking*</li><li><input type="checkbox"/> Third-party payments</li></ul> |
|--|---|--|--|

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24



# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Overview of 20 selected financial crime threats

- The publicly available information and expert input on the financial crime threats in The Netherlands was recorded in a database on which quantitative and qualitative analysis was performed to assess and cluster threats, which led to the compiled list of 88 threats (see chapter 5).
- During the workshops, expert groups selected a Top 10 threats, relevant to refine in further detail for this financial crime assessment.
- Drivers for this initial selection were:
  - expected extent of the threat for The Netherlands (volume and vulnerability)
  - societal impact (what is potentially low in volume, but could have major impact on society)
  - relevance for the financial sector (involvement in certain threats). This includes threats that were deemed to be highly relevant, such as sanction evasion, as well as those considered less relevant, such as extremism
  - new or recent threats, following innovation in payment landscape or societal and geopolitical trends
- Result of this exercise is an initial selection of 20 threats, selected for more extensive elaboration (in alphabetical order):
  - ▶ Arms trafficking
  - ▶ Bribery
  - ▶ Concealment of beneficial ownership
  - ▶ Concealment of identity
  - ▶ Drugs economy
  - ▶ Environmental crime
  - ▶ Extremism
  - ▶ Fragmentation of payment landscape
  - ▶ Market facilitators
  - ▶ Modern slavery
  - ▶ Organised crime in transport hubs
  - ▶ Payment fraud
  - ▶ Public funding fraud
  - ▶ Sanction evasion
  - ▶ State actors
  - ▶ Tax evasion
  - ▶ Terrorism financing
  - ▶ Trade-based money laundering
  - ▶ Underground banking
  - ▶ VAT fraud
- On the following pages, these threats are complemented with a description of the threat, the linked characteristics of The Netherlands, the modus operandi and the extent of the threat in The Netherlands.



# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Arms trafficking

### Description

- Trafficking of arms involves the import, export, acquisition, sale, delivery, movement, or transfer of arms, their parts and components and ammunition across national borders
- This also includes the intentional diversion of firearms from legal to illegal commerce, without involving the movements of items across physical borders.<sup>2</sup>
- Arms trafficking is often associated with sanction evasion due to the nature of the product.<sup>36</sup>

### Characteristics NL

- **International trade hub:** The Netherlands is an important hub for international trade, including the role in the illegal arms trade, serving as a transit and destination country for arms.<sup>3</sup>
- **Membership European Union:** The Netherlands is part of the EU which provides the opportunity of arms to be transferred (unhindered) across EU borders.<sup>35</sup>
- **Strategic geographic location:** Because of its geographic setting and the number of sizeable transport hubs The Netherlands possesses, the country has been an entry point to Europe for international arms traffickers.<sup>68</sup>

### Modus operandi

- Arms are often originating from Germany, Belgium and Balkan countries. There is a relatively large offer of recycled firearms and 3D-printed arms.<sup>73</sup>
- Arms are mostly traded via parcel packages and road transport and stored in storage boxes.<sup>73</sup>
- Arm traffickers are usually part of criminal networks<sup>2</sup> and smaller groups of arms dealers.<sup>34</sup>
- A relatively new way of smuggling firearms into the Netherlands is the use of parcel shipments from abroad, mainly from the United States, ordered through the darknet.<sup>36</sup>

### Extent of the threat in The Netherlands

- The Small Arms Survey estimated that more than 230,000 illegal firearms circulated in The Netherlands in 2017. Police statistics show that, in the same year, 4,252 cases of illicit possession and trade in firearms were registered. After 2017, this number increased to more than 6,500 cases by the end of 2021, which translates into 37.9 cases per 100,000 of the population
- Although the latest statistics indicate an increase in the illicit trade and illicit possession of arms in The Netherlands, including firearms, previous studies and interviews with law enforcement officials suggest that structural issues with

registration or changes in the enforcement of laws might influence these annual numbers.<sup>36</sup>

### Sources\*

1. *Expert input*
2. *Arms trafficking (Global Initiative against Transnational Organised Crime) (2023) - Global Organised Crime Index*
3. *The Netherlands Country Financial Crime Dashboard (2022) – Financial Crime News*
34. *The Netherlands Country Financial Crime Dashboard (2022) – Financial Crime News*
35. *The EU's priorities for the fight against serious and organised crime for EMPACT 2022-2024 – Europol*
36. *The Way of the Gun: Firearm trafficking and its impact on violence in The Netherlands (2022) – Universiteit Leiden*
68. *National Risk Assessment Witwassen (2019) – WODC*
73. *Nationaal Dreigingsbeeld (2017) – Politie*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Bribery

### Description

- Bribery, as a financial crime, involves the offering, giving, receiving, or solicitation of something of value to influence the actions or decisions of individuals in positions of authority, such as public officials or corporate executives. The distinction is drawn between active corruption (bribery) and passive corruption (being bribed). Further differentiation is made between public corruption, involving a public official (whether domestic or foreign) as one party to the corrupt act, and private corruption, which involves only individuals in the private sector.<sup>78</sup>
- It encompasses a broad spectrum of bribery practices involving interactions between nationals and foreign officials, entailing legal and ethical complexities within the international and domestic contexts.<sup>1</sup>
- Bribery not only undermines integrity and trust, but also extracts significant amounts of money from governments and private organisations. It distorts economic development, creating legal, reputational risks and inequalities. This is also led by shifting standards of society by condemning governance related issues such as conflict of interest as criminal instead of generally accepted.<sup>1,4</sup>

### Characteristics NL

- **International trade hub:** As a major international trading country with diverse business activities, The Netherlands presents opportunities for bribery as criminal actors seek to influence international transactions and decision-making

processes.<sup>1</sup>

- **International trade partner:** The Netherlands has strong economic ties with multiple countries, which increases the threat of bribery in international business relationships.<sup>1,68</sup>
- **Favourable business environment:** Winning contracts or gaining competitive advantages in business dealings is important for the trading position of companies, which increases the threat of bribery.<sup>68</sup>
- **Strategic geographic location:** Due to its geographic setting and the number of sizeable ports The Netherlands possesses, the country has been an entry point to Europe for international drugs traffickers. Bribery of Customs authority is part of the general modus operandi for organised crime at transport hubs.

### Modus operandi

- The modus operandi for bribery is a multifaceted process involving both individuals offering bribes and those receiving them.
- Different types of bribery include: kickbacks, secret commissions, facilitation payments, undue influence and electoral bribery.<sup>1</sup>
- Bribery perpetrators can employ various tactics, such as cash payments, lavish gifts, blackmailing, overpriced services, or concealed financial incentives<sup>5</sup>, aiming to sway the decisions or actions of individuals in positions of power or authority, including Politically Exposed Persons (PEPs).<sup>1</sup>

- These bribes serve to secure favourable outcomes, such as winning contracts, obtaining regulatory approvals, or gaining undue advantages in business transactions.
- The complexity of bribery schemes can range from simple cash transactions to intricate networks of intermediaries manipulating prices or overpricing goods/services.<sup>5</sup>

### Extent of the threat in The Netherlands

- The Netherlands has a score of 80 points and rank 8 in the Corruption Perceptions Index of Transparency International.
- A country's score is the perceived level of public sector corruption on a scale of 0-100, where 0 means highly corrupt and 100 means very clean.
- A country's rank is its position relative to the other countries in the index. Ranks can merely change if the number of countries included in the index changes. The current scale includes 180 countries, where 1 means less corrupt and 180 very corrupt compared to other countries. The score of The Netherlands decreased with two points since 2021.<sup>5</sup>

### Sources\*

1. Expert input
4. *Doing business honestly without corruption (2023) - Government.nl*
5. *Corruption Perceptions Index (2023) – Transparency International*
68. *National Risk Assessment Witwassen (2019) – WODC*
78. *Corruption (2007) – Organisation for Economic co-operation and development (hereinafter: OECD)*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Concealment of beneficial ownership

### Description

- A range of techniques and mechanisms is used to obscure the ownership and control of (illicitly) obtained assets.<sup>71</sup>
- This tactic is often used to facilitate illicit financial activities, such as hiding the proceeds of criminal activities, sanction evasion, or tax evasion behind legal structures.<sup>55,1</sup>

### Characteristics NL

- **Favourable business environment:** The Dutch business environment can be attractive to companies that set up complex ownership structures to hide beneficial owners.<sup>68</sup>
- **Strong financial sector:** The strong financial sector of The Netherlands can be attractive to companies due to the status of reliability of the financial institutions within the global network. Financial institutions can be deceived by companies using offshore entities and complex structures to hide beneficial ownership.<sup>74</sup>
- **Tax environment and financial infrastructure:** Although The Netherlands increasing efforts to promote financial transparency, certain legal provisions and tax regulations may still provide opportunities for concealing beneficial ownership. Examples are the existence of the administrative office foundation (STAK, Stichting Administratiekantoor) as a structure and bilateral international tax agreements.<sup>1</sup>
- **International trade partner:** Shell or front companies are

often based in locations with beneficial ownership secrecy provisions.<sup>74</sup>

