dutch banking association

NL FCTA 2026

Financial Crime Threat Assessment of the Netherlands 2026

strong banks
strong society

Financial Crime Threat Assessment of the Netherlands 2026

Management summary

The Financial Crime Threat Assessment (FCTA) 2026 is a joint report that provides an update on current key financial crime threats in the Netherlands, offering a public overview and a confidential bank-specific translation of risks, red flags and actionable datapoints to support AML/CFT risk management.

Introduction

The FCTA 2026 results from the collaborative efforts of public and private partners – including Dutch Central Bank (De Nederlandsche Bank), Financial Intelligence Unit Netherlands (FIU-NL), Fiscal Information and Investigation Service (FIOD), National Police (NP), ABN AMRO, ASN Bank, ING, Rabobank, Triodos, Dutch Data Protection Authority (Autoriteit Persoonsgegevens), Public Prosecution Service (OM), Ministry of Finance, Ministry of Justice.
It was originally developed by the Dutch Banking Association (NVB) together with five banks to provide a sector-specific risk assessment. The work comprises an uplift of the previous FCTA that was published in 2024 [002, 003] and consists of two complementary documents:

- Financial Crime Threat Assessment of the Netherlands 2026 (NL FCTA) – a public overview of the current, relevant financial crime threats affecting the Netherlands; and
- Financial Crime Threat Assessment for banks 2026 (FCTA for banks) – a confidential, participant-only translation of selected threats into bank-visible risk factors, red flags and actionable datapoints that banks can consider in their individual risk management processes (e.g., SIRA updates, control prioritisation, risk coverage and risk-based deployment of resources).

The assessment provides a point-in-time view (Q4 2025–Q1 2026) banks can use to enhance their risk management processes; it is not a substitute for bank-specific risk assessments. Its primary objective is to inform and support banks in targeting AML/CFT controls, to focus capacity where it adds most value, to improve risk detection and reporting of unusual transactions.

Characteristics of the NL

The updated profile of the Dutch FinCrime landscape outlines geographic, socio-cultural, economic, financial and technological characteristics. Compared with the FCTA 2024 [002, 003], this edition emphasises heightened geopolitical tensions and expanded sanctions regimes, as well as increased throughput and complexity in main ports and bonded logistics. It also highlights accelerated digitalisation – including wider adoption of fintech, payment service providers and Virtual Asset Service Providers (VASPs).

Methodology

- The FCTA 2026 introduces a clear taxonomy and conceptual framework, developed for this edition to establish uniform terminology and a reusable structure that ensures clarity and comparability across analyses. This framework distinguishes between money laundering modi operandi categories, modi operandi, predicate offences and risk factors.
- The analysis consisted of multiple activities, combining open source research, Internal Risk Assessment Platform (IRAP) data and qualitative expert input to cross-check and validate findings. The analysis process:
  - started from the modi operandi categories;
  - identified specific modi operandi within each category and described their features;
  - determined the underlying predicate offences;
  - for the FCTA for banks, risk factors to which banks are exposed and those that may arise in banking processes were identified – these became the red flags;
  - red flags were quantified, mapped into datapoints and enriched with a data layer to identify high and low value areas, aiming to help banks strengthen their risk management.

Results of the NL FCTA

The NL FCTA resulted in 14 identified modi operandi categories. Each category is profiled in depth at national level, highlighting the extent of the threat in the Netherlands, modi operandi, features and underlying predicate offences:

1 Money laundering via cash.
2 Money laundering via gambling and/or (online) casinos.
3 Money laundering via high value goods and commodities.
4 Money laundering via illegal trafficking and transportation networks.
5 Money laundering via real estate and property transactions.
6 Money laundering via underground banking or via informal remittance systems.
7 Trade-based money laundering.
8 Money laundering via professional facilitators.
9 Money laundering via corporate and legal entity networks.
10 Money laundering via jurisdictional arbitrage.
11 Sanctions evasion.
12 Terrorism financing.
13 Money laundering via virtual assets.
14 Money laundering via securities investment products and capital markets.

Due to the sensitivity of the information, the detailed results in the following sections are only available in the participant-only FCTA for banks; to aid transparency, this report includes an aggregated, non-confidential summary that outlines what that document contains.

Selecting modi operandi categories for deep-dive

To determine the selection for the deep-dive refinement for modi operandi categories, the 14 identified modi operandi categories were scored on Exposure, Identifiability, Societal Impact and Knowledge & Detection need using an ordinal 1-5 scale. Aggregated scores and plenary discussion with public and private partners determined the selection for a specific deep-dive workshop. This resulted in a list of seven modi operandi categories. Selection or non-selection varies by category based on specific considerations (e.g. substantial prior work in FCTA 2024, scope ambiguity, forward-looking priority) and does not imply exclusion or lower relevance; non-selected categories may be revisited in future cycles. The detailed scoring documentation and rationale is attached to the FCTA for banks.

Results of the FCTA for banks

The following seven modi operandi categories were selected for further deep-dive – a targeted event combining expert presentations, breakout sessions and plenary discussion to assess the selected modi operandi categories in depth for the FCTA for banks:

8 Money laundering via professional facilitators.
9 Money laundering via corporate and legal entity networks [1].
10 Money laundering via jurisdictional arbitrage [1].
11 Sanctions evasion.
12 Terrorism financing.
13 Money laundering via virtual assets.
14 Money laundering via securities investment products and capital markets.

[1] Money laundering via corporate and legal entity networks and Money laundering via jurisdictional arbitrage are treated as a single combined modi operandi category for the purpose of the FCTA for banks analysis.

For each deep-dived modi operandi category, we identified structured descriptions of modi operandi categories, developed features, identified key underlying predicate offences and compiled bank-oriented risk factors covering identity and onboarding, jurisdiction, corporate structure, business purpose, payments, documentation and counterparties.

Red flags and datapoints

Risk factors were combined into red flag patterns and, where feasible, translated into concrete, bank-detectable datapoints to support monitoring, case triage and SIRA scenario development.

Role of banks in the ecosystem

During the development of both the NL FCTA and the FCTA for banks, the role of banks in addressing the identified financial crime threats was assessed within the wider AML/CFT ecosystem. It was recognised that banks have limited visibility of all relevant client activities. Achieving full insight into the remaining activities and channels that operate outside banks' line of sight would require disproportionate measures. Effective AML/CFT outcomes therefore depend on collaboration and information sharing with public authorities and other gatekeepers (e.g., PSPs, VASPs, trust offices and designated non-financial businesses and professions).

Responsibilities should be allocated proportionately across the ecosystem. Where activities primarily occur in non-bank channels or require capabilities or powers held by other gatekeepers or competent authorities (e.g., platform providers, VASPs, trust offices), banks should provide supporting signals visible in their data and respond to legal requests, while primary detection and intervention rest with the relevant party. Reliance and information sharing mechanisms (e.g., Article 75 AMLR [2] [277]) should enable this distribution. This assessment provides practical input for prioritising public-private collaboration, and banks' insights should be complemented by public sector intelligence and sectoral expertise. Targeted guidance and datasets – for example FIU/law enforcement case intelligence, customs/port trade data and supervisory direction – are needed to strengthen detection and remediation.

Synthesis and application

Within the FCTA, a risk mapping exercise and risk factor analysis have been conducted. These serve as an initial step to make the FCTA more data-driven by combining data sources with the methodology. This has been experienced as a useful setup leading to multiple interesting observations that the banks can expand on with more detailed data from their own population, including:

- Analysis identified several sectors that combine elevated risk scores with relatively low client counts across participating banks. Other sectors combine elevated risk scores with substantial client numbers. These sectoral observations can be used to inform proportionate, targeted approaches such as thematic reviews or case-level analyses. Given the wide variation in client numbers across sectors, focused monitoring may sometimes be more efficient than uniform controls.
- Most risk factors are specific to a particular MO category, so relatively few factors recur across the seven MO categories that we performed a deep-dive on.

[2] Article 75 AMLR allows obliged entities to rely on customer due diligence carried out by specified other obliged entities under defined conditions, enabling reliance and information sharing while the relying entity remains responsible for ensuring those conditions are met. See the AMLR text for full legal requirements and limitations.

Recommended next steps that follow from this synthesis and application include:

- It is for each individual bank to map the observations onto their own data to assess relevance to their individual portfolio. In addition, the outcomes can be mapped to their control framework to potentially identify low value areas, refine segmentation and to assess whether the inherent risks identified are adequately mitigated.
- Low value areas could be considered for simplified due diligence under a harmonised approach.
- The FCTA for banks provides a basis and opportunity to further analyse, at a later stage, the remaining seven modi operandi categories, incorporating the operationalisation of AMLR [277] under supervision of AMLA.

Reading guide

The Financial Crime Threat Assessment 2026 consists of two complementary documents. This reading guide explains how to use and navigate them, clarifies their differing accessibility, outlines links to related documents and publications and summarises key limitations and appropriate use.

Introduction
The Financial Crime Threat Assessment 2026 (hereinafter: FCTA 2026) is an uplift of the previous FCTA that was published in 2024 [3] [002, 003] and consists of two complementary documents:

- The Financial Crime Threat Assessment of the Netherlands 2026 (hereinafter: NL FCTA 2026).
- The Financial Crime Threat Assessment for banks 2026 (hereinafter: FCTA for banks 2026).

How to use the documents

- NL FCTA 2026 provides a structured overview of current, relevant financial crime threats in the Netherlands and sets the foundation for the FCTA for banks 2026.
- FCTA for banks 2026 selects specific threats for deep-dives, drawing on participants' experience and subject-matter knowledge [001]. Expert workshops and analysis of aggregated bank data are used to operationalise outcomes into risk factors, red flags and datapoints that banks can consider in their individual risk management processes (e.g., SIRA updates, control prioritisation and proportional deployment of resources).
- Read NL FCTA 2026 first to understand scope and national context. Use FCTA for banks 2026 to translate selected threats into bank-visible signals and practical focus areas.

What this document contains and how to navigate it
After the introduction, the uplifted 2026 methodology is presented, explaining the updated taxonomy and the combined quantitative/qualitative approach.

[3] The FCTA 2024 is listed in the sources and is fully embedded within this edition: its material has been retained and will be referenced throughout the report where relevant. Subsequent desk research and expert input have informed the additions and refinements included in the FCTA 2026; elements from 2024 judged no longer current have been updated or superseded and are explicitly cited.

A methodology tracker is included throughout to help the reader follow how substantiation of sources and definitions are applied per threat and how outputs are derived.
Both NL FCTA 2026 and FCTA for banks 2026 include the full methodology to ensure consistent interpretation across documents.

Accessibility
The NL FCTA 2026 is publicly accessible.
The FCTA for banks 2026 is only available to participating partners due to the confidentiality and sensitivity of its content.

Relation to other documents and publications
The updated source list (Appendix A) revises the previous assessment's list and adds 2024–2025 publications. We highlight two publications:

- National Risk Assessment (hereinafter: NRA) 2023 [174]. The output of the NRA is incorporated to understand the national threat landscape and to anchor country characteristics used in this assessment's scope and framing.
- De Nederlandsche Bank (Dutch Central Bank; hereinafter: DNB) SIRA Good Practices 2025: A concise comparative analysis of terminology and approach versus FCTA 2026 is provided (Appendix C) to highlight alignments and clarify differences in objectives.

Limitations and proper use
This assessment is non-scientific in design and does not seek formal statistical substantiation; it is based on publicly available information and expert input. It should not be used as stand-alone guidance to set internal risk priorities. Rather, it offers structured insight to support banks' own risk management processes. The content reflects a snapshot of the threat landscape in Q4 2025-Q1 2026 and is subject to change as threats evolve, regulatory expectations shift and new information emerges.

Additional limitations

- Coverage is indicative rather than exhaustive and should be read alongside institution-specific risk assessments.
- The analysis relies on publicly available sources and expert judgement that were not independently audited; despite validation, errors or omissions may remain.
- Aggregated inputs from participating banks may not represent the wider market and are unsuitable for inter-firm benchmarking.
- Threats, sanctions and regulatory frameworks evolve; risk factors and red flags require periodic review and recalibration.
- Elements of the methodology used Artificial Intelligence (hereinafter: AI)-assisted extraction and clustering; outputs were manually reviewed and cross-checked with participants, using professional judgement to mitigate misclassification and interpretation risk.
- Risk factors signal elevated risk but are not determinative and must be interpreted in context and calibrated to each bank's data and risk appetite.
- This document does not constitute legal advice or supervisory guidance and does not create rights or obligations; applicable law and regulation prevail.
- Any information sharing should occur only through authorised, lawful channels and in compliance with data protection and competition law requirements.
- The primary perspective is the Netherlands; domestic definitions and constraints apply.
- Content in the FCTA for banks is confidential to participating partners.

Legend for the references in the text
[0] source list (appendix A)
[0] footnote on page

Content

Introduction

Initiated after risk-based roundtables in 2023, the 2026 assessment builds on the FCTA 2024, reflecting ministerial support, and addresses banks' continued need for sector-specific risk assessment

Background and context

The first FCTA in 2024 was developed in response to the 2023 risk-based roundtables that were initiated by DNB. These roundtables catalysed sector-wide dialogue and led to industry baselines aimed at enhancing the proportionality and risk relevance of activities that banks perform in their gatekeeper role. Together, the roundtables and baselines signalled a collective step forward in refining the risk-based approach through public–private collaboration.

To meet banks' need for concrete, risk-focused guidance, the Dutch Banking Association (Nederlandse Vereniging van Banken, hereinafter: NVB) and five participating banks developed a joint FCTA 2024 for banks [003], underpinned by the NL FCTA 2024 [002], which consolidated publicly available sources and expert input. The objective was to help banks target Anti-Money Laundering (hereinafter: AML) and Countering the Financing of Terrorism (hereinafter: CFT) controls, focus capacity where it adds most value, and strengthen their gatekeeper role by improving the identifiability and reporting of unusual transactions.

In recent years, banks have consistently expressed the continuous need for enhanced guidance on Dutch-specific risks to enhance their Systematic Integrity Risk Assessments (hereinafter: SIRAs) and wider control frameworks. Furthermore, in a letter of May 2025 [143], the Minister of Finance informed Parliament about the importance of a consolidated overview of the financial crime risk landscape to enable an effective and efficient risk-based approach. In a letter to parliament, the FCTA was acknowledged as a best practice, as it provides sector-specific guidance for a risk-based approach.

Therefore, NVB and five participating banks decided to update their view on the threat landscape, building on the foundation set in 2024. For FCTA 2026, the approach:

- Broadens stakeholder involvement, with DNB, Fiscal Information and Investigation Service (Fiscale Inlichtingen- en Opsporingsdienst; hereinafter: FIOD), Financial Intelligence Unit – Netherlands (hereinafter: FIU-NL), National Police (hereinafter: NP), ABN AMRO, ASN Bank, ING Bank, Rabobank and Triodos Bank participating actively. Participants that were informed during the process include the Dutch Data Protection Authority (Autoriteit Persoons-gegevens; hereinafter: AP), Public Prosecution Service (Openbaar Ministerie; hereinafter: OM), Ministry of Justice and Security (Ministerie van Justitie en Veiligheid) and Ministry of Finance (Ministerie van Financiën).
- Introduces a uniform taxonomy that distinguishes categories of modus operandi, specific modi operandi, features and predicate offences.
- Applies a methodology combining quantitative analysis – including open source research and Internal Risk Assessment Platform (hereinafter: IRAP) data – and qualitative expert input to triangulate and validate findings.
- Helps banks strengthen their risk management by identifying red flags, relating data points and defining high and low value areas where possible.

This updated approach resulted in two documents:

NL FCTA 2026
Publicly accessible – published on NVB site

FCTA for banks 2026
Confidential – available upon request

Strategic objective

NL FCTA 2026

- The main objective of the NL FCTA 2026 is to provide an overview of the current, relevant financial crime threats in the Netherlands.
- The document serves as foundational input for the FCTA for banks.

FCTA for banks 2026

- Findings from the FCTA for banks 2026 can be integrated into the SIRA of individual banks, enhancing their AML/CFT control framework in a data-enabled manner.
- By using insights from the FCTA for banks 2026, banks can strengthen a risk-based approach, making it possible to implement more controls where necessary and less where possible, in alignment with objectives as outlined in the ministerial letter of May 2025 [143].
- Additionally, outcomes support effective allocation of resources, enabling capacity to be deployed in a risk-based manner.
- The FCTA for banks provides a clear sector view to inform ecosystem improvement, while the regulatory environment is developing under supervision and guidance of the European Union (hereinafter: EU) Anti-Money Laundering Authority (hereinafter: AMLA) – expected to commence supervisory and enforcement functions from July 2027 – and the Financial Action Task Force (hereinafter: FATF).

Participants FCTA 2026

Actively involved: DNB [4], FIU-NL, FIOD, NP ABN AMRO, ASN Bank, ING, Rabobank, Triodos
Observing: AP [4], OM [4], Ministry of Finance, Ministry of Justice.

Scope

- Definition: Financial crime refers to illegal acts committed by individuals or groups to obtain a financial or professional advantage and encompasses offences such as money-laundering, terrorist financing and sanctions evasion (FATF Glossary [091]; Europol [223], EMPACT 2022+ [88, 217].
- Geographic scope: the Netherlands, recognising international dimensions including cross-border activities.
- Institutional scope: Banks subject to the Anti-Money Laundering and Counter-Terrorist-Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme; hereinafter: Wwft) [278] and the Sanctions Law.
- Threat coverage: Threats affecting both natural persons and legal entities, and the related financial flows.
- Predicate offences: As listed in DIRECTIVE (EU) 2018/1673 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on combating money laundering by criminal law [276], supplemented by the predicate offences 'espionage' and 'sanction evasion' to ensure coverage on sanction- and espionage-related threats.
- Sources timeframe: Desk-research sources primarily span Q1 2020 to Q4 2025, with limited pre-2020 exceptions where still relevant.
- Perspective: Both the NL FCTA and the FCTA for banks are developed from the perspective of financial crime threats in relation to the characteristics of the Netherlands.
- Characteristics basis: Aligned with the WODC NRA 2023 [174] and supplemented by expert input. See next chapter for detailed elaboration of the Characteristics.

[4] Newly involved participants compared to the FCTA 2024.

Characteristics of the NL

The revised profile of the Dutch FinCrime landscape outlines geographic, socio-cultural, economic, financial and technological characteristics shaping exposure, with emphasis on current geopolitical dynamics, main ports and digitalisation relevant to AML/CFT risk.

Context

The profile of the Netherlands has been refreshed as a foundational element for understanding its exposure within the global financial ecosystem. The WODC NRA 2023 [174] is used as the primary reference for these characteristics, supplemented with recent developments.

The characteristics have been updated to put greater emphasis on geopolitical dynamics (including conflict-driven sanctions and rerouted supply chains), the Netherlands' role as an international trade and logistics hub (mainports, bonded facilities and multimodal connectivity) and ongoing digitalisation of the financial and payments landscape.

The consolidated, updated profile summarises the principal factors that collectively shape the Netherlands' financial crime exposure.

Geographic location

Strategic access and throughput: The Netherlands' strategic location, free movement within the Schengen/European Economic Area (hereinafter: EEA) and major sea- and airports make it a hub for certain types of crime, which brings along associated financial crime. Limited internal border controls and high volumes of cross-border goods and financial flows complicate asset tracing and monitoring, increasing the risk of misuse.

Geopolitical dynamics: Turbulent geopolitical dynamics drive retrograde globalisation and a rapidly changing global financial climate, increasing risks related to sanctions (including sanctions-related volatility amplified by ongoing conflicts, notably Ukraine and the Middle-East), fluctuations in the military-industrial complex, espionage and corruption. The Netherlands remains vulnerable as an international hub for related cross-border financial crime.

Demography and density: The high population density contributes to concentrated economic activity and transaction volumes that can be exploited for the placement and layering of illicit funds.

International financial hub

Strong financial sector: The Netherlands hosts a relatively large and internationally oriented banking sector where fully digital banks are rapidly emerging due to technological advancements. The recent establishment and internationalisation of AMLA is leading to greater harmonization and higher compliance requirements for banks.

Innovative payment methods: Alongside traditional banks, the Netherlands is home to a wide range of non-banking payment providers – including Payment Service Providers (hereinafter: PSPs), money transfer offices, trust companies and Crypto-Asset Service Providers (hereinafter: CASPs) – and there is widespread adoption of such services by individuals and businesses located throughout the EU. These entities can be attractive to criminals seeking to launder funds, and the proliferation of such varied providers fragments the payments landscape, making it harder to identify, trace and disrupt illicit money flows throughout the entire chain of involved parties.

Social and cultural environment

Tolerance: A culture of tolerance has contributed to the emergence of the drugs market, associated crime and related laundering pathways.

Political environment: Partly a social and cultural environment marked by polarisation, tolerance and a tradition of consensus, the Netherlands has a strong record of public–private collaboration to combat money laundering. A change of government in early 2026 may influence policy direction and enforcement priorities.