### Modus operandi

- The concealment of beneficial ownership often involves establishing complex ownership structures.
- These ownership structures may be utilised to create layers of obfuscation, with conduit companies, offshore companies, and shell companies in different jurisdictions acting as fronts to conceal the true beneficiaries.
- (Existing or established) trust offices and service provider companies may be employed to serve as intermediaries, managing administrative aspects of these structures while keeping the beneficial owners' identities hidden.<sup>71</sup> Sometimes, the person who exerts influence or control might not even hold an official role within the organisation.<sup>1</sup>
- Schemes designed to obscure beneficial ownership often employ a 'hide-in-plain sight' strategy<sup>55</sup>, leveraging global trade and commerce infrastructures to appear legitimate.<sup>71</sup>

### Extent of the threat in The Netherlands

- 17% of the jurisdictions that participated in the FATF's Horizontal Study of supervision and enforcement of beneficial ownership obligations do not impose any

AML/CFT obligations or AML/CFT supervision on any designated non-financial businesses and professions, despite this being a requirement of the FATF Standards. As the global economy becomes increasingly interconnected, and the sovereignty of financial borders dissipates, it is important to ensure that authorities have access to the appropriate information required to effectively deliver their mandate. One of the several mechanisms to enable timely access to beneficial ownership information is the implementation of the register of beneficial ownership.<sup>71</sup>

### Sources\*

1. *Expert input*
55. *Building Effective Beneficial Ownership Frameworks (2021) – OECD*
68. *National Risk Assessment Witwassen (2019) – WODC*
71. *Concealment of Beneficial ownership (2018) – Financial Action Task Force (hereinafter: FATF)*
74. *Behind the Scenes. Beneficial ownership transparency in The Netherlands (2017) – Transparency International*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Concealment of identity

### Description

- Concealment of identity represents a significant threat in the context of financial crime and security.
- It involves the deliberate masking of one's identity by individuals or entities, often for illicit purposes such as money laundering, fraud, sanction evasion, or financing terrorism.
- This threat hampers the ability of authorities and effective gatekeeper role such as banks to identify and track those involved in illegal activities.<sup>1</sup>

### Characteristics NL

- **Digital inclusivity:** The high level of digital inclusivity and online services in The Netherlands can be useful for fraudsters to forge or misuse digital identities for financial crimes.<sup>80</sup>
- **Openness to financial innovations:** The Dutch focus on financial innovation can provide new opportunities for identity concealment through digital channels, such as virtual private networks (VPNs) or cryptocurrency transactions.<sup>68</sup>

### Modus operandi

- The general modus operandi for concealing identity includes the use of various tactics and tools such as false identities

(e.g. use of money mules or misuse of vulnerable persons), bank accounts opened with false identities (1-cent verification or pictures not matching the identity), forged documents, shell companies, and anonymising technologies like VPNs or cryptocurrency transactions.

- Additionally, cyber technologies and artificial intelligence, including deepfake technology are increasingly used for various forms of identity theft.
- These techniques create layers of obfuscation, making it challenging for law enforcement and financial institutions to ascertain true identities and trace illicit funds' sources.<sup>6</sup>

### Extent of the threat in The Netherlands

- Publicly available sources do not provide information about the extent of concealment of identity in The Netherlands.

### Sources\*

1. *Expert input*
6. *The Other Side of the Coin: An Analysis of Financial and Economic Crime (2023) – Europol*
68. *National Risk Assessment Witwassen (2019) – WODC*
80. *Identity fraud, tax evasion and money laundering vulnerabilities (2006) – OECD*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Drugs economy

### Description

- In The Netherlands, drug-related offences, encompassing import, export, production, sale, consumption, and the manufacturing of (synthetic) drugs, are considered major predicate offences. They present a significant challenge for law enforcement and public health.<sup>8</sup>
- This, and the fact that The Netherlands plays an important role as a transit country, increases the organised crime elements associated with these activities. Furthermore, it pollutes the Dutch economy and financial flows with funds derived from the drugs economy.<sup>3</sup>
- Production is mainly focused on cannabis and synthetic drugs. Distribution is mainly on cocaine and heroin. Consumption is mainly focused on cannabis.<sup>45</sup>

### Characteristics NL

- **International trade partner:** The Netherlands is a major producer, exporter, and consumer of cannabis and synthetic drugs, such as amphetamines and ecstasy (MDMA).<sup>3</sup>
- **International trade hub:** The Netherlands is also an important transit country for cocaine and heroin. Organised crime and manifestations thereof are related to the transportation of these illicit substances.<sup>1</sup>
- **Culture of tolerance:** The use of soft drugs is tolerated in The Netherlands and lack of societal disapproval of drug

abuse is translated in a Dutch drug policy consisting of harm reduction and toleration.<sup>46</sup>

- **Drugs industry:** Resource capacity and security of supplies are sufficient. Additionally, the quality of products and sales opportunities are high and raw materials to produce drugs are often for sale in smartshops, grow shops and at wholesalers.<sup>45</sup>
- **Strategic geographic location:** The Netherlands' geographical position, with access to major sea routes and proximity to other European markets, makes it a strategic hub for the distribution and transportation of drugs. The Netherlands' unique role as a vital importer and exporter of various drugs reinforces its strategic position in the global drug trade, impacting the reconciliation of financial flows.<sup>1</sup>

### Modus operandi

- The drugs economy is driven by organised crime in The Netherlands. Domestic and international cases indicate that the proceeds of drug trafficking are often laundered through cash or underground banking.<sup>68</sup>
- Transportation of drugs is facilitated via postal parcels, seaports (such as Rotterdam, IJmuiden and Vlissingen), road transport, Schiphol airport and the Dutch flower auction.<sup>1</sup>
- The drugs economy is also often associated with extortion of import companies and protection racketeering. The drugs

economy is also connected to corruption, as the trade frequently necessitates involvement from corrupt officials/employees who can for example arrange a fake passport and provide relevant police data.<sup>1,3</sup>

- The drugs economy creates large volumes of outgoing cash flows to among others South America, West Africa and Asia.<sup>1</sup>

### Extent of the threat in The Netherlands

- In 2023, the Dutch Customs authority seized nearly 60,000 kilograms of cocaine, a significant increase from 51,000 kilograms the previous year. The largest amounts were found in the ports of Rotterdam and Vlissingen, with cocaine seizures at airports doubling.<sup>9</sup>

### Sources\*

1. Expert input
3. *Criminality in The Netherlands (2023) - The Organised Crime Index*
8. *Drugs en drugscriminaliteit (2023) – Het Centrum voor Criminaliteitspreventie en veiligheid (hereinafter: CCV)*
9. *'Doone onderschept forst meer cocaine in 2023 (2024) – Rijksoverheid.nl*
45. *Vestigingsklimaat voor drugscriminaliteit in Nederland (2022) – WODC*
46. *Evaluatie Nederland (2022) – FATF*
68. *National Risk Assessment Witwassen (2019) - WODC*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Environmental crime

### Description

- Environmental crime covers the activities that breach environmental legislation and cause significant harm or risk to the environment, human health, or both.<sup>47</sup>
- Examples of environmental crime are soil, water and/or air pollution, manure fraud, waste trafficking, drug waste and trading illegal wildlife.<sup>47</sup>

### Characteristics NL

- **International trade partner:** The Netherlands, as a financial and logistic hub, serves as a significant transit and destination country for many commodities associated with illegal activities such as deforestation and illicit mining, thereby contributing to the global ecological crisis.<sup>34</sup> Lacking many natural resources itself, the Netherlands is subject to increased regulatory pressures that are often stricter than elsewhere.<sup>1</sup> The country also serves as a significant transit and destination for the illicit trade of endangered plant species, wild-caught songbirds, waterfowl, and birds of prey.
- **Strategic geographic location:** The close connection to the Dutch Caribbean Islands (Aruba, Bonaire, Curacao, Sint-Maarten, Sint-Eustatius and Saba) is associated with smuggling of wildlife and other environmental crimes due to the origin of the products and the relationship with these islands.<sup>1</sup>

- **Diversity of labour sectors:** The Netherlands has several large companies with old permits which do not fit current climate goals. The Netherlands also has a thriving drug production industry (related to drug waste), and high labour costs provide the motivation for the processing of waste elsewhere (waste trafficking).<sup>1</sup>
- **Export of food and agricultural products:** The Netherlands' large agricultural sector contributes to issues like manure fraud and misuse of crop protection agents which can lead to problematic handling of concerning substances.

### Modus operandi

- Environmental criminals often misuse complex international structures, use underground banking networks, commit TBML, infiltrate in legal business structures at senior level, set up own companies to facilitate their crimes and/or use falsified documents to conceal their crime.<sup>1,48</sup> These criminals can manipulate the supply chains, causing commodities, for example from illegal mining, to land in The Netherlands through multiple intermediaries and complex structures, making it increasingly difficult to trace their origins.<sup>1</sup>
- Some seemingly legitimate businesses do engage in illegal activities, making the distinction between legal and illegal operations challenging at times. For example, raw materials from illegal mining often end up in The Netherlands via

numerous intermediaries with complex structures, making it difficult to trace the original source.<sup>1</sup>

- Trading in illegal wildlife is often done by means of luggage of individuals, mail parcels and legal shipments imported by companies. Therefore, Schiphol Airport is a key transit point for illicit wildlife.<sup>56</sup>

### Extent of the threat in The Netherlands

- The Human Environment and Transport Inspectorate (ILT, the Dutch government inspectorate in this area) calculated the damage caused by environmental crime and violations in 2020 at €4.35 billion.<sup>1</sup>
- According to the Algemene Rekenkamer, the approach to environmental crime and violations is inadequate in The Netherlands.<sup>57</sup>

### Sources\*

1. *Expert input*
34. *The Netherlands Country Financial Crime Dashboard (2022) – Financial Crime news*
47. *Environmental Crime (2022) – Europal*
48. *Jaaroverzicht Criminele Geldstromen 2022 – Openbaar Ministerie*
56. *Dreigingsbeeld Milieucriminaliteit 2021 – Rijksoverheid*
57. *Handhaven in het duister (2021) – Algemene Rekenkamer*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Extremism

### Description

- Extremism refers in this threat assessment to the use and exploitation of financial systems and resources by extremist individuals or groups to fund and support their radical ideologies or activities.<sup>10</sup>
- This threat also involves the use of illicit financial channels and methods to raise funds, conceal the origins of funds, and finance extremist agendas, including recruitment and propaganda dissemination.<sup>53</sup>
- Extremism can lead to terrorism when socially disruptive damage is caused and/or major groups of people are threatened.

### Characteristics NL

- **Strong financial sector:** The Netherlands is home to various financial service providers and an advanced digital infrastructure.<sup>68</sup> This provides the opportunity for extremists to access obscure financial transactions and fundraising through various financial channels.<sup>1</sup>
- **Cultural diversity:** The Netherlands has a multicultural society, which can result in complex international flows of money and donations,<sup>68</sup> making it more difficult to detect extremist financing.
- **Culture of tolerance:** The open and tolerant society of The Netherlands can attract extremists or provide them with

opportunities to hide their activities.<sup>69</sup>

### Modus operandi

- The general modus operandi for extremism in financial crime includes fundraising through a range of sources, such as donations from sympathisers, criminal activities, and exploitation of charitable organisations.
- Extremists may resort to utilizing crowdfunding platforms to gather financial support for their activities. This method involves collecting small contributions from a large number of individuals through online platforms.<sup>53</sup>
- Extremists may employ money laundering techniques, utilise virtual assets and engage in fraudulent financial transactions to obscure the flow of funds.<sup>1</sup>

### Extent of the threat in The Netherlands

- Publicly available sources do not provide information about the extent of extremism in The Netherlands presumably due to the confidential and sensitive nature of such information.

### Sources\*

1. *Expert input*
10. *Anti-Money Laundering/Combating the Financing of Terrorism (2023) - IMF*
53. *Ethnically or racially motivated terrorism financing (2021) – FATF*
68. *National Risk Assessment Witwassen 2019 – WODC*
69. *National Risk Assessment Terrorisme financiering 2019 - WODC*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Fragmentation of payment landscape

### Description

- The fragmentation of the payment landscape, driven by the introduction of new payment methods in combination with the existing financial institutions, represents a growing threat to the integrity of financial systems.
- This threat arises from the increasing diversification of payment options which can lead to widely dispersed regulated financial transactions.<sup>50</sup>
- Criminals can deliberately use the fragmented payment landscape to disguise money flows and make it more difficult to follow transaction flows.<sup>14</sup>
- Additionally, due to this increased fragmentation, law enforcement agencies may struggle to obtain a full view on financial flows and patterns, and banks may find it challenging to understand the background of batch payments received from Payment Service Providers (PSPs). This evolving landscape adds another layer of complexity to the already challenging task of transaction monitoring and financial crime detection.<sup>1</sup>

### Characteristics NL

- **Openness to financial innovations:** Embracing new payment methods could lead to (more) fragmentation, as various financial technology companies and start-ups introduce new methods.<sup>72</sup>

- **Digital inclusivity:** The Netherlands has a high digital acceptance rate, which facilitates the adoption of new payment methods. This can lead to a greater variety of payment options and associated fragmented payment landscape.<sup>1</sup>

### Modus operandi

- The general modus operandi involves proliferation of various payment methods, leading to a dispersion of transaction data across multiple platforms and systems.
- Different financial institutions support these fragmented payment methods such as payment service providers, virtual IBAN providers, money transfer organisations and virtual asset service (crypto/NFT) providers (*hereinafter: VASPs*).
- Digital solutions make it also easier to open bank accounts with foreign banks.
- Additionally, individual transactions in batches of transactions are not visible to other financial institutions, which makes the source of the funds not identifiable.<sup>14,72</sup>

### Extent of the threat in The Netherlands

- Almost 50,000 registered entities in The Netherlands are

allowed to provide financial services.<sup>15</sup>

- Since the implementation of PSD2, the financial ecosystem has become an increasingly complex and fragmented chain.
- The payment chain involves many players (some regulated, some not) and complexity and interdependence continue to increase.<sup>43</sup>

### Sources\*

1. *Expert input*
14. *Money Laundering vulnerabilities at PSP's (2023) – Anti Money Laundering Centre (hereinafter: AMLC)*
15. *Openbaar register (dnb.nl)*
43. *Evaluatie PSD2 (2022) – SEO Economisch Onderzoek*
50. *Confronting Fragmentation: How to Modernize the International Payment System (2022) – IMF*
68. *National Risk Assessment Witwassen 2019 - WODC*
72. *Fintechs in the payment system: the risk of foreclosure (2017) – Autoriteit Consument & Markt (hereinafter: ACM)*



# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Market facilitators

### Description

- Market facilitators, extending beyond traditional financial institutions, encompass a range of professionals, including lawyers, accountants, real estate agents, civil law notaries, appraisers, jewellers, and others.
- Within this scope, it is important to differentiate between those who engage in criminal cooperation willingly and those being unwittingly misused by criminals.<sup>62</sup>
- This diverse involvement of (non)-financial gatekeepers poses a significant regulatory challenge, distinguishing between active accomplices and those unwittingly involved.<sup>59,60</sup>

### Characteristics NL

- **International trade hub:** As an international trading hub, The Netherlands is an attractive environment for market facilitators to offer their services, leveraging its complex financial transaction landscape and trading activities.<sup>68</sup>
- **Strong financial sector:** The diversity of financial service providers and business opportunities in The Netherlands offer market facilitators different channels to conduct their activities, often with limited supervision.<sup>73</sup>
- **Information sharing:** Market facilitators are not positioned to share information amongst each other. The different types of market facilitators require identical information

from their clients as financial institutions require. However, information sharing is not common nor allowed in most cases.<sup>1,73</sup>

### Modus operandi

- The general modus operandi for market facilitators beyond financial institutions involves using their professional knowledge and access to create opportunities for financial crimes.
- Market facilitators may provide advice on structuring transactions to conceal the origins of funds, facilitate transactions for clients with minimal scrutiny, or set up complex corporate structures to obscure ownership.
- These facilitators often exploit regulatory gaps, operate in jurisdictions with lax oversight, or use digital technologies to provide a cloak of anonymity for their clients.<sup>58</sup> However, the rationale behind the requested anonymity can also indicate legal purposes.
- Market facilitators, despite professional knowledge, may inadvertently contribute to financial crimes when lacking awareness or oversight, failing to recognize the illicit nature of transactions they facilitate.<sup>62</sup>

### Extent of the threat in The Netherlands

- The total amount of unusual transaction reports to the FIU-

NL (excluding the Caribbean part of The Netherlands) in 2022 is 1,896,176.<sup>51</sup>

- Market facilitators (lawyers, notaries etc.) reported merely ~14,000 unusual transaction reports.<sup>51</sup>
- Over the past 20 years, notaries and real estate agents have been convicted of fraud (forgery, misuse of third-party accounts), but the extent is relatively small based on registrations.<sup>51</sup>