Digital and technological development

High digital adaption: Its advanced digital infrastructure and high internet connectivity have fuelled growth in online crime and faster digital value flows, creating drivers for money laundering. Rapid advances in artificial intelligence – where regulation on privacy and model validation is still catching up – further increased risk and underscore the need for validated, privacy-aware controls.

Economic environment

Trade hub: The Netherlands is characterised by an open, trade-oriented economy. As one of the world's most competitive economies – 18th largest economy in the world – and largest exporters, these features also make the country appealing to criminals seeking to launder illicit funds. Ongoing tariff discussions and trade-volatility increase economic vulnerability.

Economic warfare: The contemporary increase in economic warfare through e.g. trade conflicts and tariff imposition requires resilience in previously unforeseen scenarios.

Fiscal and corporate attractiveness: The Dutch tax climate is attractive to major foreign companies and has produced a significant presence of special-purpose and pass-through corporate entities. These structures and the international tax-planning ecosystem increase complexity and create concealment opportunities that can be misused for laundering illicit funds.

1
Methodology

Introduction

An updated, co-created methodology and unified taxonomy establish consistent threat elements, enabling like-for-like comparison and provides more actionable outputs for banks and public partners across the 2026 assessment. The conceptual framework visualises the different elements of the FCTA 2026.

Introducing the methodology

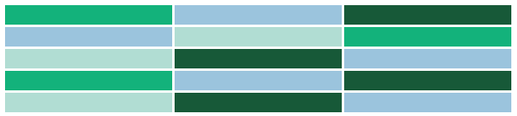
- Starting point is the methodology used in the NL FCTA 2024 [002] and the FCTA for banks 2024 [003].
- In September 2025, the previous methodology was evaluated and updated based on the received input from experts [001] and methodology testing.
- In line with the previous assessment, the FCTA 2026 uses quantitative and qualitative techniques and is developed in co-creation with experts from both public and private partners.
- Pertaining to the previous assessment, the FCTA 2026 introduces a new taxonomy that distinguishes the different elements of the threats.
- Furthermore, by using data supported activities we identify indications for high value and low value areas that banks can use to enhance their risk management processes.

Framework and taxonomy

During the FCTA 2024, Open source desk research identified a total of 88 threats containing predicate offences, modi operandi and risk factors of money laundering. This made like-for-like comparison and selecting threats difficult (‘comparing apples and oranges’).

To address this, the FCTA 2026 introduces a taxonomy and conceptual framework developed for this edition to establish uniform terminology and a reusable structure that ensures clarity and comparability across analyses. This framework distinguishes between modi operandi categories, modi operandi, predicate offence and risk factors. The process starts from the modus operandi categories, followed by identifying specific modi operandi within each category and describing its features, followed by determining underlying predicate offences. Additionally, in the FCTA for banks, we assess which risk factors banks are exposed to and which they could encounter in their bank processes— these become the red flags. By quantifying these red flags, identifying relating data points and adding a data layer, we aim to determine high and low value areas to help banks strengthen their risk management.

FCTA 2024



FCTA 2026

Modi operandi categories
Modi operandi
Predicate offences
Risk factors

Conceptual framework

The updated taxonomy resulted in a new conceptual framework where the relation between the elements of the FCTA 2026 is visualised.

Elements and description

Modi operandi categories: Broad overarching term to categorise ways or methods that can be used to launder illicit funds by transporting and/or concealing these funds, thereby disguising their origin or destination.

Modi operandi: A particular way or method used by organisations or individuals to launder illicit funds.

Features: Generic description of features and characteristics of the modi operandi – descriptive to specify for publicly available information (NL FCTA).

Predicate offences: Refers to the criminal activity that generated the illicit funds that are being laundered.

Risk factors: An observable characteristic or datapoint within banks in client activity or transactions that suggests the possible presence of a specific modus operandi associated with money laundering [5].

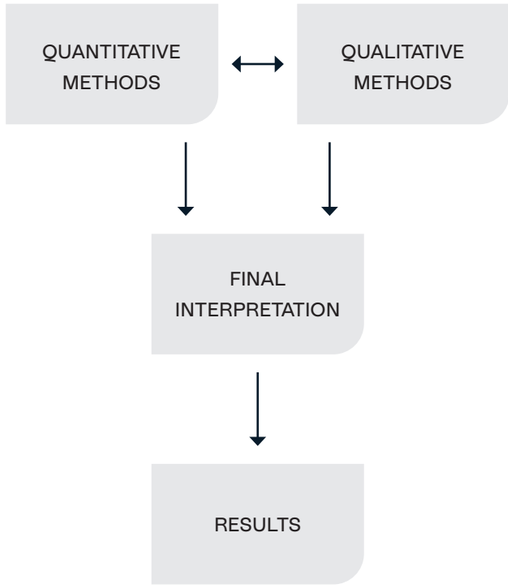
Red flags: A risk factor or combination of risk factors [5] that is/are associated with money laundering and that 1) banks are exposed to and 2) are identifiable for banks.

High and low value areas: Outlining of red flags such as client behaviour, sectors, products and segments, either individually or in combination, associated with the prioritised threat. Low value areas are areas where banks have limited scope to materially improve detection or disruption, whilst high value areas are areas where banks could potentially strengthen or introduce additional controls.

[5] Note that a single risk factor does not necessarily, by itself, constitute a risk or a red flag; risk factors should always be assessed in combination, since certain combinations are more likely to amount to a red flag. Banks should consider the relevant circumstances and decide how to use these signals in SIRA, models, scenario-planning, triage or investigative activities.

Design and approach

To compile the comprehensive overview of relevant threats following the conceptual framework, we use an approach combining quantitative and qualitative techniques. This approach is a form of methodological triangulation, meaning the quantitative and qualitative strands are deliberately used to cross-check, complement and integrate findings relating to the same threat. The methods and how they triangulate are outlined below.



Quantitative methods

Open source desk research: Systematic collection and review of public materials (reports, regulatory documents and industry publications).

AI-assisted analysis: Use of Mimir and large language model (LLM) tools for search augmentation and extraction to identify modi operandi, their risk factors and linked predicate offences; cluster related items; and remove duplicates.

Scoring methods: Application of numeric scores to measure Exposure (E), Identifiability (I), Societal Impact (SI) and Knowledge & Detection need (KDn) to select threats for further deep-dive in the FCTA for banks.

Data layering: Use of aggregated bank data to operationalise risk factors, test exposure and identifiability and link risk factors to observable datapoints.

Trend analysis: Analysis of aggregated bank data to identify trends and changes relevant to the threats.

Qualitative methods

Structured expert input: Public- and private-sector experts provide input through workshops and comment rounds on the taxonomy, categories, definitions, risk factors and red flags.

Heatmap: Synthesis of outputs into a heatmap highlighting relative exposure across threats.

Validation: Expert review to contextualise risk factors, confirm red flags, identify gaps and validate high and low value areas.

Final interpretation

The two strands are brought together to cross-check, complement and consolidate findings on each threat, creating a coherent view.

Results

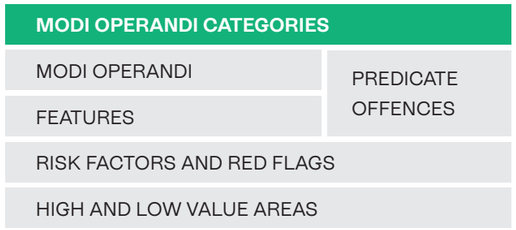
A reconciled and validated NL FCTA 2026.
A reconciled and validated FCTA for banks 2026.

Step-by-step

Foundational activities establish credibility: a curated source list, a reviewed set of MO categories and a consistent, EU-aligned predicate-offence list validated with subject-matter experts are the start activities of this FCTA. Using the source list, MO category list and predicate offence list, category-specific modi operandi and features were identified and each MO category was linked to its relevant predicate offences. After NL FCTA completion, insights informed selection of MO categories for deep-dives, followed by identifying risk factors and red flags and detectable datapoints for banks. Finally, the outcomes of the previous activities are combined and analysed to indicate potential high and low value areas. The results of steps 7 to 11 are only available in the FCTA for Banks.

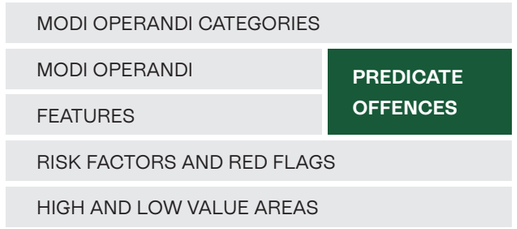
Step 1 Creating the source list

1 Started with previous source list of FCTA 2024 and verified whether each source cited has a newer version.
2 Supplemented the source list via OSINT by performing targeted open source searches for relevant publications from 2020 onwards; added only sources that clearly relate to the defined scope and add value.
3 Reassessed older sources by reviewing pre-2020 materials and retain only if clearly still relevant.
4 Classified purpose by tagging each source as primarily methodological (process/taxonomy) or primarily threat content (Modi Operandi/risk factors/typologies).
5 Performed qualitative review by assessing credibility, timeliness, relevance and any bias.
6 Record metadata and exclusion rationale: capture standard fields (ID, title, author/organisation, year, URL, classification, relevance note, date checked, reviewer) and document reasons for exclusions.
7 Finalised the source list at total of 560 sources (Appendix A, page 67).



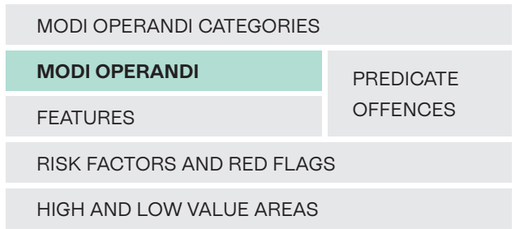
Step 2 Determine modi operandi categories

1 Formulated a definition of what a Modi Operandi Category (hereinafter: MO Category) is.
2 Conducted OSINT to develop the initial MO Category list.
3 Convened a subject-matter expert review session to confirm, adjust, expand, split and/or merge categories, producing a consolidated list of 14 categories.
4 Prepared a concise description and definition for each MO category.
5 Assessed each category to identify whether it is primarily used for transportation and/or for concealment of illicit funds (transportation = facilitates cross-border or physical/value transfer; concealment = obscures origin, ownership or transactional trail).
6 Validated the draft list by soliciting expert input during a workshop and incorporated their feedback.
7 Finalised the MO category list at total of 14 MO categories (Appendix D, page 74).



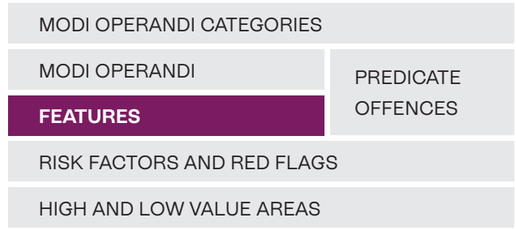
Step 3 Creating predicate offence list

1 Starting point was the Criminal offences list published in the DIRECTIVE (EU) 2018/1673 [557] as the primary reference.
2 Supplemented the list with 'Sanction evasion' and 'Espionage' to reflect the current Dutch financial crime landscape characteristics and subject-matter-expert input.
3 Prepared concise definitions for each predicate offence using legislative sources.
4 Circulated the draft list to subject-matter experts for review and incorporated agreed amendments.
5 Reviewed terminology for consistency and checked alignment with relevant domestic and EU legislation.
6 Finalised the predicate offence list at a total of 23 predicate offences (Appendix E, page 76).



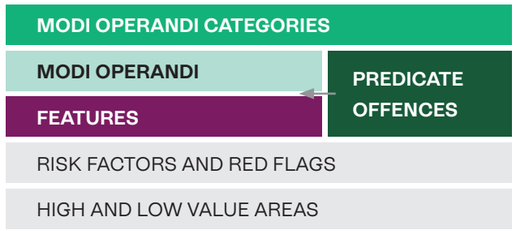
Step 4 Identifying modi operandi

1 Ingested the source list, MO categories and predicate offence list into Mimir, an Artificial Intelligence tool that supports search augmentation, entity extraction, classification and citation tracking.
2 Tasked Mimir to: identify all distinct modi operandi present in the sources; categorise the identified modi operandi to the defined MO categories with concise, objective evidence linking; identify the predicate offences related to each modus operandi with clear reasoning; extract salient features of the modi operandi; and provide source locations (page numbers or exact quotations).
3 Received an initial output listing 982 distinct modi operandi, divided over the 14 MO categories.
4 Performed extensive manual review by deleting errors and duplicates, consolidating modi operandi where possible, identifying gaps and performing manual desk research.
5 Engaged SMEs and participants for review and input.
6 Finalised the list of modi operandi, resulting in a total of 140 modi operandi.



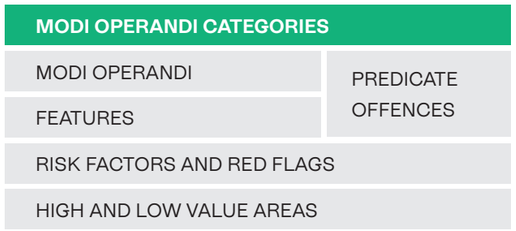
Step 5 Describing features

1 Identified, for every MO category, the main features using the risk factors extracted by Mimir.
2 Extensively reviewed manually the output by deleting errors and translating risk factors into generic description of features and characteristics of the modi operandi – descriptive to specify for publicly available information (NL FCTA).
3 Performed manual desk research to complete the features for each MO category.



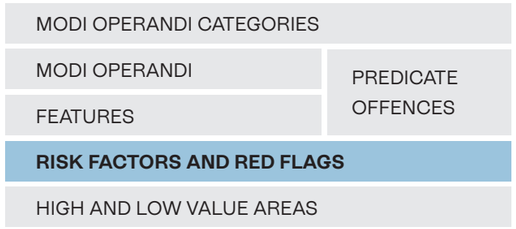
Step 6 Link predicate offences

1 Identified, for every MO category, the predicate offences linked to the associated modi operandi, using AI-assisted extraction (Mimir) followed by manual desk research.
2 Distinguished between 'proceeds-generating' offences – those that produce the criminal proceeds targeted for laundering – and 'enabling' offences – those that commonly facilitate the laundering process.
3 Highlighted, for each MO category, the three predicate offences that either generate the largest or most visible proceeds ('proceeds-generating') or commonly enable laundering ('enabling').
4 Provided the complete set of predicate offences that can be linked to each MO category.



Step 7 Selecting MO categories for deep-dive

1 To gain further insight in certain MO categories, the participants scored all categories using an ordinal scale of 1-5 (1=low, 5=high). The four scoring criteria are:
Exposure (E): How likely the banks in scope are exposed to this MO category;
Identifiability (I): How identifiable the MO category is using typical bank data and controls;
Societal impact (S): Impact on citizens, public trust, societal harm, and/or integrity financial system;
Knowledge and detection need (KDn): Extent to which additional knowledge or enhanced detection efforts are needed for this MO category.
2 The aggregated scores were used to determine if MO categories were directly selected or eliminated for deep-dive during this years' FCTA, or needed further discussion before deciding whether to select.
3 This resulted in a total of 7 MO categories that were selected for further deep-dive in the FCTA for banks 2026.



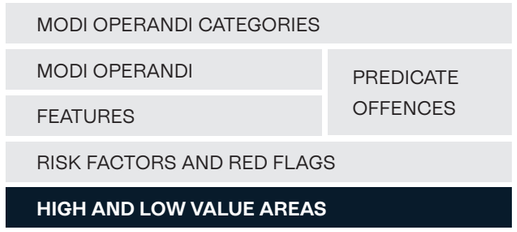
Step 8 Identify risk factors and red flags

1 Drafted an initial set of risk factors per MO category by synthesising extraction by Mimir with manual desk review.
2 Discussed and refined risk factors in deep-dive workshops.
3 Posed guiding questions to elicit expert input:
- Which risk factors or observations stand out most to you among those identified, and why?
- Do you recognise any of these risk factors from your own experience?
- Which risk factors do you not recognise and should be eliminated of the risk factors list?
- Are there specific combinations of risk factors that, in your experience, have alerted towards actual investigative cases?
- Which sectors and client segments do you consider most exposed to these risks, and why?

4 Resulted in a refined set of risk factors – organised into seven thematic categories –, a defined set of red flags (relevant and detectable for banks) and identified client sectors and segments informed by expert input. Note that a single risk factor does not necessarily, by itself, constitute a risk or a red flag; risk factors should always be assessed in combination, since certain combinations are more likely to amount to a red flag. Banks should consider the relevant circumstances and decide how to use these signals in SIRA, models, scenario-planning, triage or investigative activities.

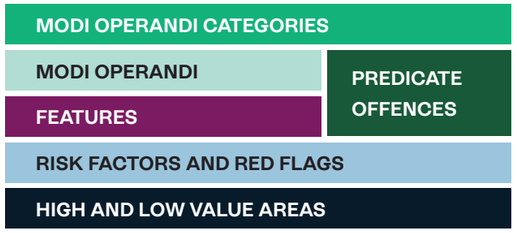
Step 9 Identify detectable datapoints

1 Distinguished between risk factors that can be used for automated detection or thematic analyses and ones that can be used during manual investigation.
2 To make the outcome of the FCTA more practical and concrete, we translated detection-oriented risk factors were translated into actionable datapoints for analysis, working with data experts from the banks. These datapoints are often proxies or operational measures used to detect a risk factor rather than one-to-one mappings.
3 Discussed how these risk factors and the related datapoints can be operationalised in the risk monitoring process, including best practices from the different banks.



Step 10 Identify high value and low value areas

1 Structured the qualitative expert input on risk factors, red flags, client segments and sectors and converted it into quantitative mappings.
2 Mapped red flags to sectors and client segments mentioned in IRAP data in a heatmap to highlight concentration and relevance.
3 Enriched the mapping with IRAP data for red flags, sectors and client segments.
4 Combined the heatmaps of all deep-dived MO categories to analyse for patterns and indications for high and low value areas.
5 Resulted high and low value areas to support or enhance control deployment (more where needed and less where possible).



Step 11 Manual analysis of risk factors for overarching themes and patterns

We performed a manual analysis to identify whether there are recurring risk factors across MO categories and if so, which risk factors recur most across the MO categories:
1 Create overview of all risk factors and red flags for the deep-dived MO categories.
2 Identify if there are recurring patterns within and across MO categories.

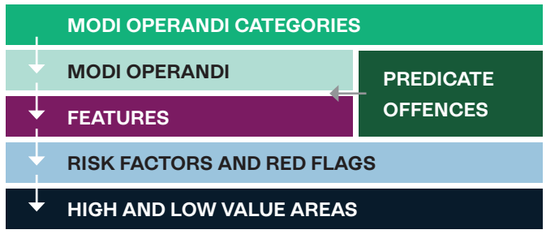
Content

The conceptual framework is used to provide a clear overview of the content and explains in which document the content is presented.

All MO categories (1-14)

Tab 2
Results of the NL FCTA
> pages 29-63

Selected MO categories (8-14)

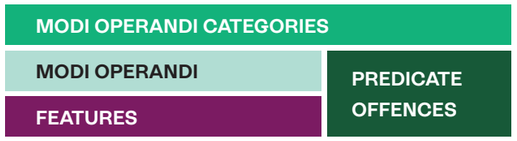


Results only available in the FCTA for banks

2 Results of the NL FCTA

MO categories NL FCTA

This chapter contains the 14 MO categories that were assessed in the NL FCTA.



MO categories

1 Money laundering via cash.
2 Money laundering via gambling and/or (online) casinos.
3 Money laundering via high value goods and commodities.
4 Money laundering via illegal trafficking and transportation networks.
5 Money laundering via real estate and property transactions.
6 Money laundering via underground banking or via informal remittance systems.
7 Trade-based money laundering.
8 Money laundering via professional facilitators
9 Money laundering via corporate and legal entity networks
10 Money laundering via jurisdictional arbitrage
11 Sanctions evasion
12 Terrorism financing
13 Money laundering via virtual assets
14 Money laundering via securities investment products and capital markets

Content

On the following pages, these MO categories are complemented with a description of the category, the extent of the threat in the Netherlands, the corresponding modi operandi, risk factors and predicate offences.

Description: A brief definition of the MO category that explains the core mechanisms and objectives of the behaviour being described.

Extent of the threat: A short, evidence-based snapshot of scale and impact in the Netherlands, drawing on recent publications (including, but not limited to, the recent NRA, FIU-NL and FIOD annual reports and other authoritative sources – e.g. AML Centre (hereinafter: AMLC)/FATF outputs – to describe SAR/UTR volumes, aggregate values or significant seizures and whether prevalence has increased or decreased compared with the FCTA 2024 baseline.

Modi operandi: A concise list of the principal ways and methods used by organisations or individuals to launder illicit funds.

Features: A generic description of features and characteristics of the modi operandi. The features should be read non-exhaustive.

Predicate offences: For each MO category, we distinguish between 'proceeds-generating' offences – those that produce the criminal proceeds targeted for laundering – and 'enabling' offences – those that commonly facilitate the laundering process. The three predicate offences judged most relevant (either because they generate the largest or most visible proceeds, or because they most frequently enable laundering) are highlighted, followed by the full set of associated predicate offences.