### Sources\*

1. *Expert input*
51. *FIU Nederland Jaaroverzicht 2022*
58. *Ending the Shell Game Cracking down on the Professionals who enable Tax and White-Collar Crimes (2021) – OECD*
59. *The Role and Responsibilities of Gatekeepers in the Fight against Illicit Financial Flows: A Unifying Framework (2021) – World Economic Forum*
60. *Professional enablers of illicit financial flows and high-risk services and jurisdictions (2021) – Transparency International*
62. *Samen (2021) – A.B. Hoogenboom*
68. *National Risk Assessment Witwassen 2019 - WODC*
73. *Nationaal dreigingsbeeld 2017 – Politie*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Modern slavery

### Description

- Modern slavery involves the exploitation of individuals through coercive or deceptive practices to extract forced labour or services for financial gain.
- This threat encompasses various forms but can be divided into four main categories: labour exploitation, sexual exploitation, criminal exploitation and forced organ removal.<sup>1,16</sup>
- The proceeds generated from these illicit activities flow into the global financial system. Those involved in modern slavery exploit their victims to generate income, often obscuring the sources of these funds through intricate financial transactions. Essentially, it refers to situations of exploitation that a person cannot refuse or escape from the situation due to threats, violence, coercion, deception, and/or abuse of power.<sup>52</sup>

### Characteristics NL

- **International trade hub:** The Netherlands is an international trade hub with a complex supply chain. This makes it possible for modern slave owners to hide labour exploitation in the various links of the supply chain, such as human trafficking, blending the victims in the legal workforces, or housing the victims.<sup>1,73</sup>

- **International trade partner:** The Netherlands, due to its open society and geographical position, is a transit and destination point for modern slavery victims and the proceeds of this exploitation.<sup>1,68</sup>
- **Diversity of labour sectors:** The Netherlands has several labour sectors, including agriculture, catering, and construction which are vulnerable to labour exploitation. This is also connected to 'slavery discount', which means that the price of products is significantly low so that decent salaries are not even possible.<sup>1</sup>

### Modus operandi

- The general modus operandi for modern slavery involves a multi-step process. Criminals typically recruit vulnerable individuals through deceptive means or coercion, promising better opportunities. Often, these victims are labour migrants from poorer European Union countries, recruited by unscrupulous recruitment agencies. Once under the control of the criminals, victims are subjected to various forms of abuse, including forced labour in industries like agriculture or construction, being used as money mule, or even sexual exploitation in cases of sex trafficking.
- The proceeds from these illegal activities are often concealed through financial transactions and money

laundering, making it challenging to trace the funds back to the source.<sup>16,17,19</sup> Examples of these transactions include cryptocurrency transactions and the purchase of real estate in Romania, Turkey or Dubai.<sup>1</sup>

### Extent of the threat in The Netherlands

- Worldwide, the number of people who are victims of modern slavery has increased to 50 million in recent years.<sup>18</sup>
- According to WODC, The Netherlands has approximately 5.000 victims of modern slavery on a yearly basis.<sup>75</sup>

### Sources\*

1. *Expert input*
16. *Veilighedsagenda 2023-2026 – Politie*
17. *FEC Jaarplan 2023*
18. *Global Slavery Index (2023) – Walk Free*
19. *Mensenhandel en (seksuele) Criminele uitbuiting (2023) – CCV*
52. *Global Estimates of Modern Slavery: Forced Labour and Forced Marriage (2022) – International Labour Organization*
68. *National Risk Assessment Witwassen 2019 - WODC*
73. *Nationaal dreigingsbeeld 2017 – Politie*
75. *Multiple Systems Estimation Slachtoffers Mensenhandel Nederland 2016-2019 - WODC*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Organised crime in transport hubs (sea and airports)

### Description

- Organised crime in transport hubs, such as sea and airports, is a multifaceted financial crime threat.
- Criminal networks engage in various illicit activities, including drug trafficking and human trafficking.
- These networks strategically exploit smuggling, bribery and corruption and contraband trade, enabling them to use logistical advantages of transport hubs, hiding illicit goods within legitimate cargo and evading customs checks.<sup>67</sup>
- The financial implications are substantial, as organised crime proceeds are often laundered through complex financial systems, making it challenging to trace the source of these funds.<sup>1</sup>

### Characteristics NL

- **Strategic geographical location:** The Netherlands has important sea and airports with excellent connections to international destinations. This favourable geographical location makes it attractive for organised crime to use The Netherlands as a transit and distribution point for illegal goods.<sup>33</sup>
- **International trade partner:** The high volumes of international trade and goods passing through Dutch transport hubs provide criminal networks with cover and opportunities to conceal illegal activities in the flow of

legitimate trade.<sup>68</sup>

- **Logistics and infrastructure:** The advanced logistics infrastructure enables criminal actors to develop efficient methods for smuggling illegal goods into and out of the country, which contributes to the increase of financial and economic crimes by organised crime in transport hubs.<sup>1,68</sup>

### Modus operandi

- The general modus operandi for organised crime in transport hubs often involves a combination of methods, including concealing illegal goods in legitimate cargo, bribing or corrupting customs officials and/or other relevant workers, using front companies and employing complex money laundering techniques to legitimise their ill-gotten gains.
- Criminal networks leverage the vast volume of international trade passing through transport hubs, taking advantage of logistical vulnerabilities and regulatory gaps to evade detection.<sup>67</sup> In particular, industries in which timelines for transport are required to be short (e.g. flowers and food) are vulnerable due to the limited ability on control of the transport.<sup>1</sup>

### Extent of the threat in The Netherlands

- The Netherlands has five main transport hubs: the ports of

Rotterdam, the Noordzeekanaalgebied and Zeeland/West-Brabant, Schiphol Airport and the flower auctions.<sup>33</sup>

- Specifically in 2023, drug trafficking as a key underlying predicate offence surged. Major ports like Rotterdam and Vlissingen saw nearly 60.000 kilograms of cocaine seized, a significant increase from the previous year. Additionally, there was a notable doubling of seizures at airports.<sup>9</sup>

### Sources\*

1. *Expert input*
9. *'Douane onderschept forst meer cocaine in 2023 (2024) – Rijksverheid.nl*
33. *Bijna 30 miljoen euro tegen drugssmokkel via mainports (2022) – Rijksverheid.nl*
67. *Criminaliteit en veiligheid in mainports (2019) – Fijnaut*
68. *National Risk Assessment Witwassen 2019 - WODC*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Payment fraud

### Description

- Payment fraud is a type of financial fraud that involves the use of false or stolen payment information to obtain money or goods.
- It involves fraudulent activities aimed at misappropriating funds, compromising financial transactions, or illegally obtaining money through unauthorised or deceptive means.
- It encompasses various tactics to manipulate payment systems, impersonate legitimate entities, or exploit vulnerabilities in financial transactions, resulting in financial losses and security breaches. Examples are helpdesk fraud (impersonation of a helpdesk employee) or marketplace fraud.<sup>20,21</sup>

### Characteristics NL

- **Digital inclusivity:** The Netherlands has an advanced digital infrastructure and is highly digitised, making it an attractive target for cybercriminals pursuing payment fraud.<sup>68</sup> The broad availability of digital payment services and the ease of online transactions in The Netherlands can also encourage criminals to undertake fraudulent activities.<sup>63</sup>
- **Strong financial sector:** As a financial centre with countless financial transactions, including international payments and e-commerce, The Netherlands provides ample opportunities for payment fraud.<sup>22</sup>

- **Openness to financial innovations:** The Dutch focus on financial innovation can provide new opportunities for payment fraud, such as Tikkies.

### Modus operandi

- Payment fraud exists in many different forms, including theft of credit card numbers from an unprotected card reader, the sale of stolen card details on the dark web and malicious fake emails.<sup>1,20</sup>
- The general modus operandi for payment fraud includes tactics such as phishing, account takeover, counterfeit payments and unauthorised fund transfers.
- Criminals may send deceptive emails or messages to trick individuals or organisations into revealing sensitive financial information.<sup>1,20</sup> They may also compromise payment methods or use stolen credentials to initiate unauthorized transactions. This form of scam occurs via Marktplaats, Facebook, Vinted and other (reselling) platforms.<sup>21</sup> With the development of Artificial Intelligence (AI) and advancements in cyber technology, these fraudulent activities have become more sophisticated.<sup>1</sup>

### Extent of the threat in The Netherlands

- The total damage of fraud in the Dutch payment system is estimated on €60.7 million in 2022.<sup>13</sup>

### Sources\*

1. Expert input
13. Veiligheid (2023) - NVB: <https://www.bankinbeeld.nl/thema/veiligheid/>
20. Six types of payment fraud—and how businesses can prevent them (2023) – Stripe
21. Wat is betaalverzoekfraude? (2023) – Politie
22. The State of Financial Crime 2023 - ComplyAdvantage
63. Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios (2020) – Bateman
68. National Risk Assessment Witwassen 2019 - WODC

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Public funding fraud

### Description

- Public funding fraud is a type of financial fraud when individuals, organisations, or organised criminal groups claim public funding or grants that they are not eligible for.
- Healthcare fraud and subsidy fraud are illustrative examples of this threat.<sup>6</sup>

### Characteristics NL

- **Healthcare and social services:** The wake of COVID-19 pandemic made criminals search for new opportunities to defraud public funding.<sup>64</sup> The Netherlands created in a short amount of time multiple public funding opportunities during the COVID-19 pandemic such as NOW (Noodmaatregel Overbrugging voor Werkgelegenheid) and TVL (Tegemoetkoming Vaste Lasten) with a lack of sufficient controls on the validity of the applications.<sup>1,6</sup>
- **Membership European Union:** The Netherlands is a member of the European Union, which makes The Netherlands vulnerable for EU subsidy fraud. This entails the submission of fraudulent applications for EU grants or tenders.<sup>64</sup>
- **Political stability and regulation:** The Netherlands' stable welfare state with numerous subsidies and allowances

creates opportunities for public funding fraud.

### Modus operandi

- Applications are often based on false declarations, progress reports and invoices.<sup>64</sup>
- Organised criminals often attempt to use corruption to access the public funds because it requires knowledge of subsidy application processes. Criminal organisations are using the government as an ATM by searching for opportunities to misuse government money.<sup>1,6</sup>
- With the EU focusing on a more sustainable, digital, and resilient economy, subsidy fraudsters are set to increasingly target sectors such as renewable energy, research programs, and the agricultural sectors.<sup>1</sup>
- Public funding fraud can be associated with exploitation (force to apply to public funds).<sup>73</sup>

### Extent of the threat in The Netherlands

- The total damage of fraud in the Dutch payment system is estimated on €60.7 million in 2022.<sup>13</sup>

### Sources\*

1. *Expert input*
6. *The Other Side of the Coin: An Analysis of Financial and Economic Crime (2023) – Europol*
13. *Veiligheid (2023) - NVB: <https://www.bankinbeeld.nl/thema/veiligheid/>*
64. *Enterprising criminals - Europe's fight against the global networks of financial and economic crime – Europol*
68. *National Risk Assessment Witwassen 2019 - WODC*
73. *Nationaal dreigingsbeeld 2017 - Politie*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Sanctions evasion

### Description

- Sanctions evasion is a threat that involves individuals, entities, or even countries seeking to bypass or circumvent economic or trade sanctions imposed by international bodies, governments, or organisations.
- These sanctions are typically imposed as a means of pressuring non-compliant entities to adhere to certain international standards, cease activities, or face economic consequences.<sup>39,70</sup> Additionally, sanctions are imposed as a means of preventing non-compliant behaviour of natural persons and legal persons.<sup>1</sup>
- Sanctions evasion involves efforts to continue prohibited activities or trade with sanctioned parties while avoiding the penalties associated with non-compliance.<sup>1</sup>

### Characteristics NL

- **International trade hub:** The Netherlands acts as a transit country for goods and capital. This connectivity can enable entities to commit sanctions evasion by taking advantage of the various trade routes, financial infrastructures<sup>68</sup> and limited control of the Customs authority.<sup>1</sup>
- **International trade hub:** Dutch law enforcement capacity is limited in comparison to the size of the Dutch financial and trade flows.<sup>1</sup>
- **Strong financial sector:** The numerous financial service providers and banks can provide potential channels for

financial transactions that facilitate sanctions evasion.<sup>1,68</sup>

- **Favourable business environment:** The Netherlands is known for its expedient to establish business entities. This can be attractive to entities attempting to commit sanctions evasion by setting up front companies or using complex corporate structures.<sup>1,68</sup>
- **Information sharing:** Restrictions on information sharing between national authorities and between different agencies (such as customs data, information on SARs and criminal records) creates a challenge in the detection of sanctions evasion.<sup>1</sup>

### Modus operandi

- The general modus operandi for sanctions evasion includes the use of deceptive tactics such as use of shell and front entities and intermediaries, sudden change of ownership (to family members or supposed shift to minority shares), use of complex and obscure ownership structures, use of a strawman, abuse of legal loopholes, payments on behalf of sanctioned persons, business relocation to non-sanctioned countries (on paper but not in practice) and use of U-turns for sectoral sanctions. Furthermore, sanctions evasion is likely to be accompanied by documentary fraud. Sometimes, sea smuggling methods are employed.<sup>39</sup> However, sanctions evasion is not always wilfully committed. Entities could have insufficient knowledge on sanctions and could be vulnerable to sanctions evasion.<sup>1</sup>

- Payment routes which are unnecessary complex to hide the trail such as several different payors and beneficiaries and multiple banks in different jurisdictions to perform a single transaction.<sup>1</sup>
- These tactics enable individuals, organisations, or nations to continue conducting business with sanctioned parties or engaging in prohibited activities, all while maintaining an appearance of compliance.<sup>68</sup>

### Extent of the threat in The Netherlands

- Given the recent global events, such as the conflict between Russia and Ukraine, the number of international sanctions has been on the rise. This trend has been underscored by the adoption of a twelfth sanctions package by the European Union.<sup>1,49</sup>

### Sources\*

1. *Expert input*
39. *3 Most Widely Used Sanction Evasion Techniques (2022) – Regtech Times*
49. *Kirgizië, Armenië, Turkije: via deze landen krijgt Rusland toch sanctieproducten - Research NOS.nl (2022) based on a database of United Nations trade figures (Comtrade) - <https://nos.nl/artikel/2457477-kirgizie-armenie-turkije-via-deze-landen-krijgt-rusland-toch-sanctieproducten>*
68. *National Risk Assessment Witwassen 2019 – WODC*
70. *Preventing and Detecting Sanctions Evasion Schemes (2019) – ACAMS Today*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## State actors

### Description

- The threat of state actors refers to governments or government affiliated entities/individuals engaging in illicit activities such as unlawful influence, interference, disinformation and espionage aimed to disrupt national security, while leveraging state resources and institutions. Additionally, state actors might engage in unauthorised knowledge transfers, seeking to unlawfully access or transfer sensitive information for strategic advantages.
- The threat that state actors can pose can also entail various financial crimes such as money laundering, corruption and economic espionage, often entailing elements of foreign influence.<sup>26</sup>

### Characteristics NL

- **International trade hub:** The Netherlands has a prominent position in international trade and economy, which can make it attractive to state actors who seek to influence or exploit economic activities for their own gain.<sup>1</sup>
- **Strong financial sector:** The Netherlands is home to an advanced financial sector with various financial service providers, which provides opportunities for state actors to manipulate or abuse financial transactions.<sup>68</sup>
- **Political stability and regulation:** The political stability and strong financial regulation in The Netherlands may give the

impression that financial manipulation by state actors is less likely, but also provide an environment in which such activities are possible due to their stealth.<sup>68</sup> The Netherlands is also the location for multiple international organisations such as the International Court of Justice and Europol. <sup>1</sup>

- **Favourable business environment:** The location of many international organisations in The Netherlands makes the country attractive for influence by state actions.<sup>1,68</sup>

### Modus operandi

- The general modus operandi for state actors in financial crime encompasses a range of tactics, such as cyber-attacks, (physical) infiltration, embezzlement, bribery, and illicit asset acquisition.
- State actors may misuse government contracts, manipulate financial markets, or employ money laundering techniques to obscure the origin of ill-gotten funds.<sup>12,26</sup>
- Influence, interference, disinformation and espionage are commonly used means to disrupt national security in the short term (up to two years).<sup>26</sup>

### Extent of the threat in The Netherlands

- Publicly available sources do not provide information about the extent of the threat of state actors in The Netherlands

presumably due to the confidential and sensitive nature of such information.