1 Money laundering via cash

MODI OPERANDI CATEGORIES

MODI OPERANDI

FEATURES

PREDICATE OFFENCES

Description

Money laundering via cash involves moving and concealing illicit proceeds through physical cash flows generated by individuals or businesses. Perpetrators blend or manipulate cash receipts to reduce transactional traceability and create the appearance of legitimate income. This exploits the limited electronic trail and weaknesses in cash handling to integrate unlawful funds into the formal financial system.

Extent of the threat in the Netherlands

- The WODC NRA (2023) ranks laundering via cash transactions/deposits at licensed banks among the Netherlands' largest money-laundering threats and records expert-estimated resilience of c. 64/100 – i.e. the threat persists despite existing mitigation [174].
- In 2024, reporting entities filed ≈3.5 million unusual transaction reports (UTRs). FIU-NL subsequently designated 118,408 transactions as suspicious (STRs) of which 10,432 had a cash characteristic as per FIU-NL categorization (noting that STRs may comprise multiple transactions and categories); the total value is concentrated in a few very large cases and high value dossiers are frequently linked to cash-based supply chains (drugs, labour-intensive sectors) and cross-border flows [134].
- Additionally, the Dutch Public Prosecution Service reported record cash seizures in 2024 (totalling €62,851,010) [135].
- Since the previous FCTA (2024) [002, 003] new cash-based modalities have amplified laundering risk. Authorities highlight the 'cash compensation model' (hereinafter: CCM), in which holders of surplus cash exchange it for giro (bank) funds via otherwise legitimate, labour-intensive organisations. Underground banking is frequently implicated in related schemes that rely on off-book value transfers [134, 146, 174].
- Concurrently, the proliferation of commercial/non-bank Automated Teller Machines (hereinafter: ATMs) and private cash-points (alongside roughly 5,000 bank ATMs) is flagged as a practical vulnerability that facilitates straightforward, high volume cash-to-account layering [273].

MODI OPERANDI

The principal modi operandi for this MO category include (non-exhaustive):

- Using cash-intensive businesses or business characteristics to disguise illicit cash as a legitimate income.
- Structuring/smurfing cash transactions to evade reporting thresholds.
- Depositing cash into bank accounts, often through intermediaries, money mules or complicit entities, to place cash into regulated financial systems.
- Holding onto or hiding of large cash sums originating from illicit activities.
- Withdrawing or loading cash via bank ATMs to convert deposits into physical cash.
- Exploiting white-label/third-party ATMs to withdraw, load and recycle cash with reduced traceability.
- Accepting or receiving cash payments of unknown or unexplained origin to place or integrate funds.
- Purchasing high value goods with cash to conceal proceeds and to integrate illicit proceeds.
- Paying workers in labour-intensive sectors in cash, often via subcontracting chains or informal payrolls, to evade taxes and integrate illicit funds.
- Replacing expected bank transfers or supplier payments with cash flows to substitute illicit cash for legitimate payment flows.
- Smuggling or physically transporting cash across borders and jurisdictions to evade reporting and controls.
- Converting cash into alternative value forms (prepaid instruments, crypto, vouchers or valuables) to obscure origin.
- Using (a variant of) the CCM: surplus illicit cash is exchanged for giro funds from labour-intensive firms that need cash (e.g., for off-book wages), with the swap disguised by false invoices/sham loans and (sub-)contracting chains, sometimes brokered for a commission.

FEATURES

Cash-intensive businesses often provide a ready front for laundering because they enable sales, wages and expenses to be settled outside electronic channels. Cash-based laundering therefore relies on moving, storing and gradually absorbing physical currency and cash-equivalent value into the legitimate economy, often in sectors where cash remains culturally or operationally embedded and economic flows are harder to reconstruct.

Structuring and smurfing are used to split value across locations, handlers and time periods to evade reporting thresholds. Perpetrators may deposit cash into bank accounts via intermediaries, money mules or complicit entities, withdraw and reload funds through ATMs (including third-party/private ATMs), or hoard and disperse sums across people and premises to delay detection and facilitate later placement.

Blending and substitution conceal illicit proceeds by mixing cash with legitimate takings or replacing expected non-cash payments. In CCM, it typically shows back-to-back giro 'compensation' for non-existent goods/services, generic or round-sum invoices without substantiation, absence of bank-paid wages despite labour-intensive activity and rapid pass-through via (sub) contractors or brokers.

Exploiting limited audit trails takes advantage of dispersed collection and pay-out points, weak record-keeping and the practical difficulties of verifying source and purpose. The physical nature of cash reduces traceability, increases opportunities for reconciliation gaps and weakens controls over provenance.

Conversion into alternative value forms and cross-border transport are used to further obscure origin: proceeds may be swapped into vouchers, prepaid instruments, crypto or valuables, used to purchase high value goods with cash, or physically carried across borders via common travel and trade routes. In essence, it turns physical currency and cash-equivalents into a flexible medium for placement, concealment and integration.

PREDICATE OFFENCES

As underlined in the FCTA 2024 [002, 003], drugs trafficking is a dominant proceeds-generating offence for laundering via cash since it generates sustained, high volume cash flows that are inherently suited to cash-based laundering; that is, wholesale drug sales and downstream distributions produce large sums that must be physically moved, concealed and integrated quickly into informal or formal channels [174, 182].

Human trafficking is another key proceeds-generating offence, yielding cash payments linked to labour and criminal exploitation, often settled off-books and channelled through cash-heavy operations (e.g. recruitment fees, transport and housing deductions). Those cash flows are readily laundered through placement in façade businesses, smurfing and cash swaps, with the added effect that reliance on cash hampers tracing and victim accounting [027, 252].

In the same vein, sexual exploitation is a primary proceeds-generating offence, producing substantial cash flows because payments for services, recruitment fees and related facilitation are frequently settled off-book in cash to avoid detection and to obscure victimisation. This creates immediate, unrecorded proceeds that require rapid placement and layering. Operators exploit cash-based mechanisms (e.g. short-term rentals, cash-intensive premises, informal labour) that lend themselves to smurfing, cash swaps and insertion through façade businesses [089, 027, 252].

Other predicate offences that could be linked to the modi operandi and risk factors of Money laundering via cash are: Arms trafficking; Corruption; Counterfeiting and piracy of products; Counterfeiting currency [6]; Extortion; Fraud; Kidnapping, Illegal restraint and hostage-taking; Organised crime; Smuggling; Tax crimes; and Trafficking in stolen goods.

[6] Counterfeiting currency: Although not highlighted as one of the three primary offences by aggregate value, counterfeiting currency is inherently cash-based and remains a notable predicate in the Dutch context; proceeds and distribution profits are often placed and layered using cash-intensive channels. We therefore flag it as a noteworthy linkage in addition to the principal offences listed.

2 Money laundering via gambling and/or (online) casinos

MODI OPERANDI CATEGORIES

MODI OPERANDI | PREDICATE OFFENCES

FEATURES

Description

Money laundering via gambling and/or (online) casinos involves deliberately using gambling services – including land-based and online casinos, betting sites, poker rooms and other gaming or gambling platforms – to launder illicit funds by converting cash or tainted balances into purported gambling winnings. The method exploits high transaction volumes, limited client verification and cross-border payment flows to integrate unlawful proceeds into the financial system.

Extent of the threat in the Netherlands

- The market's scale and professional dynamics amplify laundering opportunities. The Ksa reported roughly €600 million gross gaming revenue for licensed online operators in H1 2025 while independent estimates placed unlicensed operator turnover at about €617 million for H1 2025 (channelisation ≈49%) [166].
- Further, both the AMLC and Basel Institute identify large play volumes, junket/Vancouver-style schemes and mixing with crypto and real-estate as mechanisms that concentrate flows and facilitate placement and layering [163, 177].
- Since the FCTA 2024 [002, 003], the risk profile has changed but not disappeared, as player-protection measures introduced in late 2024 reduced average losses per account while the unlicensed market, fragmented payment rails and cross-border/virtual channels have persisted or expanded [166, 177].
- In 2024, ≈3.5 million unusual-transaction reports reached the FIU; 118,408 were treated as suspicious (STRs). Licensed online gambling operators filed roughly 30.5k unusual-transaction reports in 2024, of which the FIU declared about 3.6k as suspicious STRs – approximately 3.1% of the 118,408 STRs that year [134].
- The WODC's 2026 sectoral risk assessment finds that lotteries/and authorised slot-machine operations are assessed as low ML risk, but explicitly flags land-based sports betting as a non-low ML risk (notably for placement via smurfing) [171].

MODI OPERANDI

The principal modi operandi for this MO category include (non-exhaustive):

- Converting cash via (external) cash-in points or third-party top-ups before funds enter gambling accounts/e-wallets, followed by rapid buy-in/redemption cycles ('cash-in/cash-out') to present funds as winnings.
- Using casino or gambling accounts/platforms to layer illicit proceeds via third-party mules, payment intermediaries and cash centres.
- Using betting exchanges, peer-to-peer gambling platforms and cross-border online sites to move value through opaque counterparties.
- Using offshore or unregulated online casinos, casino-linked e-wallets, anonymous payment rails and crypto casinos to accept cash-converted funds, obscure origin, and move value rapidly across borders and chains.
- Facilitating junket [7], intermediary-led cross-border transfers and Hawala-style arrangements to deliver cash across jurisdictions that is subsequently laundered through casinos.
- Misusing VIP/high-roller accounts and loyalty programmes to deposit large sums, move money between casinos, and withdraw funds with minimal scrutiny.
- Using payment service providers (PSPs), e-wallets and intermediary payment rails to fund and withdraw from online gambling accounts, conduct minimal genuine play, and disguise illicit funds as legitimate gambling payouts.
- Purchasing another player's winnings, repaying their losses or colluding via intentional losses and coordinated bets to transfer value between players receiving repayment in clean funds.
- Converting alleged gambling proceeds into non-gaming assets (e.g. real estate, corporate investments, cryptocurrencies) to layer and integrate funds.
- Structuring/smurfing through multiple small deposits, bets, accounts or machines (including fixed-odds betting terminals) to avoid thresholds and refine cash.
- Exploiting employee collusion or internal manipulation to facilitate payouts, falsify records or bypass AML controls.

[7] A 'junket' is an intermediary-led arrangement used by casinos to attract and service high-value players (VIPs), often across borders.

FEATURES

Cash-in/cash-out schemes convert illegal funds into apparently legitimate winnings or account balances through immediate redemption and minimal genuine play; risk factors include rapid movement of balances, repeated buy-in/redemption cycles and use of multiple operators, terminals and payment options – including cross-border and online channels – to disguise origin.

Player-to-player transfers, purchased winnings, loyalty or VIP arrangements and third-party payment facilitators add distance between the original source and the ultimate cash-out; these mechanisms exploit differences between land-based and digital environments, and can be used alongside varied product types and settlement routes to mask the source of value.

Offshore and unregulated platforms, intermediated e-wallets and crypto-linked casinos further blur jurisdiction, counterparties and provenance by exploiting weaker verification standards, anonymous rails and rapid cross-border settlement, increasing opportunities to move value through opaque chains.

Overall, the sector's high turnover, product variety and frequent use of remote channels allow illicit value to be cycled through gaming ecosystems and re-emerge as plausible gambling proceeds or be converted into non-gaming assets.

PREDICATE OFFENCES

Drugs trafficking is a prominent proceeds-generating offence for money laundering via gambling and online casinos because drug networks generate sustained, high volume proceeds that are readily placed into casinos or gambling accounts (cash-in/cash-out, junkets, or coordinated player schemes) to achieve rapid placement and layering before integration into legitimate assets [163].

Proceeds from the sale of stolen items can likewise be channelled through gambling platforms or unlicensed online venues, making trafficking in stolen goods a relevant proceeds-generating offence. Operators may acquire or use existing websites and opaque payment rails to conceal transactions, then convert balances into purported 'winnings' and cash out to legitimise the criminal proceeds [163, 177].

Finally, cybercrime is an increasingly significant proceeds-generating offence for online gambling laundering because anonymity and diverse payment rails (prepaid cards, crypto, e-wallets) permit placement, layering and integration while complicating verification and traceability [163, 177].

Other predicate offences that could be linked to the modi operandi and risk factors of Money laundering gambling and/or (online) casinos are: Corruption; Extortion; Forgery; Fraud; Organised crime; Tax crimes; Terrorism; and Theft (and robbery).

3 Money laundering via high value goods and commodities

MODI OPERANDI CATEGORIES

MODI OPERANDI | PREDICATE OFFENCES

FEATURES

Description

Money laundering via high value goods and high value commodities involves converting proceeds into luxury goods, art, precious metals or vehicles to store and transfer value outside the banking system. These assets facilitate value movement, resale and price manipulation to obscure illicit origins [8].

Extent of the threat in the Netherlands

- The NRA classifies laundering via the sale, rental or lease of high value goods as a high risk threat and notes that dealers in high value goods (including vehicles) account for a large share of reported cases; it also flags that rental/operational-lease arrangements frequently fall outside Wwft [559] supervision, increasing abuse opportunities [174].
- Precious metals – especially gold – are repeatedly identified as practical, portable vehicles for value transfer and concealment; FIU-NL casework confirms seizures and cross-border movements of cash and precious-metal shipments linked to suspected illicit finance [058, 134].
- The art market is likewise an attractive but under-reported laundering channel, with FATF and WODC flagging provenance opacity, high single-item values and intermediaries as persistent risk factors [066, 153].
- The Financial Expertise Centrum (FEC) Jaarplan 2026 places luxury watches on its 2026 agenda via a dedicated public-private project, recognising their high value density and portability and the depth of secondary/grey markets that enable rapid cross-border resale and obscured provenance [136].

MODI OPERANDI

The principal modi operandi for this MO category include (non-exhaustive):

- Using trade, transport and smuggling of high value commodities (e.g., precious metals/stones, high-end electronics, high value timber) to park and move value, including falsified provenance and transport records.
- Purchasing, selling, renting or trading high value goods with cash, structured payments or falsified documents to conceal illicit origins and integrate proceeds.
- Manipulating provenance and valuations by colluding with/corrupting industry professionals to hide, move or legitimise illicit funds through art, antiquities and cultural objects.
- Using compensation, barter or non-monetary exchange schemes involving high value goods or commodities to disguise illicit payments and transfer value.
- Structuring, mis-invoicing or otherwise manipulating high value goods transactions (sales/transfers) to obscure the source, amount or destination of illicit funds.
- Using refiners, smelters, recyclers and manufacturing processes to rebrand, commingle or transform illicit commodities into seemingly legitimate product.
- Using online marketplaces, intermediary platforms, NFTs and other digital channels to trade, fractionalise or monetise high value items and obscure origin or ownership.

[8] Scope note: this MO category covers portable, high value, low-bulk assets and markets with subjective provenance/valuation (e.g., art and antiquities, precious metals and stones, jewellery, luxury vehicles/yachts and certain high value timber/collectibles). General commodity trade and value transfer embedded in trade documentation are out of scope and covered in 7 Trade-based money laundering; misuse of logistics chains to move contraband sits under 4 Illegal trafficking and transportation networks.

FEATURES

Trade, transport and smuggling of high value goods and commodities – including precious metals (notably gold), gemstones and jewellery, fine art and antiques, luxury vehicles and yachts, timber and certain agricultural products – often leverage subjective valuations, provenance uncertainty and specialised custody or storage (bonded facilities, freeports) to complicate scrutiny and move value across borders.

Purchasing, selling, renting or trading high value goods with cash, staged or split payments, third-party settlement and cross-border sourcing or disposal conceals illicit origins. Barter, compensation and other non-monetary exchanges can likewise transfer value without an obvious payment trail and further dilute links to the original source.

Manipulating provenance and valuations by colluding with or corrupting industry professionals, falsifying trade or transport documents, mis-invoicing or otherwise structuring transactions is used to hide, move or legitimise illicit funds, while refiners, smelters, recyclers and manufacturing processes can rebrand, commingle or transform commodities into products with altered identity and paperwork. Online marketplaces, intermediary platforms, tokenisation and NFTs add scale and ambiguity by enabling trading, fractionalisation and monetisation that obscure origin or ownership.

In combination, these features create flexible pathways to park, move and legitimise value, using market practices and documentation to provide a plausible commercial narrative while diluting links to original sources and facilitating eventual conversion into apparently legitimate holdings.

PREDICATE OFFENCES

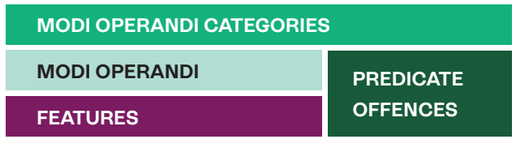
Within markets for high value goods and cross-border commodity trade, drugs trafficking serves as a frontline proceeds-generating offence because large, sustained cash flows from wholesale narcotics sales are often converted into tangible, high value items (precious metals, luxury goods, vehicles) or channelled into trade transactions that mask the origin of funds. Criminal networks exploit commodity markets, complicit intermediaries and TBML techniques to integrate drug proceeds into legitimate trade, obscure provenance and move value across borders [153, 256].

Environmental crime (notably illegal mining, unauthorised logging and illicit extraction) is likewise a proceeds-generating offence amenable to laundering through commodity chains. Illegally extracted gold, timber or minerals are channelled via informal buyers, storage facilities or freeports, mis-documented or blended with legitimate consignments and sold into global markets, with corporate actors and armed groups (including terrorist affiliates in some contexts) exploiting these supply chains to monetise resources and launder revenues using trade-based and transshipment methods [124, 156].

Fraud can be regarded a common enabling offence. Criminals exploit international trade complexity (over- and under-invoicing, multiple invoicing, false descriptions, fictitious shipments) to convert illicit cash into apparently legitimate trade receipts or cross-border payments in markets where price volatility and opaque pricing hide mismatches between contract documents and actual economic flows [036, 109].

Other predicate offences that could be linked to the modi operandi and risk factors of Money laundering via high value goods and commodities are: Arms trafficking; Corruption; Counterfeiting and piracy of products; Cybercrime; Forgery; Organised crime; Smuggling; Tax crimes; Terrorism; Theft (and robbery); and Trafficking in stolen goods.

4 Money laundering via illegal trafficking and transportation networks



Description

Money laundering via illegal trafficking and transportation networks involves integrating proceeds from criminal activity into logistics and transport routes to conceal their origins. Criminal networks exploit transshipment points, corrupt officials and cash couriers to move value both physically and electronically. In the Dutch context, main ports – notably the Port of Rotterdam and Amsterdam Airport Schiphol – can be exploited as high volume transshipment and storage hubs. Bonded warehouses, free-zones, containerised flows and multimodal connections create opportunities to commingle illicit consignments with legitimate cargo, obscure provenance and facilitate onward movement through complex supply chains.

Extent of the threat in the Netherlands

- As mentioned in the NL FCTA 2024 [002, 003], laundering embedded in trafficking and transport networks is not the numerically largest reporting category, yet single networks can move very large sums and therefore create disproportionate systemic and economic risk [134, 174].
- Echoing the NL FCTA 2024 [002, 003], the NRA notes that the country's major gateways – notably the Port of Rotterdam and Schiphol – are attractive exploitation points; their huge cargo volumes, multimodal flows and bonded/free-zone facilities enable illicit consignments to be concealed and commingled with legitimate trade [134, 174].
- Since the previous FCTA [002, 003], there have been reports of growing sophistication and hybridisation – criminals increasingly combine TBML, underground banking, third-party payments and crypto on/off-ramps inside logistics chains [134, 174].
- The FATF adds that, in the context of migrant smuggling, this hybridisation goes hand-in-hand with greater use of hawala, cash couriers and professional laundering networks, plus social-media coordination [154].

MODI OPERANDI

The principal modi operandi for this MO category include (non-exhaustive):

- Exploiting logistics hubs and lax border controls by concealing illicit goods within legitimate cargo and using trade-based manipulation to smuggle goods, arms, people and wildlife and to launder proceeds.
- Transporting bulk cash and high value commodities (precious metals, stones, jewellery) across borders to move and layer proceeds.
- Using online platforms and social media to coordinate trafficking, advertise illicit goods and facilitate payments and value transfers (including darknet and e-commerce channels).
- Facilitating migrant smuggling and human trafficking to generate proceeds and moving funds via informal value-transfer systems (hawala), cash couriers and segmented remittances.
- Establishing offshore structures, front companies and abusing trade-based and professional services to conceal ownership and legitimise proceeds.
- Exploiting corruption and collusion among customs, port and logistics personnel (bribery, circumventing controls, insider facilitation) to circumvent controls.
- Abusing postal, courier and parcel services by concealing contraband and using small-parcel routing to evade detection and to move proceeds.
- Abusing vehicles and transport assets by purchasing, leasing or renting luxury vehicles, yachts or commercial transport to integrate proceeds, move goods and obscure value chains.

FEATURES

Exploiting logistics hubs and lax border controls by concealing illicit goods within legitimate cargo exploits the movement of goods (narcotics, firearms, illicit timber, counterfeit luxury goods), people (migrant smuggling, trafficking in persons) and other contraband (wildlife, illicit cigarettes, fuel) across logistics chains. Criminal actors use the scale and complexity of ports, airports and freight corridors to hide, commingle or misdescribe shipments, often exploiting corrupt practices such as bribery of port, customs and logistics personnel and compromised inspection procedures.

Abusing multimodal routing, bonded or free-zone storage and parcel/courier networks introduces staging points that complicate provenance and destination checks: sea, air, road and rail movements, trans shipment hubs and high volume small-parcel routing all increase opportunities to evade oversight and move contraband or proceeds across jurisdictions.

Using online platforms and ancillary logistics services supports coordination, advertising and payment for illicit trade, while freight forwarding, brokerage, warehousing and handling can be misused to create documentation, enable mis-invoicing and provide operational cover.

Transporting bulk cash and high value commodities across borders, using the same transport infrastructures that carry goods to move cash, valuables or digital value, result in hybrid models where physical logistics and financial flows reinforce one another to obscure origin, ownership and purpose.

PREDICATE OFFENCES

Drugs trafficking – Synthetic-drug and opioid networks in particular – generate very large, rapidly renewable cashflows that are tightly embedded in trafficking and transport infrastructures (couriers, parcel routes and maritime supply chains). Proceeds are routinely placed, layered and moved along those same logistic corridors – by cash couriers and informal value-transfer systems, via trade-based manipulations and through front companies – so that the transport networks that carry product also enable the movement and concealment of funds [073, 127].

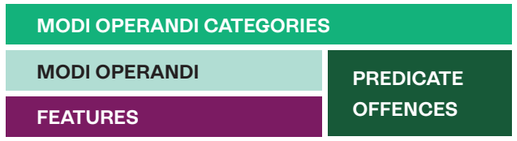
Counterfeiting and piracy of products likewise generate substantial tradable proceeds and depend on transport and logistics chains, making them both a proceeds-generating and an enabling offence. Operators exploit the same courier, parcel and container routes used by other contraband, using fraudulent descriptions, split shipments, low value HS codes and front import/export firms to commingle illicit proceeds with legitimate trade and move value across jurisdictions via formal and informal financial conduits [127].

Further, in recent years, environmental crime – notably illegal logging and illegal wildlife trafficking – has emerged as a notable transport-centred proceeds-generating offence. Protected flora and fauna and related products are concealed in parcels and specialist consignments for exotic-pet and collector markets overseas and proceeds are channelled through the same informal and formal financial conduits that service transportation networks [127, 129, 156].

Other predicate offences that could be linked to the modi operandi and risk factors of Money laundering via illegal trafficking and transportation networks are: Arms trafficking; Corruption [9]; Cybercrime; Human trafficking; Organised crime; Piracy; Sexual exploitation; Smuggling; and Trafficking in stolen goods.

[9] Corruption: Although not highlighted as one of the three primary offences, corruption – including bribery of port, customs and logistics personnel, facilitation payments and the compromise of inspection procedures – is a critical enabling offence for trafficking- and transport-centred laundering. Corrupt practices can permit misdeclared shipments, clandestine transshipments and the abuse of bonded or free-zone facilities to proceed with reduced scrutiny, while also enabling the manufacture of false documentation and the deliberate diversion of goods and value into opaque payment and settlement chains. We therefore flag it as a noteworthy linkage in addition to the principal offences listed.

5 Money laundering via real estate and property transactions



Description

Money laundering via real estate and property transactions involves purchasing, developing or selling property – including both commercial and non-commercial real estate – to integrate illicit funds, often through over- or under-valuation, nominee buyers, mortgage fraud or rapid resale schemes. Real estate provides a high value, durable asset class that can absorb and legitimise large sums.

Extent of the threat in the Netherlands

- The NRA flags real-estate transactions as a high-impact laundering channel, often using ABC-deals, loan-back constructions and professional intermediaries to hide provenance and beneficial ownership [174].
- Real estate property-linked laundering has clear social and financial effects – it distorts the housing market, increases credit and reputational risk for banks and leads to high value seizures in major cases (e.g. Klimop case) [103, 253].
- Yet, as noted in the FCTA 2024 [002, 003], prosecutions of notaries and real-estate professionals remain limited when measured against the scale of registrations. Reflecting this gap between harm and enforcement, the FIU logged ≈3.5 million unusual-transaction reports in 2024, with 118,408 ultimately classified as suspicious (STRs). The FIU's figures show just 155 unusual transaction reports from real-estate professionals (submitted by 74 firms), only 12 of which were declared suspicious roughly 0.01% of the year's 118,408 STRs [134].
- Investigative reporting indicates that, since 2023, drug networks nationwide have moved into mortgage fraud as an easier, lower risk laundering model [074].
- Further, FATF warns real-estate laundering is increasingly combined with trade-based and service-based techniques, underground banking and virtual asset on/off-ramps, so detection and mitigation must adapt to more cross-border, tech-enabled and layered schemes [116].

MODI OPERANDI

The principal modi operandi for this MO category include (non-exhaustive):

- Converting illicit proceeds into real estate property to store and disguise value.
- Manipulating valuations and using ABC/back-to-back/loan-back schemes and opaque intermediaries to disguise illicit flows via real estate property.
- Acquiring real estate property using nominees, proxies, straw purchasers or opaque offshore corporate structures (including front businesses and escrow misuse) so the beneficial owner is obscured and proceeds can be held or integrated.
- Purchasing and redeveloping real estate property, including large developments and investor-migration/residency schemes, to integrate illicit funds.
- Exploiting coerced or forced real estate property transfers and undervalued disposals to launder proceeds.
- Exploiting weak or negligent due diligence and undisclosed cash flows in real estate property transactions to obscure source, destination and ownership.
- Obtaining mortgages/finance with falsified documents or using paper/legal technicalities to mask ownership.
- Transacting in real estate property linked to sanctioned, high risk or high profile persons/entities to move or disguise illicit funds.
- Purchasing of foreign or target-jurisdiction real estate property to distance the origin of funds.
- Using rental payments or letting arrangements, including cash rents, phantom tenants and short-let income, to launder proceeds.
- Flipping properties via rapid consecutive sales at manipulated prices to move funds and legitimise illicit proceeds.
- Corrupting or exploiting real-estate gatekeepers and professionals (e.g. agents, valuers, notaries, lenders) to facilitate laundering.

FEATURES

Converting illicit proceeds into real estate property to store and disguise value offers a durable vehicle to absorb large sums. Purchases are frequently funded from mixed or opaque sources, include cross-border acquisitions and purchases in target jurisdictions to distance origin, and can involve sanctioned or high risk parties to move or obscure funds.

Manipulating valuations and using ABC, back-to-back or loan-back schemes and opaque intermediaries to disguise flows enables rapid resales (flipping) at manipulated prices, staged or split payments and development or refurbishment projects that create substantial, hard-to-reconcile payment streams. Obtaining mortgages or finance with falsified documents and exploiting undervalued disposals or coerced transfers further facilitate layering.

Acquisitions by PEPs and connected parties, unexplained-wealth signals relative to declared income and the use of gifts/loan-backs, trusts/foundations/STAKs, escrow arrangements and nominee buyers are recurrent techniques to disguise beneficial ownership and conceal bribery proceeds and undue influence.

Acquiring property using nominees, proxies, straw purchasers or opaque offshore corporate structures separates legal title from beneficial ownership: front companies, escrow misuse and professional intermediaries (agents, valuers, notaries, lenders) are used to obscure the true controller and legitimise proceeds, while weak or negligent due diligence increases vulnerability.

Using rental payments, short-let income, phantom tenants and letting arrangements to launder proceeds provides a steady integration path. Purchasing and redeveloping property, portfolio-building and investor-migration/residency schemes can convert illicit funds into ongoing legitimate cashflows, often aided by corrupt or complicit real-estate gatekeepers.

Collectively, these features enable illicit proceeds to be converted, layered and ultimately integrated into seemingly ordinary property markets, with potential distortionary effects on pricing and availability.

PREDICATE OFFENCES

Drugs trafficking merits particular emphasis as a primary proceeds-generating offence for real estate property laundering because it typically generates sustained, high volume cash flows that require fast and reliable concealment. Drug proceeds are frequently channelled through cash-intensive brokerage systems and special-purpose vehicles, and invested in hotels, apartment blocks, retail centres and commercial developments. These structures enable rapid placement, layering and integration via large lump-sum investments, intermediaries and manipulated valuations [161, 247].

Fraud likewise operates as both a key enabling and proceeds-generating offence. Falsified income statements, forged documents and mortgage-application fraud allow criminals to place and integrate illicit proceeds into property markets. By using fabricated pay-slips, inflated accounts or sham corporate invoices to secure mortgages, loans or large cash purchases, they conceal the funds' criminal origin and create a seemingly legitimate paper trail when properties are later sold or rented [103, 109, 116, 247].

Corruption (including bribery and embezzlement) is a core proceeds-generating and enabling offence for real-estate laundering. Misappropriated public funds and kickbacks are commonly channeled into domestic and offshore property through opaque vehicles, nominee purchasers and proxies. High value acquisitions by politically exposed persons (PEPs) and connected parties convert illicit payments into tangible, appreciating assets that are difficult to trace and that can conceal and perpetuate undue influence [116, 161, 247].

Other predicate offences that could be linked to the modi operandi and risk factors of Money laundering via real estate and property transactions are: Arms trafficking; Cybercrime; Extortion; Forgery; Human trafficking; Insider trading & market manipulation; Organised crime; Smuggling; Tax crimes; Terrorism; Theft (and robbery); and Trafficking in stolen goods.

6 Money laundering via underground banking or via informal remittance systems

MODI OPERANDI CATEGORIES

MODI OPERANDI

FEATURES

PREDICATE OFFENCES

Description

Money laundering via underground banking or via informal remittance systems involves using trust-based, non-bank remittance networks to transfer value without formal banking records. These systems rely on informal settlement and minimal documentation, enabling fast cross-border movement and evasion of surveillance.

Extent of the threat in the Netherlands

- Underground banking and informal remittance systems operate in the Netherlands, used in specific migrant/diaspora corridors and cash-intensive sectors. Their scale is hard to quantify; they constitute a relatively small share of detected ML cases and are seldom visible to banks but can still pose significant threats in certain contexts. The NRA ranks 'criminal underground/ hawala banking' as a top single-issue threat (RPI score 42, i.e. high impact with weak mitigants) [174].
- In 2024, the FIU handled ≈3.5 million unusual-transaction reports and identified 118,408 as suspicious (STRs). The FIU's 2024 figures show 80 files containing indications of underground banking, covering 833 executed transactions – c. 0.7% of the STRs that year. FIU analyses indicate this mechanism has been used to supply terrorist groups with weapons and/or funds [134].
- RIEC casework shows these networks materially facilitate international drug and illicit goods flows – for example narcotics, human trafficking, firearms, contraband cigarettes, counterfeit luxury goods and illicit precious metals – and large cash movements, making them an urgent enforcement priority because they enable high value criminal markets and obscure money trails [146].
- Since the FCTA 2024 [002, 003], the threat has evolved rather than grown explosively. Networks have greater international reach, higher transaction velocity, wider use of hybrid techniques (business structures/TBML, crypto on/off-ramps) and younger operators increasingly combine banking and drug-market roles [243].

MODI OPERANDI

The principal modi operandi for this MO category include (non-exhaustive):

- Using trust-based broker networks to transfer value without physical cross-border movement (Hawala/hundi-style).
- Using unlicensed remittance agents, street exchangers and cash couriers to conduct rapid cross-border transfers and currency swaps.
- Using formal bank accounts and regulated channels in combination with Informal Value Transfer Systems (hereinafter: IVTS) to integrate or move proceeds (hybrid layering).
- Using encrypted communications, smartphone apps and tokenisation to coordinate transfers and reduce traceability of operational steps.
- Converting between cash, crypto and other stores of value (e.g. luxury goods, vouchers) within informal networks and reconverting to fiat to move or store value.
- Using cryptocurrency mixers/tumblers, privacy coins and decentralised peer-to-peer exchanges (P2P) to move illicit funds within underground banking systems via cryptocurrencies.
- Using cash compensation to transfer illicit cash via underground banker to parties that require cash and into the regulated financial system.
- Using trade-based methods to settle the balance between correspondent underground bankers.
- Using third-party/money mule payments or accounts for 'pass-through' activities to obscure the origin of funds, conceal the involvement of certain parties and complicate detection.
- Using prepaid/open-loop cards, vouchers and semi-anonymous payment instruments to load, move and withdraw value across jurisdictions.
- Using transaction splitting/structuring across multiple informal channels and low-value transfers to avoid reporting thresholds and detection.
- Using stash locations, coordinated cash-pools and designated couriers/staff to aggregate, store and distribute bulk cash within IVTS network.

FEATURES

Trust-based broker networks (Hawala/hundi-style) operate on trust, reputation and obligations rather than formal contracts or records. They typically feature cash pools, brokers and family or community ties that match senders and receivers across borders without physically moving funds.

Unlicensed remittance agents, exchangers and cash couriers settle balances through offsetting flows, trade, valuables or third-party payments and operate alongside legitimate remittances; simple records, coded communications and mobile apps coordinate transfers, while hybrid layering – converting between cash, crypto and other stores of value (vouchers, prepaid/open-loop cards, luxury goods) and reconverting to fiat – boosts speed and reach. These methods often intersect with logistical facilitation, including misdeclared shipments and exploitation of compromised port or logistics personnel via facilitation payments, smoothing cross-border movement of value.

These networks use cryptocurrency mixers, privacy coins and decentralised P2P exchanges, third-party/ money-mule pass-through payments, trade-based settlement techniques and transaction splitting/ structuring to obscure origin, with stash locations, coordinated cash-pools and designated couriers or staff aggregating, storing and distributing bulk cash. The result is a resilient, low visibility mechanism for rapid cross-border value movement that can mask the origin and destination of funds while relying on social infrastructure rather than institutional processes.

PREDICATE OFFENCES

As supported by the FCTA 2024 [002, 003], drugs trafficking is a frequently connected proceeds-generating offence to money-laundering via underground banking and informal remittance systems because the cash-intensive, high velocity transnational drug market aligns with the strengths of IVTS – rapid cross-border transfers, cash pools, brokers, stash locations. Underground bankers move and reconcile cash volumes for drug networks, provide 'on-account' facilities and convert cash into trade flows or other stores of value – performing placement and layering functions for drug proceeds [146, 243].

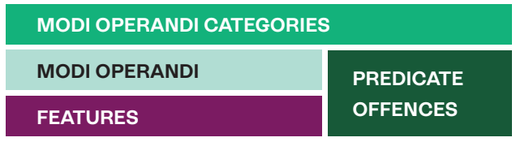
Moreover, as similarly noted in the FCTA 2024 [002, 003], cybercrime is a proceeds-generating offence which increasingly fuels laundering via IVTS. Cyber-enabled thefts and darknet sales yield proceeds already in, or quickly convertible to, cryptocurrency. Informal bankers and brokers may accept or swap such assets, use peer-to-peer exchanges, mixers or custodial services and then reconcile flows through traditional IVTS cash pools, creating fast, hybrid cross-border layering that is harder to trace [012, 146, 243].

Organised crime both generates predicate proceeds and provides the organising logic for IVTS exploitation, including smuggling. Smuggling – notably bulk cash smuggling – directly intersects with IVTS modalities: where net settlement cannot be achieved or currency shortages exist, IVTS actors physically move bulk cash across borders (secret compartments, couriers, stash locations) or combine smuggling with IVTS reconciliation techniques to bridge imbalances and inject cash into jurisdictions for further integration [012, 146, 243].

Other predicate offences that could be linked to the modi operandi and risk factors of Money laundering via underground banking/money laundering via informal remittance systems are: Arms trafficking; Corruption [10]; Extortion; Fraud; Human Trafficking; Smuggling; Tax crimes; Terrorism; and Trafficking in stolen goods.

[10] Corruption: Although not highlighted as one of the three primary offences by aggregate value, corruption – including port-level bribery, facilitation payments and compromised logistics personnel – is a critical enabler of trafficking and illicit supply-chain activity; it both generated proceeds and materially lowers barriers to cross-border movement and concealment of goods.

7 Trade-based money laundering



Description

Trade-based money laundering involves embedding illicit value within international trade transactions through complex arrangements using goods and/or services, leveraging legitimate commercial flows and trade documentation across borders to conceal or legitimise the illicit origin, ownership and destination of funds.

Extent of the threat in the Netherlands

- The FCTA 2024 [002, 003] cited the Dutch Public Prosecution Service's Annual Review 'Criminele Geldstromen 2022', which, based on intercepted/encrypted communications, found a substantial share of criminal proceeds moved via trade channels. The 2024 Dutch Public Prosecution Service review reiterates this and the NRA likewise identifies TBML as one of the highest-impact threats [135, 174].
- The FIU likewise flags TBML as high impact: intercepted communications and selected case evidence indicate that a substantial share of criminal proceeds are moved through trade channels. Detection is hindered by data gaps, cross-border complexity and limited beneficial ownership transparency, so TBML is prioritised despite relatively few publicly reported case counts [134].
- FIU casework and intelligence also show rising attention to commodity-linked value-flows. Since 2023, the Ukraine war's price volatility and disrupted routes have increased TBML vulnerability in agri-commodities (grain), enabling TBML techniques [134].
- Since the research during the previous FCTA in 2023 [002, 003], schemes have become even more sophisticated and digital – including greater use of e-commerce, layered supply chains and opaque corporate vehicles – while vulnerable sectors and new payment/settlement models broaden the risk. Supervisory scrutiny has increased (DNB), the FATF calls for better trade-data analytics, beneficial ownership transparency and cross-agency collaboration, and the WODC notes implementation and information sharing gaps that hinder detection and enforcement [134, 174, 230, 233].
- Notably, the Dutch trust sector is increasingly exposed, as trust services can create opacity and layering that align with more digital and complex TBML methods, as well as increasing legal, regulatory and reputational risk for providers [134, 174, 230, 233].

MODI OPERANDI

The principal modi operandi for this MO category include (non-exhaustive):

- Exploiting trade-based techniques, including multiple/over- and under-invoicing, goods misdescription and phantom shipments to obscure illicit funds and transfer value through trade transactions.
- Using shell, front and nominee companies and multi-jurisdictional intermediary chains to disguise trade value flows.
- Using third-party payments and surrogate payers both to separate payment flows from the underlying commercial relationship and to inject/launder criminal proceeds through trade-linked transactions (including via PSPs and settlement hubs).
- Misusing legitimate businesses and established supply chains/logical trading routes to blend licit and illicit goods.
- Splitting transactions, carouselling and round-tripping (including via captive re-invoicing or re-billing centres) to repeatedly move and obscure value.
- Using underground exchange systems and parallel settlement networks that settle value via trade transactions to convert and move funds across jurisdictions.
- Integrating illicit cash into trade via surrogate shopping, cash compensation schemes and underground bankers to convert physical cash into cross-border trade value.
- Collaborating with freight forwarders and customs brokers providers to facilitate deceptive trade constructions.
- Violating or circumventing sanctions and embargoes and abusing ownership changes through trade constructs (e.g. ownership transfers, informal re-routing) to preserve access to assets or conceal designated persons.
- Using service-based mis-invoicing (e.g., consultancy, marketing, logistics, IT) to transfer value without movement of goods (service-based money laundering).
- Exploiting tariff and duty differentials by misclassification, false declarations of origin or routing via preferential regimes to violate or circumvent customs/tariff requirements while embedding value movements in trade.

FEATURES

Exploiting pricing, product and routing discrepancies (over- and under-invoicing, goods misdescription, phantom shipments) embeds illicit value in ordinary commerce by manipulating pricing, quantities, product descriptions, routes and delivery terms. Multi-party supply chains, transshipment via hubs, free-zone storage and re-invoicing add layers of documentation and counterparties that complicate verification.

Using third-party payments, shell companies and surrogate payers separates the flow of goods from the flow of money and creates insertion points for illicit funds: third-party/surrogate settlements, front and nominee companies and multi-jurisdictional intermediary chains enable concealment of true value flows, while captive re-billing, rapid buy-sell cycles, splitting/carouselling and round-tripping repeatedly move and obscure funds. In parallel, service-based mis-invoicing (consultancy, marketing, logistics, IT and similar services) leverages the subjectivity of scope, deliverables and pricing to transfer value without movement of goods, making Service-based money laundering a practical variant that is difficult to evidence with trade records alone.

Abuse of tariff schedules and rules of origin – including misclassification of tariff codes, false declarations of origin and opportunistic re-routing via preferential regimes – creates financial incentives and concealment opportunities that can be coupled with over/under-invoicing to violate or circumvent customs and tariff requirements while embedding value movements in trade. Underground exchange systems, parallel settlement networks and cash-to-trade techniques (surrogate shopping, cash-compensation and underground bankers) further convert and transfer value across borders.

Collaborating with logistics providers and abusing documentation exploits legitimate trading routes and paperwork: freight forwarders, customs brokers and other professional service providers can be co-opted to facilitate deceptive trade constructions, mis-invoicing and amended or generic transport records, while evading sanctions and embargoes and abusing ownership changes, as well as informal re-routing preserve access to assets and conceal designated persons.