### Sources\*

1. *Expert input*
12. *Tussen uitschakeling & inschakeling (2023) - WODC*
26. *The Threat Assessment State-sponsored Actors (2023) - AIVD, MIVD and NCTV*
68. *National Risk Assessment Witwassen 2019 - WODC*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Tax evasion

### Description

- Tax evasion is a financial crime that entails deliberate efforts to underreport income, inflate deductions or hide assets, not only to reduce tax liability but also to defraud government revenue agencies.
- This may also involve fraudulent claims for tax refunds when not entitled to them.
- Tax evasion is a predicate offence for money laundering since the money earned by not paying taxes needs to be laundered.<sup>1</sup>
- These illicit tactics lead to significant financial losses for governments, undermine the integrity of the tax system, and contribute to societal inequality.<sup>28</sup> However, international pressure increases to prevent tax evasion.<sup>1</sup>

### Characteristics NL

- **Tax environment and financial infrastructure:** Due to its open economy The Netherlands unintentionally became attractive for tax avoidance structures, aided by a complex tax environment with various tax benefits such as bilateral international tax agreements and favourable regulations for companies.<sup>23</sup>
- **International trade hub:** As an international trade and investment hub,<sup>68</sup> The Netherlands can be used as a transit country for international financial transactions, making it

possible to avoid taxes.<sup>1</sup>

### Modus operandi

- Strategic use of various tactics include the use of free trade zones abroad to minimize or avoid taxes on imported or exported goods, dividend stripping by manipulating financial transactions to exploit tax credits and conduit companies to channel income through entities with favourable tax treatment.<sup>28</sup>
- These tactics often exploit regulatory gaps and international tax treaties to conceal income and assets, resulting in substantial revenue losses for governments.<sup>28</sup>

### Extent of the threat in The Netherlands

- It is estimated that 16.2% of global corporate tax avoidance (~ 51 billion dollars) and 4.9% of private wealth related tax avoidance is channelled through The Netherlands.
- Every year, developing countries lose at least approximately €460 million due to tax avoidance via The Netherlands.<sup>27</sup>

### Sources\*

1. *Expert input*
23. *Aanpak belastingontwijking en belastingontduiking (2023) – Rijksoverheid.*  
<https://www.rijksoverheid.nl/onderwerpen/aanpak-belastingontwijking-en-belastingontduiking>
27. *The State of Tax Justice (2023) - Tax Justice Network*
28. *Tax Evasion (2023) – Transparency International.*  
<https://www.transparency.org/en/corruptionary/tax-evasion>
68. *National Risk Assessment Witwassen 2019 - WODC*



# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Terrorism financing

### Description

- Terrorism financing (TF) encompasses the solicitation, collection, or provision of funds intended to support terrorist acts, terrorists, or terrorist organisations, including the planning, recruiting, and execution of such acts.
- This illicit activity often involves transfer of money, assets or goods, camouflaged as legitimate transactions to facilitate operations of terrorist groups or individuals.<sup>69</sup>

### Characteristics NL

- **International trade hub:** The Netherlands has an extensive international trade network, making it possible for terrorist financing sources to hide financial flows in the complex world of international trade.<sup>68</sup>
- **Strong financial sector:** The Netherlands is home to a wide range of financial service providers, including banks and financial intermediaries. This diversity provides opportunities for financial transactions that can be misused for terrorism financing.<sup>68</sup>
- **Favourable business environment:** Legal entities can be misused for terrorism financing. Due to the favourable business environment, terrorists could hide between a number of legal entities in The Netherlands.<sup>11</sup>

### Modus operandi

- The general modus operandi for terrorism financing includes fundraising through a variety of sources, such as charitable organisations, crowdfunding using social media platforms including messaging apps<sup>1</sup>, criminal activities and legitimate businesses.
- Informal financial systems may be exploited such as the use of hawala or hundi networks, but also modern financial technologies are misused including cryptocurrencies to move funds discreetly.<sup>46,69</sup>

### Extent of the threat in The Netherlands

- The terrorist threats in The Netherlands have increased over the past six months (Q4 2023).
- The current terrorism threat level in The Netherlands is level 4, which indicates that the risk of an attack in The Netherlands is substantive.<sup>11</sup>
- In 2022, 24 people were arrested for terrorism, 21 for Jihadism and 3 for right-wing extremism.<sup>1</sup>

### Sources\*

1. *Expert input*
11. *Dreigingsbeeld Terrorisme Nederland (2023) - NCTV*
46. *Evaluatie Nederland (2022) – FAFT*
68. *National Risk Assessment Witwassen 2019 – WODC*
69. *National Risk Assessment Terrorisme financiering 2019 - WODC*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Trade-based money laundering (TBML)

### Description

- Trade-based money laundering involves complex arrangements using goods and/or services to facilitate the movement of funds, concealing, or legitimising the illicit origins of criminal proceeds.<sup>68,79</sup>
- This method operates internationally, encompassing intricate trade structures and transactions across borders, aiming to disguise the illegal source of funds by manipulating trade activities.<sup>1,79</sup>

### Characteristics NL

- **International trade hub:** The Netherlands is characterised by an open, trade-oriented economy. Therefore, The Netherlands has an attractive environment for trade constructions with goods and/or services. Especially goods used for TBML such as metals, construction equipment, real estate, art and other high value goods are produced and/or traded in The Netherlands.<sup>79</sup>
- **International trade partner:** The Netherlands has strong international relations and an important trade position. These strong international relationships are used as a mechanism to carry out TBML activities, exploiting import channels to conceal or legitimise financial crime.<sup>68</sup>
- **Information sharing:** Restrictions on information sharing between national authorities and between different

agencies (such as customs data, information on SARs and criminal records) creates a challenge in the detection of TBML.<sup>79</sup>

- **Export of food and agricultural products:** TBML schemes also involve the exploitation of agricultural products which is one of the main products that is exported from The Netherlands.<sup>79</sup>

### Modus operandi

- TBML involves a spectrum of deceptive tactics, including over-invoicing or under-invoicing, third-party payments, phantom shipments and multiple invoicing, which significantly challenge efforts to track the illegitimate sources of funds.
- These methods often utilise fabricated documentation, incorporate shell and front companies and collaborate with freight forwarders and customs brokers to facilitate trade constructions involving goods and services.<sup>79</sup>
- These manipulative practices create substantial hurdles in uncovering the illicit origins of money within international trade transactions.<sup>1</sup>

### Extent of the threat in The Netherlands

- Analysis of hacked encrypted communications shows that approximately 40% of criminal money is moved via forms of TBML.<sup>48</sup>

### Sources\*

1. *Expert input*
48. *Jaaroverzicht Criminele geldstromen 2022 – Openbaar Ministerie*
68. *National Risk Assessment Witwassen 2019 - WODC*
79. *Trade Based Money Laundering (2006) – FATF*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## Underground banking

### Description

- Underground banking, referred to as informal or parallel banking, operates without a permit outside regulated systems, constituting an illicit financial network. It enables cross-border fund transfers without transparency via informal value transfer systems.<sup>40</sup>
- While unregulated and deemed illegal in various countries like The Netherlands, underground banking serves both legitimate and illegitimate purposes, contrasting with the conventional financial system.
- Moreover, it intertwines cultural nuances, posing challenges in distinguishing lawful and unlawful transactions and complicating efforts to combat financial crimes.<sup>64,68</sup>

### Characteristics NL

- **International trade partner:** The Netherlands has strong economic ties with multiple countries which increases the need for fast and cross-border financial transactions. Underground banking could act as a solution for fast and cross-border financial transactions.<sup>1</sup>
- **Cultural diversity:** The Netherlands has a rich history of migration movements and as a result there is presence of a lot of diverse communities in The Netherlands. This provides a context in which relationships with countries abroad are close and informal value transfer networks, such

as hawala, can thrive, contributing to the possibility of underground banking.<sup>1</sup>

- **Information sharing:** Restrictions on information sharing between national authorities and between different agencies (such as customs data, information on SARs and criminal records) creates a challenge in the detection of underground banking.<sup>1</sup>

### Modus operandi

- Underground banking operates through unregistered money transfers within trust-based networks, avoiding regulatory scrutiny.
- Money brokers play a pivotal role in facilitating cross-border transactions, charging commissions for their services.<sup>1,64</sup>
- This structure employs various methods like hawala banking, misuse of cryptocurrencies, peer-to-peer platforms or unlicensed payment service providers, informal value transfers, cash trades and third-party payments to conceal funds' origins and destinations.
- This framework is exploited for various threats and predicate offences such as trade-based money laundering (TBML), laundering the proceeds of the drugs economy and sanctions evasion.<sup>64</sup>

### Extent of the threat in The Netherlands

- DNB received more reports about underground banking in the past year.<sup>61</sup>
- The police indicates underground banking has increased over time.<sup>61</sup>

### Sources\*

1. *Expert input*
40. *Underground Banking through Unregistered Money Services Businesses (2022) – Government of Canada*
61. *Aanhangsel van de Handelingen II, 2021/20, nr. 290. Tweede Kamer der Staten-Generaal*
64. *Enterprising criminals: Europe's fight against the global networks of financial and economic crime (2020) – Europol*
68. *National Risk Assessment Witwassen 2019 – WODC*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

## VAT fraud

### Description

- VAT (Value Added Tax) fraud is a complex financial crime that revolves around the manipulation or falsification of transactions associated with the collection and payment of VAT.
- It predominantly exploits the VAT rules for cross-border transactions, involving questionable business transactions where entities may fail to register, file tax returns or make the required tax payments.<sup>24,25</sup>

### Characteristics NL

- **International trade hub:** The Netherlands is an important hub for international trade, with numerous import and export activities. These extensive trading activities can increase the likelihood of VAT fraud occurring.<sup>24</sup>
- **Tax environment and financial infrastructure:** The Dutch tax system is quite complex with different schemes for tax credits and refunds. This complexity provides opportunities for fraudsters to exploit legal loopholes.<sup>68</sup>
- **Favourable business environment:** The Netherlands is home to numerous international companies and holding companies, which can lead to complex business structures that can be abused to commit VAT fraud.<sup>1</sup>