Overall, by leaning on the scale, speed and paperwork of international trade, these manipulative methods convert and layer value behind apparently regular commercial activity, often intersecting with trusted logistics providers and well-established trading routes to create plausible cover and substantial hurdles to uncovering illicit origins.

PREDICATE OFFENCES

As supported by the FCTA 2024 [002, 003], drugs trafficking is a core proceeds-generating offence to be linked to TBML because large scale drug proceeds require covert, cross-border value transfer mechanisms. Criminals therefore exploit trade techniques – over/under-invoicing, phantom shipments, parallel value-exchange schemes (informal value-transfer and barter-style exchanges) and cash-intensive business (CIB) revenue inflation – to move and convert illicit cash without physical cross-border transfers [232, 233].

Also consistent with the FCTA 2024 [002, 003], tax crimes – including VAT-related offences and other tax-evasion schemes – frequently operate in tandem with TBML. False invoicing, carousel VAT structures and complex cross-border supplier chains both facilitate evasion and provide a convenient cover to move value through trade documentation, rendering these offences both enabling mechanisms and

sources of launderable proceeds. This fiscal nexus therefore often feeds directly into wider trade-based abuse [232, 233].

Linked to that fiscal nexus, fraud – covering commercial frauds, procurement fraud and large-scale false-invoicing schemes – is frequently primarily proceeds-generating, though it may also be enabling when it produces the documents or corporate vehicles used to legitimise trade transactions. Perpetrators exploit trade channels to convert stolen or defrauded funds into apparent commercial receipts, using techniques such as shell companies, third-party settlements and mis-described shipments to distance proceeds from the underlying crime [109, 230, 232].

Other predicate offences that could be linked to the modi operandi and risk factors of Trade-based money laundering are: Arms trafficking; Corruption; Counterfeiting and piracy of products; Cybercrime; Extortion; Forgery; Organised crime; Smuggling; and Trafficking in stolen goods.

8 Money laundering via professional facilitators and money mule networks

MODI OPERANDI CATEGORIES

MODI OPERANDI | FEATURES | PREDICATE OFFENCES

Description

Money laundering via professional facilitators and money-mule networks involves engaging professionals (accountants, lawyers, bankers, notaries, trusts, and other gatekeepers) and recruited individuals to create paperwork, open accounts, or move funds on behalf of criminals. Professional criminal facilitators might create networks of individual money mules to launder proceeds, with those money-mule networks receiving and forwarding illicit funds to create distance between the original source and the final beneficiary, frequently operating as 'money laundering as a service'.

Extent of the threat in the Netherlands

- The NRA ranks abuse of professional service providers as the highest-potential-impact laundering threat (impact score 67/100), reflecting how facilitators (notaries, accountants, trust- and legal-service providers) enable conversion, legitimisation and layering of proceeds [174].
- FIU-NL reporting in 2024 shows accountants and civil-law notaries filed the most unusual-transaction reports among professional categories (3,388 and 998 unusual-transaction reports respectively), while real estate agents, valuers and lawyers reported comparatively little (155, 6 and 24 unusual-transaction reports respectively) [134].
- Experts reported a clear trend towards exploiting smaller, less-regulated facilitators – including the rise of unregulated service providers offering partial TCSP services to avoid supervision, as well as increased use of multi-jurisdictional corporate structures, nominee arrangements and recurring adviser networks; the growth of digital channels and alternative finance – together with emerging AI-driven document forgery – complicates detection [001].
- Regarding money mule networks, since the previous FCTA (2024) [002, 003], mule recruitment has risen and become more digital: nearly 10% of 16-25-year-olds report being approached (often via social media); recruiters exploit social ties and promises of quick money to use accounts to move and rapidly cash out illicit funds [105].
- Further, Europol finds that over 90% of money-mule transactions identified in European operations are linked to cybercrime [165]. FATF, in its February 2026 report, confirms the widespread scale and the central role of mule networks in cyber-enabled fraud [055].

MODI OPERANDI

The principal modi operandi for this MO category include (non-exhaustive):

- Use of lawyers, accountants, trust/formation agents and professional intermediaries to create, manage or quickly activate shell/shelf companies, nominee arrangements, trusts and multi-jurisdictional corporate chains that receive, mix and re-route criminal proceeds.
- Coordinated use of money-mule networks, leased (rented/controlled) bank accounts, third-party accounts and physical cash couriers to receive, aggregate and rapidly disperse illicit funds across accounts and jurisdictions.
- Outsourcing laundering by recruiting accomplices and coordinating services via online platforms.
- Opening accounts (personal or corporate) using stolen, forged or synthetic identities and falsified corporate documents to create on-ramps for illicit funds.

- Exploiting charities, NGOs or non-profit vehicles with opaque governance to comingle, misappropriate or conceal criminal funds.
- Misusing payment service providers (PSPs), brokers, MSBs, regional agents or intermediaries to mask client identities, commingle funds and blend illicit flows with legitimate flows.
- Using trade, procurement and commodity instruments – false invoices, manipulated valuations, commodity certificates – to integrate and move value across borders while masquerading as legitimate commerce.

FEATURES

Use of lawyers, accountants, trust/formation agents and professional intermediaries provides paperwork, structures and narratives that make illicit movements look conventional; formation agents and advisers set up legal vehicles, manage documentation and orchestrate flows between related parties and service providers across borders to receive, mix and re-route criminal proceeds.

Coordinated use of money-mule networks, leased or third-party bank accounts and physical cash couriers enables rapid receipt and onward transfer of funds and the quick turnover of value; recruited intermediaries, short-lived accounts or wallets and accounts opened with stolen, forged or synthetic identities create distance from the original source, while the combination of credible documentation, recognised professional roles and dispersed, short-term actors makes each step appear routine yet collectively enables funds to be represented as legitimate.

Increasingly, digital outreach and platform-based coordination reduce the cost and accelerate the recruitment and orchestration of participants, while intersections with trade, corporate networks and virtual assets – and misuse of charities, PSPs or other intermediaries – further dilute provenance and complicate detection.

PREDICATE OFFENCES

Professional facilitators operate across the full spectrum of proceeds-generating offences – from drug trafficking to tax crimes – but this section focuses on enabling offences, as these reflect the facilitators' toolkit and are more recognisable to banks.

Corruption, for example, is a key enabling offence frequently linked to laundering through professional facilitators. It is used to enlist or secure the collaboration of professional facilitators: bribery and illicit payments can bind or coerce lawyers, accountants, Trust and Company Service Providers and nominee directors into forming, administering and operating opaque entities on behalf of corrupt actors. These actors establish shell companies, trusts and multi-jurisdictional ownership chains that enable bribe payments to be commingled and rerouted with limited transparency. Professional laundering networks then exploit differences in disclosure and beneficial ownership rules to obscure the ultimate beneficiaries [024].

Forgery is another principal enabling offence for professional facilitators. They routinely produce or procure falsified documents – counterfeit identifications, fabricated bank statements, false invoices and bogus incorporation papers – to enable rapid account openings, shell-company formation and misrepresentation of commercial transactions. Such documents underpin placement and layering by providing apparently legitimate on-ramps and provenance [024].

With respect to money mule networks specifically, cybercrime is the dominant proceeds-generating offence. Many mule transfers originate from phishing, malware, business-email compromise, online auction/e-commerce fraud and romance/booking scams. Mule networks receive, aggregate and forward these proceeds, often across multiple jurisdictions and payment rails, serving as the conduit that converts cybercrime takings into laundered value while severing the traceable link to offenders [109, 165].

Other predicate offences that could be linked to the modi operandi and risk factors of Money laundering via professional facilitators and money mule networks are: Drugs trafficking; Extortion; Fraud; Human trafficking [11]; Organised crime; Smuggling; Tax crimes; Theft (and robbery); and Trafficking in stolen goods.

[11] Human trafficking: Although not highlighted as one of the three primary offences, human trafficking warrants particular attention in the context of money mule networks. Victims can be coerced or manipulated into opening accounts, receiving and forwarding funds, or otherwise acting as unwilling intermediaries; in such cases human trafficking functions both as a source of proceeds and as an enabling offence for mule-based laundering.

9 Money laundering via corporate & legal entity networks [12]

MODI OPERANDI CATEGORIES

MODI OPERANDI | PREDICATE OFFENCES

FEATURES

Description

Money laundering via corporate and legal entity networks involves deliberately using companies, trusts and other legal vehicles to conceal ultimate beneficial ownership, fabricate commercial activity and layer illicit proceeds through intercompany transfers, false invoices and circular flows, with the effect of disguising the origin of funds and impeding regulatory oversight and tracing.

Extent of the threat in the Netherlands

- Abuse of corporate and legal entity networks is a material, high impact money laundering enabler in the Netherlands – not large by case count (of which numbers are hard to find in publicly available documents) but disproportionate in value and consequence, because relatively few corporate network investigations can involve very large sums and prolonged concealment; this is reflected in the NL FCTA 2024, the most recent NRA and the 2024 FIU Annual Review [134, 174].
- Europol reports that 86% of the EU's most threatening criminal networks exploit legal business structures to launder proceeds and expand operations [148].
- Since the previous FCTA, published in 2024 [002, 003], criminal actors have become more professional and hybrid, combining layered corporate chains, trade-based techniques, underground banking and crypto on/off-ramps to obscure provenance and re-layer proceeds; experts note a shift to engineered corporate complexity – multi-tier ownership, circular intercompany transfers, address and directorship clustering and nominee services [001, 134, 174].
- Furthermore, criminal groups increasingly exploit foreign registries, opaque jurisdictions and cross-border service providers to evade domestic transparency, reflecting growth in corporate-style organised crime and foreign facilitators [001, 134, 174].

[12] In the NL FCTA, the MO categories Money laundering via corporate and legal entity networks and Money laundering via jurisdictional arbitrage are presented separately; in the FCTA for banks, these two MO categories are combined.

MODI OPERANDI

The principal modi operandi for this MO category include (non-exhaustive):

- Creating and use of multi-jurisdictional shell/shelf companies, conduit networks and front companies (multi-tier ownership, nominees/straw directors) to fragment flows, obscure beneficial ownership and disguise movement of illicit goods or proceeds.
- Using false documentation, sham transactions, or manipulated records to channel illicit funds through corporate entities.
- Using legitimate businesses and sectors (e.g. construction, hospitality, scrap/recycling, real estate) as façades to conceal illicit proceeds within legitimate income, including through co-mingling, overstated revenues and cash-intensity masking.
- Using trust, foundations, STAKs and opaque legal forms to hide beneficial ownership and launder funds.
- Using securities, loans, bonds and share manipulations through corporate structures to transfer value and launder funds.
- Exploiting fragmented corporate registries and data silos to hide entity linkages and avoid detection across jurisdictions.
- Abusing fintechs, payment processors and alternative payment rails (including embedded finance) as rapid conduits to layer and move illicit funds.

FEATURES

Creation and use of multi-jurisdictional shell and conduit networks fragment ownership and control through layered ownership structures, frequent changes in office-holders or addresses and clusters of entities that claim distinct activity. Intercompany transfers, loans, dividends and service charges move value through circular or opaque patterns that are hard to reconcile with operational substance.

Using false documentation, sham transactions and manipulated records disguises flows behind plausible commercial activity: legal forms and contractual arrangements may bear little relation to a firm's size, maturity or stated purpose, while co-mingling, overstated revenues and cash-intensity masking in sectors such as construction, hospitality, scrap/recycling and real estate hide illicit proceeds. Securities, loan and share manipulations and rapid buy-sell cycles further transfer value within corporate structures.

Abusing professional intermediaries, fragmented registries and fintech rails conceals beneficial ownership and accelerates movement: trusts, foundations, STAKs and other opaque legal forms are used alongside notaries, trustees and advisers to form and manage entities. Fragmented corporate registries and data silos reduce whole-chain visibility, and payment processors, embedded finance and alternative payment rails provide rapid conduits to layer and re-route illicit funds.

In combination, these features create engineered opacity: credible corporate façades enable the steady conversion, movement and reclassification of funds so that illicit proceeds eventually appear as legitimate income, investment returns or retained profits.

PREDICATE OFFENCES

Drugs trafficking is a principal proceeds-generating offence, routinely exploiting legitimate business structures across production, transport and distribution. Import/export and freight companies, port agents and repackaging firms conceal shipments or act as consignee façades, while legitimate logistics firms and courier networks can be infiltrated or exploited unwittingly. Criminal groups also blend legal and illicit trade through buying/selling companies, use hospitality and retail outlets as cash-intensive fronts and invest proceeds in real estate or trading firms to layer funds [134, 148].

Fraud is an important enabling offence since shell and front companies, sham invoices and circular intercompany loans create a manufactured commercial trail that masks misappropriation. This engineered façade permits diversion of proceeds into the legal economy by obscuring origin and ownership and enabling internal transfers and reclassifications that hide the illicit source before funds reappear as legitimate income or distributions [109, 134, 148].

Building on that, tax crimes – notably VAT-carousel/MTIC schemes, dividend stripping, excise and subsidy fraud – are typically enabled by multi-tier, cross-border corporate structures: networks of conduits, missing traders, buffers, cross-invoicers and invoice-mills exploit jurisdictional VAT differences (services and intangibles) and corporate lifecycle timing to claim refunds and disappear, while generating illicit proceeds and enabling layering and jurisdictional arbitrage via foreign accounts and liquidation through third-party payments, rendering tax offences both proceeds-generating and enabling for TBML [134, 148].

Other predicate offences that could be linked to the modi operandi and risk factors of Money laundering via corporate and legal entity networks are: Corruption, Counterfeiting and piracy of products, Cybercrime, Environmental crime, Extortion, Insider trading & market manipulation, Forgery, Organised crime; Theft (and robbery); and Trafficking in stolen goods.

10 Money laundering via jurisdictional arbitrage [13]

MODI OPERANDI CATEGORIES

MODI OPERANDI | PREDICATE OFFENCES

FEATURES

Description

Money laundering via jurisdictional arbitrage involves exploiting differences in laws and regulations, supervision and enforcement between jurisdictions to move prohibited funds through weakly regulated or opaque financial centres. Perpetrators fragment and layer transactions across borders to exploit regulatory gaps and hamper tracing.

Extent of the threat in the Netherlands

- Jurisdictional arbitrage is a material, high impact money laundering threat in the Netherlands – not large by case count (of which numbers are hard to find in public available documents) but disproportionate in value and consequence, because organised-crime actors and professional facilitators exploit cross-border regulatory, supervisory and transparency gaps to move and integrate large sums [134, 174].
- Since the publication of the previous FCTA in 2024 [002,003], criminal networks have become noticeably more 'corporate' and international, by adopting business-style methods, structures and professional roles that legitimate firms while a rise in cross-border corporate vehicles and foreign facilitators has facilitated jurisdictional arbitrage and more complex, multi-jurisdictional money-laundering schemes [134, 174].
- Notably, experts warn of a rising pattern of jurisdictional arbitrage using multilayer corporate chains, frequent UBO/director turnover and registration in conduit or secrecy jurisdictions – sometimes involving Dutch-linked entities – facilitated by small professional networks [001].
- AML Network notes rapid AI/big-data adoption, deeper international AML collaboration and EU-led harmonisation (AMLR/AMLA), plus tougher scrutiny of fintech/crypto and beneficial ownership – but these reforms take time to mature and can create interim arbitrage dynamics that offenders exploit [262].

MODI OPERANDI

The principal modi operandi for this MO category include (non-exhaustive):

- Using foreign trusts and favourable jurisdiction laws to obscure beneficial ownership and conceal and transfer illicit assets.
- Using or opening foreign/offshore bank accounts, correspondent banking relationships and complex third-party or cross-border payment routes in weak AML jurisdictions to conceal ownership, move and layer illicit funds.
- Establishing operations in weak AML jurisdictions to conceal, move and launder illicit funds.
- Exploiting the absence or slowness of cross-jurisdictional collaboration, asynchronous implementation of controls or temporary enforcement gaps to move, 'park' or stage illicit funds in these jurisdictions while controls tighten elsewhere.
- Using foreign corporate, nominee, letter-box, shelf or shell entities specifically to exploit jurisdictional secrecy to obscure beneficial ownership, hold assets and layer illicit funds.
- Using cross-border investments and investment programmes to obscure illicit origins and evade scrutiny.
- Exploiting free movement and residency schemes within the EEA to conceal illicit funds and capital.
- Using anonymity enhancing prepaid instruments, e-money and offshore crypto/exchange platforms in weak AML jurisdictions to move and obscure funds.
- Using sham or collusive arbitration and court proceedings to obtain enforceable awards or titles that mask and facilitate cross-border transfer of illicit assets.
- Using fabricated contracts to create plausible economic narratives and conceal source of funds in cross-border schemes.

FEATURES

Using permissive or favourable jurisdictions to establish entities, book activity or stage funds exploits differences in law, disclosure, collaboration and enforcement across countries. Perpetrators make strategic use of these locations to route sequential cross-border movements through several intermediaries, frequently change formal control and park funds in places while controls tighten elsewhere or route flows through hubs that offer speed and limited transparency.

Using foreign corporate, nominee, letter-box, shelf or shell entities and trust or foundation structures to separate legal title, management and benefit combines vehicles from multiple jurisdictions and frustrates straightforward assessments of ownership and purpose. Payment and investment activity can be framed as routine treasury or holding services, while cross-border accounts, correspondent relationships and complex third-party payment routes conceal ownership and move or layer funds.

Overall, the approach relies on asynchronous rules, fragmented information and cross-border complexity to keep origin and control unclear, buying time and distance until value is integrated into ordinary economic channels.

PREDICATE OFFENCES

Corruption is a closely linked enabling offence to money laundering via jurisdictional arbitrage. Bribery and related practices enable the cross-border concealment and protection that arbitrage exploits. Corruption can facilitate the creation or acceptance of opaque foreign corporate structures, delay or obstruct domestic investigations and provide local protection that allows illicit assets to be parked or moved through weaker AML jurisdictions. In arbitration, these dynamics can be exploited to legitimise tainted assets and secure enforceable cross-border transfers through a binding decision or settlement [041].

Fraud is another central enabling offence where sham or collusive legal proceedings are used. Fabricated contracts, manufactured disputes and front companies can be deliberately placed in more permissive jurisdictions so that an arbitral or court decision masks the illicit origin of funds and permits cross-border enforcement or transfer [109, 226].

Furthermore, tax crimes are particularly relevant since differences in taxation, beneficial ownership disclosure and financial reporting create routine arbitrage pathways. Serving as both proceeds-generating and enabling offences, tax crimes perpetrators exploit weaker reporting regimes, residency or investment schemes and asymmetric exchange of tax information to reclassify, relocate or 'park' assets, shielding proceeds of crime from scrutiny before later integrating them into the formal economy – precisely the behaviour regulatory arbitrage frameworks seek to prevent [262].

Other predicate offences that could be linked to the modi operandi and risk factors of Money laundering via jurisdictional arbitrage are: Arms trafficking; Cybercrime; Drugs trafficking; Extortion; Forgery; Human trafficking; Insider trading & market manipulation; Organised crime; Smuggling; Terrorism; and Trafficking in stolen goods.

[13] In the NL FCTA, the MO categories Money laundering via corporate and legal entity networks and Money laundering via jurisdictional arbitrage are presented separately; in the FCTA for banks, these two MO categories are combined.

11 Terrorism financing

MODI OPERANDI CATEGORIES

MODI OPERANDI | PREDICATE OFFENCES

FEATURES

Description

Terrorism financing (hereinafter: TF) involves providing, moving or concealing funds to support terrorist activity through – often small –, seemingly legitimate transactions and non-transparent channels, exploiting legal loopholes and rapid, complex routing to disguise their purpose. TF primarily concerns the concealment of the intended use or ultimate beneficiary of funds rather than necessarily concealing the origin. It is increasingly decentralised and may be self-financed by lone actors, petty crime or licit sources, and can in some contexts converge with organised crime or involve abuse of humanitarian aid in conflict zones, including environmental crime tied to exploitation, trade and trafficking of natural resources.

Extent of the threat in the Netherlands

- Similar to the NL FCTA 2024 [002, 003], the current terrorism threat level in the Netherlands remains level 4 on a scale from 1 to 5, which indicates that the risk of an attack in the Netherlands is substantive, with jihadism remaining the principal terrorist threat. The NRA TF 2023 indicates that vulnerabilities are concentrated in giro and cash transactions via licensed banks and money-transfer offices, internet PSPs, providers of crypto services (licensed and unlicensed), and unlicensed payment providers and hawala networks [173].
- TF activity in the Netherlands remains numerically small – prosecutions typically number in the low tens per year – but rose in 2024: the FIU produced 309 TF-related dossiers (≈1.9% of 16,306 STR dossiers), covering 2,554 transactions; each TF file carries high security consequences (13 dossiers in 2024 had a firearms component) and automated detection yields relatively weak signals (for natural persons; for legal entities, automated detection is more effective), with information sharing (strategic and tactical) a key source for identifying and prioritising cases, while adverse media may provide additional leads [134, 173].
- Since the previous FCTA (2024) [002, 003], methods have diversified and become harder to detect, such as online/social media fundraising, the use of virtual assets and rapid online radicalisation of youth increases vulnerability [001, 038, 077, 134, 173].
- Furthermore, right-wing normalisation and online radicalisation have increased the potential for violent acts while left-wing extremist activity shows isolated escalation rather than a sustained terrorist threat; 'extremism' is a broader socio-political concept and is distinct from legally defined terrorism [001, 077, 173].

MODI OPERANDI

Due to the complex and often overlapping nature of TF, three groups of modi operandi are distinguished – fundraising; movement/distribution; and cash/in-kind [14]. The principal modi operandi for these groups include (non-exhaustive).

Fundraising

- Using non-profit and charities with weak governance, front companies and shell entities with weak transparency or regulation to solicit, generate or conceal funds.
- Raising funds through crowdfunding on online platforms (including gaming and streaming) and via social media and messaging apps to solicit, move or obscure contributions.
- Generating revenue through direct criminal activities (extortion/taxation-like collections, kidnapping for ransom, trafficking, smuggling, drug and arms offences).
- Exploiting illicit trade networks and commodity supply chains (looting, smuggling of high value goods, trade mis-invoicing) to generate, store or conceal funds.
- Exploiting healthcare and social-benefit systems through fraudulent billing, fabricated claims or phantom providers to generate, move or conceal funds.

Movement/distribution

- Using formal banking and payment service channels (bank accounts, wire transfers, cards, PSPs, virtual IBANs, neobanks) to transfer funds to and from high risk jurisdictions or by PEPs to extremist groups.
- Using informal value transfer systems (hawala/hundi, unlicensed money service providers, mobile-money platforms) to move value and bypass formal controls.
- Using virtual assets and related services (unhosted wallets, VASPs, stablecoins, mixers, privacy coins) to hold, transfer or obfuscate funds and facilitate cross-border distribution.

Cash/in-kind

- Using cash couriers and bulk cash smuggling to physically move and conceal value across borders.
- Investing in or using legitimate businesses and real-world assets and in-kind value (real estate, jewellery, precious metals, vehicles, merchandise) to store, launder or legitimise proceeds.

FEATURES

Using non-profit, charitable organisations, front companies and shell entities to generate, move or conceal funds, TF often draws on both legal and illegal sources and increasingly uses small, frequent transfers and community-based fundraising to reduce visibility. These channels may operate via digital platforms, informal value networks and cash-based methods, often with rapid movement between rails.

Using illicit trade networks and direct criminal activities to generate proceeds, TF can converge with exploitation of commodity supply chains, looting, smuggling of high value goods, healthcare and social-benefit fraud (e.g., fraudulent billing, fabricated claims or phantom providers), extortion, trafficking, kidnapping for ransom and other offences to produce steady income, while in other contexts funding reflects spontaneous, decentralised contributions.

Using informal value-transfer systems, cash methods and formal payment channels to move funds, the financial signatures of TF range from micro-donations and platform payouts to transfers associated with travel, equipment or facilitation. This includes use of hawala/hundi, unlicensed MVTS, cash couriers and bulk cash smuggling as well as bank accounts, PSPs, virtual IBANs and cards when suitable for the objective.

In recent years, virtual assets and online fundraising have been increasingly used to solicit, hold and move funds; unhosted wallets, Virtual Asset Service Providers (hereinafter: VASPs), stablecoins, mixers and privacy coins are employed alongside crowdfunding via social media, gaming and streaming platforms, and perpetrators also invest in or use legitimate businesses and in-kind value (real estate, jewellery, vehicles, merchandise) to store, launder or legitimise proceeds.

The overall profile is adaptive and agile: a blend of local and cross-border activity, formal and informal rails, and legitimate-appearing narratives that mask the ultimate purpose. This makes clarity of end-use and beneficiary difficult, particularly where community, ideological or humanitarian language provides plausible cover.

PREDICATE OFFENCES

While many offences generate proceeds that are subsequently used to finance terrorism, TF does not always require an underlying criminal act; financing can originate from legitimate sources, illicit proceeds, or a mixture of both. The entries below therefore identify offences commonly associated with TF-related funding, while recognising that TF may also occur absent a prior predicate offence.

A common illustration is drugs trafficking: illicit drug markets generate substantial, readily convertible cash that funds operations, procurement and fighters' pay. Traffickers and militant networks exploit the same transport routes, corrupt officials and informal value-transfer systems (hawala, unlicensed MVTS, cash couriers) and may tax or

[14] Many modi operandi may, in practice, straddle categories.

‘protect’ shipments, turning smuggling corridors into recurring revenue streams [038, 086, 173].

Extortion (including taxation-like collections) is another core proceeds-generating offence for TF because groups that control territory or criminalised trade routes convert local economic activity directly into liquid funds: ‘road taxes’, protection fees and levies on traders and transporters reliably generate cash that fuels operations and procurement [038, 072, 086, 173]. Moreover, environmental crime tied to exploitation, trade and trafficking of natural resources (oil/gas, artisanal/illicit mining, charcoal/timber, precious stones, wildlife) is a structural proceeds-generating offence for TF where groups control territory or smuggling chains. By levying taxes, extorting miners and traders, running illicit extraction and using corrupt or informal trade networks they convert resources into cash or tradable value; those proceeds are laundered via informal and formal channels while commodity flows provide cover for trade-based value transfers and links to professional enablers for cross-border movement [038, 156, 173].

Other predicate offences that could be linked to the modi operandi and risk factors of TF are: Arms trafficking; Corruption; Counterfeiting and piracy of products; Cybercrime; Forgery; Fraud; Human trafficking; Kidnapping, illegal restraint and hostage-taking; Organised crime; Piracy; Sexual exploitation; Smuggling; Terrorism; Theft (and robbery); and Trafficking in stolen goods.

12 Sanctions evasion

MODI OPERANDI CATEGORIES
MODI OPERANDI
FEATURES
PREDICATE OFFENCES

Description

Sanctions evasion (hereinafter: SE) involves using deceptive tactics such as shell and front companies, intermediaries, sudden ownership changes, strawmen and legal loopholes to conceal the involvement of sanctioned persons or jurisdictions, often routing funds through unnecessarily complex multi-jurisdictional payment chains to obscure the trail and maintain a façade of compliance.

Extent of the threat in the Netherlands

- In line with the NL FCTA 2024 [002, 003] observation that international sanctions were increasing (noting the EU’s twelfth package at that time), the sanctions landscape has continued to expand – most recently reflected by the adoption of the EU’s twentieth sanctions package [085].
- Six months after the publication of the NL FCTA 2024 [002, 003] a report from Statistics Netherlands (Centraal Bureau voor de Statistiek; hereinafter: CBS) confirmed sanctioned exports to Russia fell by c. 86% in 2023 versus 2018–21, while exports of the same goods to seven high risk transshipment countries rose sharply and aggregate Eurasian Economic Union (hereinafter: EAEU) exports were c. 90% higher, signalling diversion risk [151].
- In 2024, FIU-Netherlands recorded SE-related dossiers (≈1.4% of 16,306 STR dossiers), covering 6,437 transactions [134]; the FIOD subsequently pursued multiple high profile export-to-Russia cases (originating from FIU/bank referrals) [101, 174].
- Since the research of the previous FCTA in 2023 [002, 003], state and non-state actors have increasingly exploited intermediaries, opaque corporate structures, virtual assets and maritime/shipping techniques to evade sanctions, as reflected in controls on advanced semiconductors to the PRC and controls on components for Iranian drone production [001, 037] A February 2026 report from the General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst; hereinafter: AIVD) and the Military Intelligence and Security Service (Militaire inlichtingen en veiligheid; hereinafter: MIVD) documents intensified Russian hybrid activity – encompassing cyber operations, clandestine influence and sabotage preparations – which may further amplify these risks by expanding diversion routes and covert logistics [237].
- Further, diversion more commonly uses permissive transit hubs (e.g. Turkey, India), falsified trade documents, PSPs/fintech settlement routes and weak goods-flow visibility [001].

MODI OPERANDI

The principal modi operandi for this MO category include (non-exhaustive):

- Performing transactions in commonly used currencies through unnecessary, complex payment routes – routing via multiple neighbouring or permissive jurisdictions and through several different payers and beneficiaries to hide the trail (e.g. U-turn transactions).
- Leveraging intermediaries, including front and shell companies, complex corporate structures and third-party payments to obscure connections to sanctioned entities and disguise ultimate ownership.
- Abusing humanitarian, diplomatic or sanctions exemption mechanisms that lack transparency to cover sanctioned flows.
- Using networks of unlicensed financial facilitators and intermediaries (unlicensed MSBs, hawala-style operators and Over-The-Counter (hereinafter: OTC) brokers to procure services and approvals.
- Exploiting trade-based techniques (over/under invoicing, multiple invoicing, phantom shipments) to mask end users or cargo, or using stablecoins for rapid value transfer and layering.

- Using virtual assets and related technologies (stablecoins, cross-chain bridges, mixers, DeFi and OTC conversion) to facilitate direct or indirect financial flows to sanctioned destinations.
- Transferring liabilities or contractual obligations from sanctioned parties to third parties to circumvent controls.
- Concealing sanctioned parties via aliases, name variants or nominee identities to hide the true beneficiary.
- Transferring ownership to family members or adjusting shareholdings (e.g. reducing a majority stake from 51% to 49%) to evade controls.
- Using ship-to-ship transfers, Automatic Identification System (hereinafter: AIS) disabling and other maritime techniques to hide movement of goods, technologies or ancillary services.
- Using PSPs to obfuscate counterparty information across sectors (not limited to maritime, though notable there).
- Routing via permissive third-country transit hubs to exploit globalised supply chains and obscure procurement activities.
- Using real estate and high value assets to store value and launder proceeds from sanctioned activity.
- Using cyberattacks, theft of virtual assets and ransomware-style operations to generate and launder proceeds for sanctioned actors.

FEATURES

Enlisting intermediaries by using front and shell companies, complex structures and third-party payments seeks to conceal the link between restricted persons, goods or destinations and the financial or logistical steps that support them. Sudden changes in ownership or routing and the use of permissive transit hubs are commonly deployed to obscure true counterparties.

Exploiting trade-based techniques (over- and under-invoicing, multiple invoicing, phantom shipments) and employing ship-to-ship transfers or multi-leg journeys may under-state, misdescribe or repeatedly re-invoice consignments, while AIS-disabling and other shipping tactics further obscure end-user and cargo identity, particularly where dual-use goods are involved.

Performing transactions through complex payment chains and alternative rails, and using virtual asset bridges, mixers or unlicensed facilitators, introduces unnecessary hops and third-party settlements to disguise counterparties. Routing via multiple neighbouring or permissive jurisdictions, U-turn-style transactions, misuse of PSPs, and abuse of humanitarian or diplomatic exemptions add layers of indirection that conceal sanctioned linkages.

The essential feature is choreography: aligning goods-flows and money-flows across borders, entities and records so that each individual step appears defensible, yet the overall pattern conceals the sanctioned linkage.

PREDICATE OFFENCES

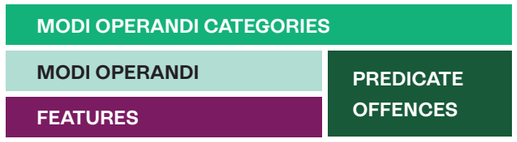
As underlined in the FCTA 2024 [002, 003], arms trafficking is often associated with SE due to the nature of the product: weapons, components and dual-use technologies are frequently sanctioned and therefore concealed using front and shell companies, falsified end-user certificates and trade documents, and by routing consignments through permissive third countries. Arms trafficking thus has a dual role: it supplies illicit materiel that can facilitate violent crime or conflict, and it is a proceeds-generating offence that produces substantial illicit revenues for traffickers, brokers and networks; these proceeds are commonly concealed and laundered using the same techniques employed to evade sanctions and detection [037, 240].

Further, as likewise mentioned in the FCTA 2024 [002, 003], fraud is a common and direct enabler of SE: sham sales, mis-declaration of goods and falsified end-user certificates permit sanctioned cargo and payments to be disguised as legitimate trade. Forgery – notably counterfeit bills of lading, altered invoices and bogus insurance or export licences – is a pervasive element of these frauds and directly undermines sanctions-screening and export-control checks [037, 109, 240].

Smuggling also serves as a common enabling offence where the physical concealment or illicit carriage of goods is used to bypass export controls and sanctions. As noted in the FCTA 2024 [002, 003], this encompasses sea smuggling such as ship-to-ship transfers, as well as AIS manipulation, the use of alias flags and transshipments via third countries [037, 202].

Other predicate offences that could be linked to the modi operandi and risk factors of SE are: Corruption; Espionage; Organised crime; Terrorism; Counterfeiting and piracy of products; Cybercrime; and Trafficking in stolen goods.

13 Money laundering via virtual assets



Description

Money laundering via virtual assets (including crypto assets) is the process of concealing the illicit origin of criminal proceeds by using cryptocurrencies, stablecoins and tokenised assets, exploiting the high speed borderless and pseudonymous nature of blockchains.

Extent of the threat in the Netherlands

- Money laundering via virtual assets is considered a material and evolving integrity risk in the Netherlands. The domestic crypto ecosystem has grown and professionalised under EU frameworks (EU Markets in Crypto-Assets Regulation (hereinafter: MiCAR)) with licensed providers active in the Dutch market and increasing touchpoints with banks [001, 174].
- Since VASPs came under reporting obligations, FIUs have observed a marked increase in crypto-related filings. In the Netherlands, crypto-linked UTRs now form a meaningful share of intake. Volumes from VASPs are largely driven by objective criteria, whereas banks' filings are predominantly subjective; figures are therefore not directly comparable and should be interpreted with care [134].
- Since the FCTA 2024 [002, 003], criminal activity has professionalised and converged with cybercrime – a development that is underscored in a February 2026 FATF report, noting the proliferation of organised scam centres and large scale social engineering operations [055]. A March 2026 FATF report further emphasises the heightened ML/TF/SE risks posed by stablecoins and unhosted wallets in P2P transactions [210]. This trend is consistent with the 2026 BIS analysis showing a tendency for illicit activity to migrate to payment instruments with weaker monitoring ('waterbed effect') [104].
- Public blockchains provide visibility when wallet ownership is attributed (e.g., client-consented addresses or VASP statements), but obfuscation tools (e.g., mixers or privacy coins [15]) limit traceability; combined on-/off-chain analysis can still be predictive when applied proportionately and lawfully [001, 017, 174, 257].
- Globally, over the past few years, the crypto crime landscape has professionalised with illicit organisations now operating large scale on-chain infrastructure to help transnational criminal networks launder illicit crypto. In 2025, nation-state activity in crypto rose as states tapped these professionalised service providers and stoop up their own bespoke infrastructure to evade sanctions at scale [053].
- Finally, reports indicate increased use of crypto by sanctioned actors and terrorist organisations to move value, raise funds and pay facilitators, notably since recent geopolitical conflicts (e.g., Russia-Ukraine, Israel-Palestine, Iran-US tensions). Furthermore, state-linked groups associated with the DPRK (e.g., 'Lazarus Group') have been reported to steal large amounts of crypto and launder the proceeds to fund weapons programmes; some funds have been successfully cashed out via weakly controlled channels. Recent reporting also shows the emergence of bespoke or privately issued stablecoins designed explicitly to circumvent sanctions controls, enabling sanctioned actors and facilitators to route value outside traditional rails [053, 257].

MODI OPERANDI

The principal modi operandi for this MO category include (non-exhaustive):

- Using anonymity enhancing on-chain techniques (e.g., mixers/tumblers, privacy coins [15], chain-hopping and decentralised exchanges) to break provenance before or between fiat conversion points.
- Using crypto debit or virtual cards to spend or cash out crypto on card rails (often small, frequent withdrawals and round amounts), including rapid funding from VASPs or PSPs.
- Exploiting fragmented payment ecosystems (VASPs, PSPs, virtual IBANs, money transmitters and card intermediaries) to disperse or aggregate flows around on-/off-ramp events.
- Conducting OTC desk and peer-to-peer conversions that culminate in bank-visible cash deposits, incoming transfers, or third-party pass-through activity.
- Breaking transaction trails through a combination of mixers, cross-chain swaps/bridges and rapid conversions into and out of stablecoins before fiat cash-out.
- Accepting or paying in crypto via darknet marketplaces or high risk merchant channels, followed by consolidation and off-ramping to bank accounts.
- Creating or obtaining virtual assets, coin offerings and token sales, inflate valuation and at some point, sell their holdings (pump and dump).
- Using automated bots to snipe newly launched tokens on decentralised exchanges, create apparent liquidity/volume and rapid pump-and-dumps, then cycle proceeds via token swaps/bridges and weakly-regulated VASPs before fiat off-ramp.
- Using online crypto casinos, Initial Coin Offerings (hereinafter: ICOs), Non-Fungible Tokens (hereinafter: NFTs), mining pools and staking operations to relabel illicit crypto earnings as legitimate winnings, earnings or sale proceeds cashed out via crypto on- and offramps into bank accounts.

FEATURES

Crypto on- and offramps can be used to place, layer or integrate illicit funds into the virtual asset ecosystem by turning fiat, cash or criminal proceeds into cryptocurrencies, stablecoins or tokenised assets. Conversion points on- and off-ramps, rapid cross-chain transfers and repeated cycling between digital and traditional channels enable swift placement and layering while obscuring provenance.

Anonymity enhancing tools and fragmented payment ecosystems conceal ownership and disrupt traceability: pseudonymous or unhosted wallets, privacy coins, mixers/tumblers, chain-hopping and crypto payment cards are used alongside VASPs, PSPs, virtual IBANs, crypto ATMs, informal brokers, underground bankers and unregulated third parties to break transaction trails, disperse transaction data and convert crypto to cash (including withdrawals split into small amounts to avoid reporting thresholds).

Darknet markets and merchant conversion and creation/monetisation schemes provide laundering routes and exit opportunities. Criminals buy or sell goods on darknet platforms, accept crypto for illicit sales, or create crypto assets, coin offerings or token sales (including pump-and-dump tactics) to generate plausible liquidity and conceal proceeds before cashing out.

The approach benefits from global reach, 24/7 markets and new forms of custody or settlement, while intersecting with cyber-enabled crime and online marketplaces; its defining characteristics are velocity, borderlessness and a reliance on technical mechanisms that dilute the clarity of origin, counterparties and purpose.

[15] Privacy coins and anonymous wallets will be illegal in the EU per 1 July 2027.

PREDICATE OFFENCES

Traditional crimes increasingly use virtual asset payment rails. For example, drugs trafficking is a recurring source of virtual asset proceeds: darknet vendors and buyer networks commonly transact in crypto, after which proceeds are fractured and layered through multiple chains, mixers and decentralised services and ultimately converted into fiat or spent via prepaid/merchant channels – rendering it a prominent proceeds-generating offence [051, 052, 258].

Furthermore, cybercrime – including ransomware, hacking and the unauthorised misappropriation of virtual assets – features prominently as both a proceeds-generating and enabling offence for laundering via virtual assets. Cyber-enabled offending yields readily transmittable proceeds and makes intensive use of crypto rails that can be rapidly obfuscated (mixers, chain-hopping, bridges and unhosted wallets), while the same technical infrastructure and third-party services also enable wider laundering activity across jurisdictions [017, 051, 258].

Fraud – encompassing investment scams, Ponzi schemes, ICO/token-launch abuse, 'rug-pulls' and sophisticated social-engineering cons – similarly operates both as a large proceeds-generating offence and as an enabling offence where sham platforms, fake liquidity or merchant fronts are used to manufacture apparent 'legitimate' flows. Proceeds from such schemes are readily cycled through multiple token swaps, P2P venues, privacy coins and weakly-regulated VASPs before cash-out or reuse as purported trading income. In coin-offering contexts, market manipulation – prohibited under MiCAR's market-abuse regime for in-scope crypto-assets – and related fraud can create inflated or fictive valuations that are later integrated via fiat off-ramps as ostensible investment income. Additionally, natural persons or business customers acting as de facto VASPs create nested-intermediary and authorisation risks and can be used to channel or relabel illicit proceeds as 'legitimate' trading or investment income [006, 052, 109].

Other predicate offences that could be linked to the modi operandi and risk factors of Money laundering via virtual assets are: Arms trafficking; Corruption; Extortion; Insider trading & market manipulation; Organised crime; Sexual exploitation; Smuggling; Tax crimes; Theft (and robbery); and Trafficking in stolen goods.

14 Money laundering via securities investment products and capital markets

MODI OPERANDI CATEGORIES

MODI OPERANDI | FEATURES | PREDICATE OFFENCES

Description

Money laundering via securities, investment products and capital markets involves channelling illicit funds into securities, funds or capital-markets transactions to create a veneer of lawful investment income. Abuse techniques exploit the opacity of market actors and structures – brokers, fund managers/advisers, custodians and other intermediaries – which can obscure ultimate beneficial owners and complicate attribution. Perpetrators use complex legal, corporate or fund arrangements and investments in non-listed private companies to place and conceal proceeds. They also exploit omnibus or pooled custody arrangements to fragment investor visibility and facilitate layering and integration. In some markets, over-the-counter (OTC) trades introduce price opacity that helps mask valuation and provenance. The high velocity of funds and rapid cross-border settlement enables quick movement of large values, aiding layering and concealment.