- **Membership European Union:** The Netherlands is a member of the European Union. VAT fraudsters often use different regimes between the EU member states to commit the fraud.<sup>1</sup>
- **Information sharing:** Restrictions on information sharing between national authorities and between different agencies (such as customs data, information on SARs and criminal records) creates a challenge in the detection of VAT fraud.<sup>1</sup>

### Modus operandi

- VAT fraud is considered a form of tax fraud, usually involving a VAT-registered business underreporting its sales and overreporting purchases.
- The general modus operandi for VAT fraud encompasses various tactics, including fictitious invoicing and the complex and deceptive technique known as carousel fraud.
- In carousel fraud, organised criminal networks engage in a circular movement of goods or services, involving multiple transactions designed to generate fraudulent VAT claims.
- Criminals manipulate this scheme to exploit gaps in the VAT collection process and undermine government revenue.<sup>25,68</sup>

### Extent of the threat in The Netherlands

- The VAT gap in the European Union in 2020 was €93 billion, which is 9.1% of the expected VAT revenues. For The Netherlands, the VAT gap in 2020 was €1.7 billion.<sup>38</sup>

### Sources\*

1. *Expert input*
2. *The Other Side of the Coin: An Analysis of Financial and Economic Crime (2023) – Europol*
24. *MTIC (Missing Trader Intra Community) fraud (2023) – Europol.*  
<https://www.europol.europa.eu/crime-areas/economic-crime/mtic-missing-trader-intra-community-fraud>
25. *VAT Fraud: Scope, Penalties, VAT Rights, and Report Procedure (2023) – Legend Financial*
38. *VAT gap in the EU (2023) – European Commission*
68. *National Risk Assessment Witwassen 2019 – WODC*

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

Assembled cluster of threats to cover the complete results of the desk research and workshops\*

Threat	Description
Alternative value transfer commodities	<ul style="list-style-type: none"> <li>The threat of alternative value transfer commodities is related to the use of non-traditional or unconventional items to transfer value and potentially engage in financial crime.</li> <li>These commodities can include goods (e.g. gold and grain), assets (e.g. art), or even digital items with inherent value, such as cryptocurrencies, digital currencies, virtual assets in online games or proceeds gained from online gambling. Criminal actors may exploit these commodities to obscure the origins and destinations of funds, potentially facilitating money laundering, tax evasion, or other illicit financial transactions. This exploitation may involve 'passing on' or 'shuffling' winnings in online gambling to further complicate the tracing process.</li> </ul> <p><b>Sources**</b>            1. Expert input            65. Trade-based money laundering: trends and developments (2022) – FATF            76. United States Department of the Treasury Financial Crimes Enforcement Network (2013) – ACAMS</p>
Cash-intensive business	<ul style="list-style-type: none"> <li>Cash-intensive businesses are vulnerable to criminal exploitation due to their reliance on substantial cash transactions as a core aspect in their operations.</li> <li>These businesses, such as casinos, jewellery stores, high-value good traders and cash-intensive retail operations are vulnerable to money laundering, tax evasion and fraud, as large volumes of physical currency flow through those businesses.</li> </ul> <p><b>Source</b>            77. Global Money Laundering &amp; Terrorist Financing Threat Assessment (2010) – FATF</p>
Cybercrime	<ul style="list-style-type: none"> <li>Cybercrime is a multifaceted financial crime threat encompassing any illegal activity employing a computer, either as the attacker's weapon or target.</li> <li>This threat spans a wide array of criminal activities, from phishing emails and identity theft affecting individuals to ransomware and denial-of-service (DoS) attacks targeting businesses and organisations.</li> </ul> <p><b>Source</b>            30. Internet organised crime threat assessment (2023) – Europol</p>
Fraud	<ul style="list-style-type: none"> <li>Fraud is an umbrella term for offences designed to deceive, resulting in the unlawful transfer of money, goods, or undue advantages. It encompasses a wide array of fraudulent schemes, including identity theft, Ponzi schemes, embezzlement, tax fraud, and insurance fraud.</li> <li>These activities can cause substantial financial losses to individuals, businesses, and financial institutions. It occurs both online and offline.</li> </ul> <p><b>Sources</b>            29. Illicit Financial flows from Cyber-enabled fraud (2023) – FATF            32. Fighting Fraud: Breaking the Chain (2022-2023) – Authority of the House of Lords</p>

\* 68 threats were not selected for elaboration at this stage, based on relevance, volume and extent. These threats are clustered into 11 overarching threats to include a baseline description of the threat.

\*\* A complete overview of the sources can be found in appendix I

## 6. Financial Crime Threat Assessment of The Netherlands 2023-24

Assembled cluster of threats to cover the complete results of the desk research and workshops\*

Threat	Description
High-risk industries	<ul style="list-style-type: none"> <li>This threat encompasses various sectors, including real estate, professional services and online marketplaces, that are vulnerable to financial crime. Criminals can exploit these sectors for money laundering, fraud and the movement of illicit funds.</li> <li>The international aspect and complexity of these industries, combined with the potential for anonymity and the possibility of large financial transactions creates opportunities for criminals. Furthermore, prices can be subjective and manipulated and transactions are often private.</li> </ul> <p><b>Source**</b> 66. High-Risk Industries for Money Laundering and Terrorist Financing (2020) – Sanctions.io</p>
Illegal smuggling and trade	<ul style="list-style-type: none"> <li>The threat of illegal trade and smuggling extends to a broad range of activities, including the illicit movement of goods and commodities across borders or within regions.</li> <li>This encompasses contraband goods, counterfeit products, human trafficking, drug smuggling, as well as the illegal trade in wildlife and plants. Financial crimes associated with this threat encompass money laundering, tax evasion, and the utilization of unregulated funds for criminal enterprises.</li> </ul> <p><b>Source</b> 47. Environmental Crime (2022) – Europol</p>
Money mules	<ul style="list-style-type: none"> <li>Money muling involves individuals known as money mules. These individuals, often recruited through cybercrime activities, receive funds from third parties into their bank accounts and then transfer it to another account (or the other way around) or convert it into cash.</li> <li>Money mules often earn a commission. While money mules may not directly engage in the criminal activities generating these funds, such as fraud, drug trafficking, or human trafficking, they play a crucial role as accomplices by laundering the proceeds of these crimes. In essence, money mules assist criminal organisations in maintaining anonymity while facilitating the global movement of illicit funds.</li> </ul> <p><b>Source</b> 31. Money Muling (2023) – Europol</p>

# 6. Financial Crime Threat Assessment of The Netherlands 2023-24

Assembled cluster of threats to cover the complete results of the desk research and workshops\*

Threat	Description
Non-compliance with regulations	<ul style="list-style-type: none"> <li>It involves individuals, organisations, or financial institutions failing to adhere to legal and regulatory requirements designed to prevent and detect financial crimes such as money laundering, fraud, tax evasion, and corruption.</li> <li>This threat compromises the integrity of the financial sector, allowing for the exploitation of vulnerabilities that can lead to illicit financial activities.</li> <li>Non-compliance may result from negligence, inadequate due diligence or a deliberate disregard for established regulations, making it challenging for authorities to uncover, prevent and detect financial crimes.</li> </ul> <p><b>Source**</b> 41. Partnering in the fight against financial crime (2022) – FATF</p>
Organised crime	<ul style="list-style-type: none"> <li>We speak of organised crime when groups that are primarily focused on illegal gain systematically commit crimes with serious consequences for society and are capable of these crimes in a relatively effective manner.</li> <li>Generally, organised criminal networks are involved in many different types of criminal activities spanning several countries. These activities may include trafficking in people, drugs, illicit goods and weapons, armed robbery, counterfeiting, and money laundering.</li> </ul> <p><b>Source</b> 54. Serious and organised crime threat assessment – EU SOCTA 2021 – Europol</p>
Service-based money laundering	<ul style="list-style-type: none"> <li>Service-based money laundering is a financial crime threat involving the exploitation of legitimate service providers to legitimise illicit funds. Service-based money laundering schemes rely on exploiting the trade in services or other intangibles to disguise and justify the movement of illicit proceeds.</li> <li>This threat often encompasses a wide range of services, including legal, financial, and consultancy services, which criminals use to launder the proceeds of various criminal activities.</li> </ul> <p><b>Source</b> 65. Trade-based money laundering: trends and developments (2020) – FATF</p>

# 7. Appendices





# 7. Appendix I

Overview of sources used to assess the selected threats and complement with additional information (1/4)\*