Extent of the threat in the Netherlands

- Money laundering through securities, investment products and capital-markets in the Netherlands is a real but niche and high impact threat – observable case counts are modest compared with cash/crypto ML, yet individual schemes can move very large values and cause major concealment challenges [014, 134, 174].
- FIU and police analysis report focused, lower volume SARs and investigations in the investment and/or capital markets space, with growing analytical attention – authorities treat such cases as high priority because of scale and cross-border complexity [014, 134, 174].
- Since the previous FCTA [002, 003], scrutiny of capital markets money laundering has intensified. Recent analysis by the UK FCA reports a sharp rise in SARs related to capital-markets money laundering in the UK, albeit with uneven coding and data quality. While these findings are UK-specific, the weaknesses the FCA identifies – notably transaction-monitoring that is not tailored to capital-markets activity – are likely to be informative for the Netherlands [014].
- Experts have signalled recurring operational blind-spots in the securities settlement chain – notably omnibus/pool custody arrangements and limited visibility of natural persons behind pooled positions – which reduce whole-chain traceability and complicate attribution [001].

MODI OPERANDI

Given the technical and multi-stage nature of capital-markets abuse, the modi operandi below are organised according to the three classic ML phases (placement, layering, integration) [16]. The principal modi operandi in these phases include (non-exhaustive).

Placement

- Using private placements, pre-IPO allocations or fund subscriptions to introduce illicit proceeds while obscuring ultimate beneficial owners.
- Using third-party payments or unexplained funding (including via brokers, PSPs or counterparties in offshore/secrecy jurisdictions) to place value into trading or fund accounts.

[16] Modi operandi are grouped by the phase(s) they most commonly support; several modi operandi may operate across multiple phases in practice.

- Using investments in securities, funds or hard-to-price instruments (e.g. emission-allowance) to bring proceeds onto market rails where valuation or market opacity facilitates placement.

Layering

- Using nominee, omnibus and multi-tier custody arrangements to fragment investor visibility and conceal beneficial ownership.
- Using opaque OTC or bespoke transactions together with coordinated artificial trading (for example wash trading, parking, round-trip trades) to obscure pricing, volumes and the origin of assets and funds.
- Using free-of-payment (FOP) settlements, custody give-ups and routing via unrelated third parties to break the direct cash-for-asset trail and complicate settlement tracing.

Integration

- Using temporary transfers or structuring around corporate-action dates to extract economic value (for example dividend-stripping) and create a market-based rationale for payouts.
- Using rapid redemptions, transfers or payouts to unrelated beneficiaries or to jurisdictions inconsistent with investor profiles to reintroduce integrated proceeds.
- Converting apparent trading gains into other assets or legitimate channels (e.g. corporate investments) to finalise integration under a plausible economic rationale.

FEATURES

Regarding placement, using subscription-style entry points (private placements, fund subscriptions and investments in non-listed private companies) and unexplained third-party payments – often routed via brokers, PSPs or counterparties in offshore/secrecy jurisdictions – to introduce illicit value onto market rails while obscuring UBOs. OTC pricing opacity affects valuation transparency rather than ownership, but can be exploited to mask initial valuation and provenance.

Concerning layering, nominee, omnibus and multi-tier custody arrangements fragment investor visibility and conceal beneficial ownership. Opaque or bespoke trades, combined with coordinated patterns (e.g. wash trading, parking or round-trip trades), hide pricing and volumes and misrepresent market activity. Brief holding periods and rapid in-and-out trading are deliberate short-term obfuscation tactics. Free-of-payment (FOP) settlements, custody give-ups and routing via unrelated third parties can transfer value without a clear payment leg – effectively legitimising ill-gotten gains and breaking the cash-for-asset trail – and complicate settlement tracing. Multi-jurisdictional corporate chains, repeated use of nominee directors and Trust & Company Service Provider addresses reduce visibility of the legal owner; shared contact details or device identifiers reveal operational links that mask the actual beneficiary or controller.

Pertaining to integration, temporary transfers around corporate-action events (for example to exploit dividend/tax treatments or extract value) can create a market-based rationale for payouts. Rapid redemptions, transfers to unrelated beneficiaries or destinations inconsistent with investor profiles and converting apparent trading gains into other assets or corporate actions are used to finalise reintegration under a plausible economic narrative.

PREDICATE OFFENCES

Within securities markets, insider trading and market manipulation are both proceeds-generating and enabling offences: they produce illicit trading gains that can be realised, reinvested or transferred through settlement and payment flows in market channels, and they create a market-level rationale for anomalous activity (for example large or rapid position changes). Such activity can facilitate layering when combined with nominee/omnibus custody, free-of-payment transfers or third-party settlement routing [014].

Additionally, client-facing fraud involves sham investment advisers or counterfeit intermediaries that induce investors into schemes (for example pump-and-dump, penny-stock scams, pyramid or Ponzi schemes) which generate proceeds from victimised investors. Transaction-facing fraud involves sham investment strategies executed via rapid buy/sell patterns (for example wash trading, mirror or round-trip trades) that create the appearance of legitimate trading, inflate liquidity or obscure the money trail – functioning as layering or market-manipulation mechanisms that hide provenance and misrepresent market activity. Fraud therefore functions as both a proceeds-generating and an enabling offence [014].

Further, proceeds derived from corruption (for example embezzlement or bribery) are a direct source of launderable funds and can also facilitate concealment, meaning corruption operates as both a proceeds-generating and an enabling offence. Misappropriated funds may be invested in securities, while corrupt insiders or networks can arrange sham transactions, abuse market access or organise nominee and custody arrangements that obscure beneficial ownership and the origin of assets and funds [014].

Other predicate offences that could be linked to the modi operandi and risk factors of Money laundering via securities investment products and capital markets are: Organised crime and Tax crimes.

3
Appendices

A | Source list

The source list contains 279 entries. During the FCTA project we worked from a larger working set of 560 individual materials. The principal reason for the difference in counts is that the 'Jurisprudentie AMLC' item (see Source ID 274) is presented here as a single consolidated entry, while it actually comprises 282 separate jurisprudence records. As a result, the working total (560) and the published list (279) differ even though they cover the same underlying evidence base.

001 Expert input, NVB, 2026
002 Financial Crime Threat Assessment of The Netherlands 2023-24, NVB, 2024
003 Financial Crime Threat Assessment for banks, NVB, 2024
004 5 ways criminals launder money through real estate, First AML, 2022
005 A Guide to 'The Original 6AMLD': An Update on the EU's AML Criminal Law Directive, Comply Advantage, 2023
006 A Guide to Anti-Money Laundering for Crypto Firms, Comply Advantage, 2023
007 A Guide to Real Estate Money Laundering, FOCAL, 2025
008 A Risk Scoring Model for Managing Money Laundering Transactions, GCFFC, 2025
009 ABN Amro nam 18 miljoen euro in contanten van drugscriminelen aan, FTM, 2024
010 AML compliance in the remittance industry, Comply Advantage, 2025
011 AML/CTF in Real Estate, ANTI-MONEY LAUNDERING, 2023
012 Anti-money laundering guidance for remittance service providers, UNCDF, 2025
013 Arts and Antiques, CIFA-BC, 2025
014 Assessing and reducing the risk of Money Laundering Through the Markets (MLTM), FCA, 2025
015 Authorities struggle to shut illegal gambling sites that target European players, FTM, 2025
016 Automobile and Transportation-Linked Criminality: Understanding the Risks, Ripjar, 2024
017 Banking crypto clients: better monitoring through adoption, Compliance, Ethics & Sustainability Journal, 2025
018 Basel AML Index 2024: 13th Public Edition: Ranking money laundering risks around the world Draft | Embargoed until 2, Basel Institute, 2024
019 Battle Against Hidden Transactions: Understanding Hawala Money Laundering, Financial Crime Academy, 2025
020 BENEFICIAL OWNERSHIP OF LEGAL PERSONS, FATF, 2023
021 Beneficial ownership registries and trade-based money laundering, CIFA-BC, 2024
022 BEST PRACTICES ON COMBATING THE TERRORIST FINANCING ABUSE OF NON-PROFIT ORGANISATIONS, FATF, 2023
023 Bitcoinbendes scammen honderden Nederlanders: "Ik zie dat geld nooit meer terug, of wel?", FTM, 2025
024 Bulletin Professional Money Laundering Facilitators, Egmont Group, 2019
025 Case Studies: How organised criminals have exploited dealers in precious metals and stones to launder the proceeds of their crimes and how you can prevent this happening in your business, Artic Intelligence, 2025
026 Case Studies: How organised criminals have exploited real estate agents and property developers to launder the proceeds of their crimes and how you can prevent this happening in your business, Artic Intelligence, 2025
027 Cash Compensatie Model in arbeidsintensieve branches: kennisdocument, Politie/FIU/NCT/FIOD/AMLC, 2025
028 Cash Intensive Businesses: Exemplary Methods of Money Laundering in Non-Banks, Financial Crime Academy, 2025
029 Cash-based money laundering, FCA, 2023
030 Cash-intensive businesses and red flags, First AML, 2025
031 Casino AML Compliance: The 2025 Ultimate Guide, Sanctions.io, 2025
032 Cleaning Up the Market: Addressing Money Laundering in Real Estate, Financial Crime Academy, 2025
033 Combating the exploitation of international students as money mules, AUSTRAC, 2024
034 Combating the sexual exploitation of children for financial gain, AUSTRAC, 2023
035 Combating the sexual exploitation of children for financial gain activity indicators report, AUSTRAC, 2023
036 Commodities en witwassen: de graansector, AMLC, 2023
037 Complex Proliferation Financing and Sanctions Evasion Schemes, FATF, 2025
038 Comprehensive Update on Terrorist Financing Risks, FATF, 2025
039 Consultation Paper : Proposed RTS in the context of the EBAs response tot he EC Call for advice on new AMLA mandates, EBA, 2025
040 Contant geld, AMLC, 2023
041 Corruption and Money Laundering in International Arbitration, Basel Institute, 2019
042 Countering Ransomware Financing, FATF, 2023
043 Cracking Down on Illicit Funds: Real Estate Money Laundering Schemes Exposed, Financial Crime Academy, 2025
044 Criminal Networks in EU Ports, Europol, 2024
045 Criminal Networks in Migrant Smuggling, Europol, 2023
046 Criminaliteit en veiligheid in mainports, WODC, 2019
047 Criminality in The Netherlands, The Organized Crime Index, 2023
048 Criminelen haken voor een prik aan bij het financiële netwerk SWIFT, FTM, 2023
049 Cross-Border Payments Survey Results on Implementation of the FATF Standards, FATF, 2021
050 Crowdfunding for Terrorism Financing, FATF, 2023
051 Crypto Assets Risk Indicators for Financial Institutions, The Joint Chiefs of Global Tax Enforcement (J5), 2024

052 Cryptocurrency, CIFA-BC, 2023
053 Crypto Crime Reaches Record High in 2025 as Nation State Sanctions Evasion Moves On Chain at Scale, Chainanalysis, 2026
054 Cyber Dependent and Cyber Enabed Financial Crime, CIFA-BC, 2025
055 Cyber-Enabled Fraud: Digitalization and Money Laundering, Terrorist Financing and Proliferation risks, FATF, 2026
056 Cybersecuritybeeld Nederland, NCTV, 2024
057 De CO2-handel is een 'ideaal instrument' voor witwassers, FTM, 2025
058 De goudhandelaar, FIU, 2022
059 Decoding the EU's most threatening criminal networks, Europol, 2024
060 Deepfakes and synthetic media in the financial system: assessing threat scenarios', Carnegie Endowment for International Peace, 2023
061 Detect and report cuckoo smurfing, AUSTRAC, 2023
062 Detecting and stopping forced sexual servitude in Australia, AUSTRAC, 2023
063 Detecting and stopping ransomware payments, AUSTRAC, 2023
064 Detecting, Disrupting and Investigating Online Child Sexual Exploitation, FATF, 2024
065 DIRECTIVE (EU) 2024/1640 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Europese Commissie, 2024
066 'Dirty money, pretty art': Witwassen en ondermijning in tijden van financialisering van kunst, University College Maastricht, 2021
067 Dossier drugscriminaliteit, CCV, 2025
068 Dossier Mensenhandel en (seksuele) Criminele uitbuiting, CCV, 2024
069 Dossier vastgoedcriminaliteit, CCV, 2025
070 Douane jaarplan 2025, Douane, 2024
071 Dreigingsbeeld Milieucriminaliteit 2024, Strategische milieukamer, 2024
072 Dreigingsbeeld Terrorisme Nederland Juni 2025, NCTV, 2025
073 Drug Trafficking, CIFA-BC, 2025
074 Drugscriminelen in hele land actief met hypotheekfraude, FD, 2024
075 EBA REPORT ON ML/TF RISKS ASSOCIATED WITH PAYMENT INSTITUTIONS, European Banking Authority (EBA), 2023
076 Economic Crime Areas of Research Interest – NECC (NCA) & Home Office 2025, NECC, 2025
077 Een web van haat – De online grip van extremisme en terrorisme op minderjarigen, AIVD, 2025
078 Effecten op de online gokmarkt, Kansspelautoriteit, 2024
079 Enterprising criminals: Europe's fight against the global networks, Europol, 2023
080 Environmental Crime Threat Assessment, Politie (ILT-IOD), 2024
081 ESG en witwassen, AMLC, 2023
082 EU Drug Market Analysis, Europol, 2024
083 EU ETS: Detecting, preventing, and fighting money laundering in emissions trading, Umwelt Bundesarmt, 2023
084 EU-hoofdaanklager: Criminelen verdienen miljaren per jaar met 'risicovrije' belastingfraude, FTM, 2024
085 Europese Unie (EU) neemt 20ste sanctiepakket aan tegen Rusland, Rijksoverheid, 2025
086 European Union Terrorism Situation and Trend report 2025, Europol, 2025
087 Europol: Money Laundering at the Heart of a Multi-Billion EU Criminal Economy, OCCRP, 2023
088 Fact Sheet 2023 Results, Empact, 2024
089 Factsheet contant geld, AMLC, 2025
090 FATF Evaluatie, FATF, 2022
091 FATF Glossary, FATF, 2026
092 FATF recommendations 2025, FATF, 2025
093 FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, FATF, 2020
094 FEC – Kennisdocument Dividenstripping Extern (2021), FEC, 2021
095 Final report on amending Guidelines on MLTF risk factors, EBA, 2024
096 Financial Crime Principles for Correspondent Banking, Wolfsberg Group, 2023
097 Financial inclusion and Anti-money laundering and terrorist financing measures, FATF, 2025
098 Financial Sanctions Evasion Typologies: Russian Elites and Enablers, GOV.UK, 2022
099 Financieel en fiscaal rechercheren in een digitale internationale wereld, FIOD, 2021
100 Financing of terrorism, COE, 2025
101 FIOD Jaarverslag 2024, FIOD, 2025
102 Following The Treasure Trail: Luxury Goods And Financial Crime, Mondaq, 2022
103 Fraude met vastgoed, OM, 2025
104 From cash to crypto: Towards a consistent regulatory approach to illicit payments, BIS, 2026
105 Geldezel aanpak, CCV, 2025
106 General Issue, CIFA-BC, 2024
107 Georganiseerde criminaliteit en ondermijning, WODC, 2020
108 Global Advisory on Russian Sanctions Evasion, Multilateral REPO Task Force, 2025
109 Global Financial Fraud Threat Assessment 2026, Interpol, 2026
110 Global money mule networks: Using behavioural and device intelligence to shine a light on money laundering, BioCatch, 2024
111 Global Risks Report 2025, World economic forum, 2025
112 Good Practices SIRA, DNB, 2025
113 Good Practices Wwft Q&As and Good Practices, DNB, 2024
114 Group statement on Developing an Effective AML/CTF Programme, Wolfsberg Group, 2020
115 GUIDANCE FOR A RISK-BASED APPROACH – BENEFICIAL OWNERSHIP AND TRANSPARENCY OF LEGAL ARRANGEMENTS, FATF, 2024
116 GUIDANCE FOR A RISK-BASED APPROACH – REAL ESTATE SECTOR, FATF, 2022
117 Het vestigingsklimaat voor drugscriminaliteit in Nederland, Universiteit Tilburg, 2022
118 Honderden vonnissen ontrafeld tot waardevolle witwastypologieën, FIU, 2025
119 How crime is accelerated by AI, Europol, 2025
120 How crime is nurtered online, Europol, 2025
121 How Criminals Exploit Money Remittance: Understanding The Risks And AML Solutions, AML Watcher, 2024
122 How do organised criminals exploit dealers in precious metals and stones to launder the proceeds of their crimes and what can you do to prevent this happening in your business?, Artic Intelligence, 2025
123 How do organised criminals exploit real estate professionals to launder the proceeds of their crimes and what can you do to prevent this happening in your business?, Artic Intelligence, 2025
124 How luxury goods are exploited in money laundering schemes, Fintech Global, 2024
125 How suspected Iranian spy ships docked in Antwerp for years, FTM, 2025
126 Human Trafficking and Child Exploitation, CIFA-BC, 2024
127 Illicit Trade Report 2023, WCO, 2023
128 Illegal phoenix activity indicators report, AUSTRAC, 2023
129 Illegal wildlife trafficking financial crime guide, AUSTRAC, 2023
130 Illicit Financial Flows from Cyber-Enabled Fraud, FATF, 2023
131 Illicit Money In, Clean Money Out: Money Laundering Through ATMs, Cense, 2025
132 Integrity Supervision in Focus 2025, DNB, 2025
133 Internet organised crime threat assessment (IOCTA), Europol, 2024
134 Jaaroverzicht 2024, FIU, 2025
135 Jaaroverzicht Criminele Geldstromen 2024, OM, 2024
136 Jaarplan 2026, FEC, 2026
137 Jaarrapportage Maatschappelijk Overleg Betalingsverkeer, Maatschappelijk Overleg Betalingsverkeer, 2024
138 Jaarverslag 2023 FIU Duitsland, FIU Duitsland, 2024
139 Jaarverslag 2024, AIVD, 2025
140 Jaarverslag 2024, FEC, 2024
141 Jaarverslag 2025, Infobox Crimineel en Onverklaarbaar Vermogen, 2025
142 Kabinet komt met wetsvoorstel voor toekomstbestendige sanctiemaatregelen, Rijksoverheid, 2025
143 Kamerbrief nieuwe anti-witwasaanpak, MinFin, 2025
144 Kansspelen – Enkele cijfers op een rij – Factsheet, WODC, 2025
145 Kennisdocument cryptobetaalkaarten en criminele geldstromen, RIEC, 2024
146 Kennisdocument ondergronds bankieren, RIEC, 2023
147 Leaked Letters Give Insight Into Anti-Money Laundering Gaps at Swiss Bank Reyl, OCCRP, 2025
148 Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures, Europol, 2024
149 Misuse of Citizenship and Residency by Investment Programmes, FATF, 2023
150 Misuse of professional services, CIFA-BC, 2023
151 Mogelijke omzeiling sancties tegen Rusland door jonge, kleine bedrijven, CBS, 2024
152 Mondiale bank van de onderwereld wast miljoenen wit met hulp van ING, FTM, 2023
153 Money Laundering and Terrorist Financing in the Art and Antiquities Market, FATF, 2023
154 Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling, FATF, 2022
155 Money laundering as a service: Investigating business like behavior in money laundering networks in the Netherlands, Trends in Organised Crime, Kramer et al., 2023
156 Money Laundering from Environmental Crime, FATF, 2021
157 Money Laundering from Fentanyl and Synthetic Opioids, FATF, 2022
158 Money Laundering in Property Markets: Techniques, Red Flags, and Compliance, AML Network, 2025
159 MONEY LAUNDERING IN THE HIGH VALUE GOODS SECTOR, Themis, 2022
160 Money Laundering in the Luxury Goods Market: A Comprehensive Analysis!, Fin Telegram, 2025
161 Money Laundering Risks in Commercial Real Estate: An Analysis of 25 Case Studies, FACT Coalition et al., 2024
162 Money laundering through online gambling, Comply Advantage, 2024
163 Money laundering through the gambling industry, Basel Institute, 2022
164 Money Laundering, Terrorist Financing Typologies, One AML, 2022
165 Money Muling, Europol, 2025
166 Monitoringsrapportage online kansspelen, Kansspelautoriteit, 2025
167 NATIONAL ECONOMIC CRIME CENTRE ANNUAL REPORT, NECC, 2025
168 Navigating the Gray: A Deep Dive into Alternative Remittance Systems, Financial Crime Academy, 2025
169 NDIS fraud financial crime guide, AUSTRAC, 2023
170 Nederlandse bedrijven omzeilen Iran-sancties via Clandestiene brievenbusconstructies, FTM, 2024
171 Nieuwe risico-inschatting witwassen en financieren van terrorisme bij kansspelen, WODC, 2026
172 Nieuwe vormen van oplichting en fraude, WODC, 2020
173 NRA terrorismefinanciering, WODC, 2023
174 National Risk Assessment Witwassen 2023, WODC, 2023
175 Oligarchen, miljonairs, en criminelen gebruiken Nederlandse rechtsvorm wereldwijd als dekmantel, FTM, 2023
176 Onderzoek naar illegaal gokken en witwassen, FIOD, 2025
177 Online gambling as a money laundering method, AMLC, 2021
178 Online Gambling Services, ANTI-MONEY LAUNDERING, 2024
179 Online gaming, CIFA-BC, 2023
180 Overzicht witwasindicatoren, AMLC, 2025
181 PARTNERING IN THE FIGHT AGAINST FINANCIAL CRIME: Data Protection, Technology and Private Sector Information Sharing, FATF, 2022
182 Politie onderschept miljoenen contant geld op de Nederlandse wegen, Politie, 2024
183 Precious Metals Money Laundering Red Flags, AML Square, 2025
184 Preventing misuse and criminal communication through payment text fields, AUSTRAC, 2023
185 Preventing the criminal abuse of digital currencies, AUSTRAC, 2023
186 Preventing the exploitation of emergency and disaster support payments, AUSTRAC, 2023
187 Preventing trade-based money laundering in Australia, AUSTRAC, 2023
188 Protecting the Prestige: Compliance with AML Requirements for Luxury Goods, Financial Crime Academy, 2025
189 Psychological Risk Factors for Money Laundering and Other Financial Crime, CIFA-BC, 2024
190 Q&A on the Sanctions Act for non-life insurance companies, DNB, 2022
191 Rapport Signalen fraude in de zorg 2023, Inspectie Gezondheidszorg en Jeugd, 2024
192 Real Estate Money Laundering: Methods, Vulnerabilities and Red Flags, AML Cube, 2025
193 Reassessing the Financing of Terrorism in 2025, RUSI, 2025