Sources for Financial Crime Threat Assessment of The Netherlands 2023-24							
1	Expert input	n.v.t.	2023	13	Veiligheid	NVB	2023
2	Arms trafficking (Global Initiative against Transnational Organised Crime)	Global Organised Crime Index	2023	14	Money Laundering vulnerabilities at PSP's	AMLC	2023
3	Criminality in The Netherlands	The Organised Crime Index	2023	15	Openbaar register (dnb.nl)	DNB	2023
4	Doing business honestly without corruption	Government.nl	2023	16	Veiligheidsagenda 2023-2026	Politie	2023
5	Corruption Perceptions Index	Transparency International	2023	17	Jaarplan	FEC	2023
6	The Other Side of the Coin: An Analysis of Financial and Economic Crime	Europol	2023	18	Global Slavery Index	Walk Free	2023
7	Politiewerk aan de horizon	Politie & Wetenschap	2023	19	Mensenhandel en (seksuele) Criminele uitbuiting (thema's)	CCV	2023
8	Drugs en Drugscriminaliteit (thema's)	CCV	2023	20	Criminal networks in EU ports	Europol	2023
9	'Douane onderschept fors meer cocaïne in 2023' <a href="https://www.rijksoverheid.nl/actueel/nieuws/2024/01/16/douane-onderschept-fors-meer-cocaine-in-2023">https://www.rijksoverheid.nl/actueel/nieuws/2024/01/16/douane-onderschept-fors-meer-cocaine-in-2023</a>	Rijksoverheid.nl	2024	21	Wat is betaalverzoekfraude?	Politie	2023
10	Anti-Money Laundering/Combating the Financing of Terrorism	IMF	2023	20	Six types of payment fraud—and how businesses can prevent them	Stripe	2023
11	Dreigingsbeeld Terrorisme Nederland	NCTV	2023	22	The State of Financial Crime 2023	ComplyAdvantage	2023
12	Tussen uitschakeling & inschakeling	WODC	2023	23	Aanpak belastingontwijking en belastingontduiking	Rijksoverheid	2023

# 7. Appendix I

Overview of sources used to assess the selected threats and complement with additional information (2/4)\*

Sources for Financial Crime Threat Assessment of The Netherlands 2023-24							
24	MTIC (Missing Trader Intra Community) fraud	Europol	2023	36	The Way of the Gun: Firearm trafficking and its impact on violence in The Netherlands	Universiteit Leiden	2022
25	VAT Fraud: Scope, Penalties, VAT Rights, and Report Procedure	Legend Financial	2023	37	Unmasking Control	IMF	2022
26	The Threat Assessment State-sponsored Actors	AIVD, MIVD en NCTV	2023	38	VAT gap in the EU	European Commission	2022
27	The State of Tax Justice	Tax Justice Network	2023	39	3 Most Widely Used Sanction Evasion Techniques	Regtech Times	2022
28	Tax Evasion	Transparency International	2023	40	Underground Banking through Unregistered Money Services Businesses	Government of Canada	2022
29	Illicit Financial Flows from Cyber-Enabled Fraud	FATF, Interpol & Egmont Group	2023	41	Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing	FATF	2022
30	Internet Organised Crime Assessment (IOCTA) 2023	Europol	2023	42	Environmental Crime in the age of climate change	Europol	2022
31	Money Muling	Europol	2023	43	Evaluatie PSD2	Soe Economisch onderzoek	2022
32	Fighting Fraud: Breaking the Chain	UK Parliament	2022-2023	44	Supranational Risk Assessment Report	European Commission	2022
33	Bijna 30 miljoen euro tegen drugssmokkel via mainports	Rijksoverheid.nl	2022	45	Vestigingsklimaat voor drugscriminaliteit in Nederland	WODC	2022
34	The Netherlands Country Financial Crime Dashboard	Financial Crime News	2022	46	Evaluatie Nederland	FATF	2022
35	The EU's priorities for the fight against serious and organised crime for EMPACT 2022-2024	Europol	2022	47	Environmental Crime	Europol	2022

# 7. Appendix I

Overview of sources used to assess the selected threats and complement with additional information (3/4)\*

Sources for Financial Crime Threat Assessment of The Netherlands 2023-24							
48	Jaaroverzicht Criminele geldstromen	Openbaar Ministerie	2022	60	Professional enablers of illicit financial flows and high-risk services and jurisdictions	Transparency International	2021
49	Kirgizië, Armenië, Turkije: via deze landen krijgt Rusland toch sanctieproducten	NOS.nl	2022	61	Aanhangsel van de Handelingen II, 2021/20, nr. 290.	Tweede Kamer der Staten-Generaal	2021
50	Confronting Fragmentation: How to Modernize the International Payment System	IMF	2022	62	Samen	A.B. Hoogenboom	2021
51	Jaaroverzicht 2022	FIU	2022	63	Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios	Bateman	2020
52	Global Estimates of Modern Slavery: Forced Labour and Forced Marriage	International Labour Organization	2022	64	Enterprising criminals: Europe's fight against the global networks of financial and economic crime	Europol	2020
53	Ethnically or racially motivated terrorism financing	FATF	2021	65	Trade-Based Money Laundering. Trends and Developments	FATF & Egmont Group	2020
54	Serious and Organised Crime Threat Assessment (SOCTA)	Europol	2021	66	High-Risk Industries for Money Laundering and Terrorist Financing	Sanctions.io	2020
55	Building Effective Beneficial Ownership Frameworks	OECD	2021	67	Criminaliteit en veiligheid in mainports	Fijnaut	2019
56	Dreigingsbeeld Milieucriminaliteit 2021	Rijksoverheid	2021	68	National Risk Assessment Witwassen	WODC	2019
57	Handhaven in het duister	Algemene Rekenkamer	2021	69	National Risk Assessment Terrorisme financiering	WODC	2019
58	Ending the Shell Game Cracking down on the Professionals who enable Tax and White-Collar Crimes	OECD	2021	70	Preventing and Detecting Sanctions Evasion Schemes	ACAMS Today	2019
59	The Role and Responsibilities of Gatekeepers in the Fight against Illicit Financial Flows: A Unifying Framework	World Economic Forum	2021	71	Concealment of Beneficial ownership	FATF	2018

## 7. Appendix I

Overview of sources used to assess the selected threats and complement with additional information (4/4)\*

Sources for Financial Crime Threat Assessment of The Netherlands 2023-24							
72	Fintechs in the payment system: the risk of foreclosure	ACM	2017	77	Global Money Laundering & Terrorist Financing Threat Assessment	FATF	2010
73	Nationaal Dreigingsbeeld	Politie	2017	78	Corruption	OECD	2007
74	Behind the Scenes. Beneficial ownership transparency in The Netherlands	Transparency International	2017	79	Trade Based Money Laundering	FATF	2006
75	Multiple Systems Estimation Slachtoffers Mensenhandel Nederland 2016 - 2019	WODC	2016	80	Identity fraud, tax evasion and money laundering vulnerabilities	OECD	2006
76	United States Department of the Treasury Financial Crimes Enforcement Network	ACAMS	2013				

## 7. Appendix II

### Sources for the identification of Dutch financial crime threats\*

Sources for Financial Crime Threat Assessment of The Netherlands 2023-24					
Dreigingsbeeld Terrorisme Nederland	NCTV	2023	Evaluatie Nederland	FATF	2022
Douane Jaarplan 2023	Douane	2023	Jaaroverzicht Criminele geldstromen	OM	2022
Cybersecuritybeeld Nederland	NCTV	2023	Het vestigingsklimaat voor drugscriminaliteit in Nederland	Universiteit Tilburg	2022
Internet Organised Crime Threat Assessment (IOCTA)	Europol	2023	Rapport Signalen fraude in de zorg 2021	Inspectie Gezondheidszorg en Jeugd	2021
The Other Side of the Coin: An Analysis of Financial and Economic Crime. European Financial and Economic Crime Threat Assessment 2023	Europol	2023	Dreigingsbeeld Milieucriminaliteit 2021	OM	2021
National Risk Assessment Witwassen	WODC	2023	Enterprising criminals: Europe's fight against the global networks of financial and economic crime	Europol	2020
Themarapportage economische dreigingen 2022	NCTV	2022	World Atlas of Illicit Flows	Interpol	2018
Veiligheidsagenda 2023-2026	Politie	2022	Risks Factors Guidelines	European Supervisory Authorities (EBA, ESMA en EIOPA)	2017
NRA terrorismefinanciering	WODC	2022	Nationaal dreigingsbeeld georganiseerde criminaliteit 2017	Politie	2017
Risico-indicatoren offshore vennootschappen	AMLC	2022	FATF Recommendations 2012	FATF	2017



**dutch  
banking  
association**

Gustav Mahlerplein 29-35  
1082 MS Amsterdam

[www.nvb.nl](http://www.nvb.nl)

**strong banks  
strong society**