194 Recovering the International Proceeds of Crime through Inter-Agency Networks, FATF, 2023
195 Report: Money Laundering via Cryptocurrencies up 30% in 2021, OCCRP, 2022
196 Risico-indicatoren offshore vennootschappen, AMLC, 2022
197 Rusland en verdachte transacties, AMLC, 2022
198 Russia-Ukraine Circumvention of Financial Sanctions, CIFA-BC, 2022
199 Sanctions check, DNB, 2022
200 Sanctions evasion typologies and advisories, GOV.JE, 2025
201 Sanctions evasion: the art of hiding and not getting caught, LSEG, 2024
202 Sanctions Screening Guidance, Wolfsberg Group, 2019
203 Sectordocument internationale handel plastic afval, AMLC, 2024
204 Smokkel, TLN, 2025
205 Staat van mainport Rotterdam 2021, Inspectie Leefomgeving en Transport (ILT), 2021
206 STOCKTAKE ON DATA POOLING, COLLABORATIVE ANALYTICS AND DATA PROTECTION, FATF, 2021
207 STUDY ON ILLICIT FINANCIAL FLOWS ASSOCIATED WITH SMUGGLING OF MIGRANTS AND TRAFFICKING IN PERSONS FROM GLO.ACT PARTNER COUNTRIES TO EUROPE, UNODC, 2025
208 Supranational Risk Assessment Report, European Commission, 2022
209 System Prioritisation priorities, NCA, 2025
210 Targeted Report on Stablecoins and Unhosted Wallets: Peer-to-Peer Transactions, FATF, 2026
211 Terrorismefinanciering, FIOD, 2021
212 Terrorist Financing, ANTI-MONEY LAUNDERING, 2025
213 Terrorist Financing, CIFA-BC, 2024
214 Terrorist Financing Red Flags And Suspicion, Financial Crime Academy, 2025
215 Terrorist Threat Assessment for the Netherlands June 2025, NCTV, 2025
216 The Anatomy of Cash-Based Money Laundering Schemes, Number Analytics, 2025
217 The EU's priorities for the fight against serious and organised crime for EMPACT 2022-2025, EMPACT, 2021
218 The Hawala System – Its operations and misuse by opiate traffickers and migrant smugglers, UNODC, 2023
219 The IRS Criminal Investigation (CI) annual report, IRS, 2024
220 The Money Trail: How Criminals Exploit Real Estate for Money Laundering, Financial Crime Academy, 2025
221 The Money Trail: Unveiling Trade-Based Money Laundering Statistics, Financial Crime Academy, 2025
222 The Netherlands Country Financial Crime Dashboard, FCN, 2022
223 The Other Side of the Coin: An Analysis of Financial and Economic Crime. European Financial and Economic Crime Threat Assessment 2023, Europol, 2023
224 The prevention of money laundering and combating the financing of terrorism: Guidance for remote and non-remote casinos, Gambling Commission, 2025
225 The Real Estate Cover-Up: Unveiling Money Laundering Tactics, Financial Crime Academy, 2025
226 The risk of abuse of arbitration proceedings in jurisdictions where corruption is pervasive, JEC, 2023
227 The Sanctions Evasion Threat: Six Common Typologies All Compliance Officers Should Know, Institute for Financial Integrity, 2024
228 Themarapportage economische dreigingen 2022, NCTV, 2022
229 Threat Radar-2025, EFIPPP, 2025
230 Trade Based Money Laundering: uitdagingen en ontwikkelingen binnen de opsporing, AMLC, 2024
231 Trade-Based Money Laundering, ANTI-MONEY LAUNDERING, 2025
232 Trade-Based Money Laundering Techniques to Know, IFC; CBR, 2023
233 Trade-Based Money Laundering Trends and Developments, FATF; Egmont Group, 2020
234 Trade-Based Money Laundering: Risk Indicators, FATF; Egmont Group, 2021
235 TRAFFICKING AND MONEY LAUNDERING – Strategies Used by Criminal Groups and Terrorists and Federal Efforts to Combat Them, GAO, 2021
236 Trends for Financial Investigation, FEC, TBD
237 Tussen vrede en oorlog: De oorlog in Oekraine en de Russische dreiging in Europa, AIVD, MIVD, 2026
238 Typologieën, FIU, 2025
239 Typologies And Trends Of Terrorist Financing, Financial Crime Academy, 2025
240 Typologies: Sanctions and Trade Based Money Laundering, FIU, 2023
241 Uncovering Cash-Based Money Laundering Tactics, Number Analytics, 2025
242 Uncovering the Hidden Economy: Demystifying Underground Banking, Financial Crime Academy, 2025
243 Underground banking in relation to organised crime in the Netherlands, WODC, 2025
244 Understanding Hawala Based Money Laundering: Mechanisms, Challenges, and Strategies for Combat, URPR, 2024
245 Understanding informal remittances, Central Banking, 2022
246 Understanding money laundering in casinos, Comply Advantage, 2024
247 Understanding money laundering in real estate, Comply Advantage, 2023
248 Unorthodox Money Channels: Analyzing Informal Value Transfer Systems, Financial Crime Academy, 2025
249 Unveiling the Dark Secrets: Money Laundering Through Casinos Exposed, Financial Crime Academy, 2025
250 Unveiling the Tactics: Trade-Based Money Laundering Typologies Demystified, Financial Crime Academy, 2025
251 UPHOLDING INTEGRITY: The causes and trends of corruption risk in Europe, LUISS, 2025
252 USE OF CASH FOR MONEY LAUNDERING PURPOSES: A MODERN-DAY PERSPECTIVE, FSREG, 2025
253 Vastgoed- en hypotheekfraude: de criminele financiële snelweg van onder- naar bovenwereld, NVB, 2022
254 Vastgoed en hypotheekfraude: hoe crimineel geld de woningmarkt binnendringt, Bijzonder strafrecht, 2025
255 Veiligheidsagenda 2023-2026, Politie, 2022
256 Verschijningsvormen van malafide goudhandel, NSOC, 2023
257 VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, FATF, 2021
258 Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, FATF, 2020
259 Wetgevingsbrief DNB 2023: knelpunten in wet- en regelgeving op het terrein van de financiële markten, DNB, 2023
260 What is Alternative Remittance System in Anti-Money Laundering?, AML Network, 2025
261 What is Hawala System in Anti-Money Laundering?, AML Network, 2025
262 What is Regulatory Arbitrage in Anti-Money Laundering?, AML Network, 2025
263 What is Value Laundering in Anti-Money Laundering (AML)?, AML Network, 2025
264 Who is this – how scammers exploit regulatory weakness to pocket your money, FTM, 2025
265 Wildlife crime, CIFA-BC, 2023
266 Witwassen bij PSPs, AMLC, 2022
267 Witwassen en zorgfraude, AMLC, 2024
268 Witwassen met Vastgoed, AMLC, 2022
269 Witwassen via Trade Based Money Laundering, AMLC, 2025
270 Witwastechnieken, AMLC, 2023
271 Wolfsberg Anti-Bribery and Corruption Programme Guidance, Wolfsberg Group, 2023
272 World atlas of illicit flows, Interpol; RHIPTO; GIATOC, 2019
273 Zwart erin, wit eruit: witwassen via geldautomaten, Kennisplatform Ondermijning, 2025
274 Jurisprudentie AMLC (period 2020-2025; total of 282 sources. Detailed list of URLS available at request), AMLC, 2020-2025
275 Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, European Council, 2014
276 DIRECTIVE (EU) 2018/1673 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on combating money laundering by criminal law, European Parliament; European Council, 2018
277 Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Text with EEA relevance), CELEX: 32024R1624 (AMLR), European Parliament; European Council, 2024
278 Wet ter voorkoming van witwassen en financieren van terrorisme (Anti Money Laundering and Counter Terrorist Financing Act), Staatsblad, 2026
279 Wet toezicht trustkantoren 2018 (Trust Offices Supervision Act), Staatsblad, 2025

B | Abbreviations

AIVD | General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst)
AI | Artificial Intelligence
AIS | Automatic Identification System
AML | Anti-Money Laundering
AMLA | Anti-Money Laundering Authority
AMLC | Anti-Money Laundering Centre
AMLR | Anti-Money Laundering Regulation
AP | Dutch Data Protection Authority (Autoriteit Persoonsgegevens)
ATMs | Automated Teller Machines
CBS | Statistics Netherlands (Centraal Bureau voor de Statistiek)
CCM | Cash Compensation Model
CFT | Countering the Financing of Terrorism
DNB | De Nederlandsche Bank (Dutch Central Bank)
DEX | Decentralised Exchange
EEA | European Economic Area
EAEU | Eurasian Economic Union
EU | European Union
FATF | Financial Action Task Force
FEC | Financial Expertise Centre
FIU/FIU-NL | Financial Intelligence Unit Netherlands
FIOD | Fiscal Information and Investigation Service (Fiscale Inlichtingen- en Opsproingsdienst)
FCTA | Financial Crime Threat Assessment
NL FCTA | Financial Crime Threat Assessment of the Netherlands
FCTA for banks | Financial Crime Threat Assessment for banks
FCA | Financial Conduct Authority
FTZ | Free-Trade Zone
HRTC | High Risk Third Countries
IBAN | International Bank Account Number
IRAP | Internal Risk Assessment Platform
ID | Identification/identity documentation
IMF | International Monetary Fund
IVTS | Informal Value Transfer Systems
Ksa | Dutch Gambling Authority (Kansspelautoriteit)
KRI/KRIs | Key Risk Indicators
KYC | Know Your Client
KYB | Know Your Business
KvK | Dutch Chamber of Commerce (Kamer van Koophandel)
LLM | Large Language Model
MiCAR | Markets in Crypto-Assets Regulation
MIVD | Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligeheidsdienst)
MO | Modus operandi/modi operandi
MO Category | Modus operandi category
MSB | Money Service Business
MVTS | Money Value Transfer Service(s)
NP | National Police (Nationale Politie)
NPO | Non-Profit Organisation
NRA | National Risk Assessment
NVB | Dutch Banking Association (Nederlandse Vereniging van Banken)
NGO | Non-Governmental Organisation
OM | Public Prosecution Service (Openbaar Ministerie)
OTC | Over-The-Counter
PEP | Politically Exposed Person
PSP | Payment Service Provider
RIEC | Regional Information and Expertise Centre
SAR | Suspicious Activity Report
STR | Suspicious Transaction Report
SIRA | Systematic Integrity Risk Assessment
STAK | Foundation for administering shares (Stichting Administratiekantoor)
SoF | Source of Funds
TBML | Trade-Based Money Laundering
TCSP | Trust and Company Service Providers
TF | Terrorism Financing
UBO | Ultimate Beneficial Owner
UTR | Unusual Transaction Report
VASP | Virtual Asset Service Provider
VAT | Value Added Tax
WODC | Research and Documentation Centre (Wetenschappelijk Onderzoek- en Datacentrum)
Wtt | Trust Offices Supervision Act (Wet toezicht trustkantoren)
Wwft | Dutch Anti-Money Laundering and Countering the Financing of Terrorism Act (Wet ter voorkoming van witwassen en financieren van terrorisme)

C | DNB Terminology

DNB SIRA Good Practices versus FCTA 2026

There is a clear need to clarify the relation between the FCTA 2026 terminology and DNB terminology used in the DNB Systematic Integrity Risk Assessments (SIRA) Good Practices.

The DNB SIRA Good Practices [112] provides supervisory, institution-level guidance, showing institutions how to convert scenarios into controls and KRIs. The FCTA 2026, on the other hand, produces a national, sector-level threat taxonomy, including red flags that banks can detect.

We decided to retain the FCTA 2026 methodology and analytic steps, while aligning the terminology with DNB's 'Risk factors'.

Important considerations are:

- Scenario-based thinking, as described in DNB SIRA Good Practices, follows the same premise as the FCTA 2026 methodology: both focus on the systematic identification of risk factors and red flags (or manifestations) to underpin scenario development and risk assessment.
- Key Risk Indicators (KRIs) are not explicitly referenced in the FCTA 2026, albeit the methodology does make use of actionable data points banks can use to develop KRIs.
- Risk factors, on the other hand, are part of the primary output of the FCTA 2026's, as it uses the previously called 'indicators'; the terminology has since been revised to align with DNB's SIRA Good Practices and the forthcoming AMLR [277], which adopts the same language.

Term	Definition in DNB SIRA Good practices	Alignment with FCTA 2026 methodology and terminology
Scenarios	Detailed, well-developed descriptions of how a risk can concretely materialise (sequence of steps/chain of events).	Aligns with the outcomes of the FCTA 2026: we aim to identify the combination of Risk factors that together can be seen as a red flag (or manifestation) of a certain type of money laundering. FCTA is less focussed on the sequence/chain of events, and more focussed on identifying the red flags and risk factors that are part of such a sequences.
Manifestation	Concrete manifestations of a risk (types of behaviours or outcomes) – that often form the basis for scenario design.	Similar to red flags in FCTA 2026: A risk factor or combination of risk factors that is/are associated with money laundering and that banks are exposed to and that are identifiable for banks.
Indicators/ AML Risk factors	Signals or observations that may indicate a manifestation (e.g. cash in foreign currencies, unexplained flows).	Similar to risk factors in FCTA 2026: Features predicate offences and/or the money laundering modus operandi, or combinations thereof, that may indicate red flags. The FCTA 2026 formerly used the term 'indicators'; the terminology has since been revised to 'Risk factors' to align with DNB's SIRA Good Practices and the forthcoming AMLR,277 which adopts the same language.
Key Risk Indicators (KRIs)	Measurable metrics/thresholds derived from data analyses that trigger monitoring and Event Detection and Response (EDR) initiatives.	The FCTA 2026 aims to identify standardised datapoints (client behaviour, sectors, product or client segments) that are associated with a threat and enable banks to use these datapoints to develop appropriate KRIs.

D | MO categories list

The list of 14 modus operandi (MO) categories is based on desk research and expert input. All MO categories can both conceal value (e.g. by obscuring origin, ownership or the transactional trail) and transport value (e.g. via cross-border, physical or other forms of value transfer); the exact role an MO plays in the money laundering process depends on the context.
The MO categories are listed in alphabetical order.

Money laundering via cash

Money laundering via cash involves moving and concealing illicit proceeds through physical cash flows generated by individuals or businesses. Perpetrators blend or manipulate cash receipts to reduce transactional traceability and create the appearance of legitimate income. This exploits the limited electronic trail and weaknesses in cash handling to integrate unlawful funds into the formal financial system.

Money laundering via corporate and legal entity networks

Money laundering via corporate and legal entity networks involves deliberately using companies, trusts and other legal vehicles to conceal ultimate beneficial ownership, fabricate commercial activity and layer illicit proceeds through intercompany transfers, false invoices and circular flows, with the effect of disguising the origin of funds and impeding regulatory oversight and tracing.

Money laundering via gambling and/or (online) casinos

Money Laundering via gambling and/or (online) casinos involves deliberately using gambling services – including land-based and online casinos, betting sites, poker rooms and other gaming or gambling platforms – to launder illicit funds by converting cash or tainted balances into purported gambling winnings. The method exploits high transaction volumes, limited client verification and cross-border payment flows to integrate unlawful proceeds into the financial system.

Money laundering via high value goods and commodities

Money Laundering via high value goods and high value commodities involves converting proceeds into luxury goods, art, precious metals or vehicles to store and transfer value outside the banking system. These assets facilitate value movement, resale and price manipulation to obscure illicit origins.

Money Laundering via illegal trafficking and transportation networks

Money Laundering via illegal trafficking and transportation networks involves integrating proceeds from criminal activity into logistics and transport routes to conceal their origins. Criminal networks exploit transshipment points, corrupt officials and cash couriers to move value both physically and electronically. In the Dutch context, main ports – notably the Port of Rotterdam and Amsterdam Airport Schiphol – can be exploited as high volume transshipment and storage hubs. Bonded warehouses, free-zones, containerised flows and multimodal connections create opportunities to commingle illicit consignments with legitimate cargo, obscure provenance and facilitate onward movement through complex supply chains.

Money laundering via jurisdictional arbitrage

Money Laundering via jurisdictional arbitrage involves exploiting differences in laws and regulations, supervision and enforcement between jurisdictions to move prohibited funds through weakly regulated or opaque financial centres. Perpetrators fragment and layer transactions across borders to exploit regulatory gaps and hamper tracing.

Money laundering via professional facilitators and money mule networks

Money laundering via professional facilitators and money-mule networks involves engaging professionals (accountants, lawyers, bankers, notaries, trusts, and other gatekeepers) and recruited individuals to create paperwork, open accounts, or move funds on behalf of criminals. Professional criminal facilitators might create networks of individual money mules to launder proceeds, with those money-mule networks receiving and forwarding illicit funds to create distance between the original source and the final beneficiary, frequently operating as 'money laundering as a service'.

Money laundering via real estate and property transactions

Money laundering via real estate and property transactions involves purchasing, developing or selling property – including both commercial and non-commercial real estate – to integrate illicit funds, often through over- or under-valuation, nominee buyers, mortgage fraud or rapid resale schemes. Real estate provides a high value, durable asset class that can absorb and legitimise large sums.

Money laundering via securities investment products and capital markets

Money laundering via securities, investment products and capital markets involves channelling illicit funds into securities, funds or capital-markets transactions to create a veneer of lawful investment income. Abuse techniques exploit the opacity of market actors and structures – brokers, fund managers/advisers, custodians and other intermediaries – which can obscure ultimate beneficial owners and complicate attribution. Perpetrators use complex legal, corporate or fund arrangements and investments in non-listed private companies to place and conceal proceeds. They also exploit omnibus or pooled custody arrangements to fragment investor visibility and facilitate layering and integration. In some markets, over-the-counter (OTC) trades introduce price opacity that helps mask valuation and provenance. The high velocity of funds and rapid cross-border settlement enables quick movement of large values, aiding layering and concealment.

Money laundering via underground banking or via informal remittance systems

Money laundering via underground banking or via informal remittance systems involves using trust-based, non-bank remittance networks to transfer value without formal banking records. These systems rely on informal settlement and minimal documentation, enabling fast cross-border movement and evasion of surveillance.

Money laundering via virtual assets

Money laundering via virtual assets (including crypto assets) is the process of concealing the illicit origin of criminal proceeds by using cryptocurrencies, stablecoins and tokenised assets, exploiting the high speed borderless and pseudonymous nature of blockchains.

Sanctions evasion

Sanctions evasion involves using deceptive tactics such as shell and front companies, intermediaries, sudden ownership changes, strawmen and legal loopholes to conceal the involvement of sanctioned persons or jurisdictions, often routing funds through unnecessarily complex multi-jurisdictional payment chains to obscure the trail and maintain a façade of compliance.

Terrorism financing

Terrorism financing involves providing, moving or concealing funds to support terrorist activity through – often small –, seemingly legitimate transactions and non-transparent channels, exploiting legal loopholes and rapid, complex routing to disguise their purpose. TF primarily concerns the concealment of the intended use or ultimate beneficiary of funds rather than necessarily concealing the origin. It is increasingly decentralised and may be self-financed by lone actors, petty crime or licit sources, and can in some contexts converge with organised crime or involve abuse of humanitarian aid in conflict zones, including environmental crime tied to exploitation, trade and trafficking of natural resources.

Trade-based money laundering

Trade-based money laundering involves embedding illicit value within international trade transactions through complex arrangements using goods and/or services, leveraging legitimate commercial flows and trade documentation across borders to conceal or legitimise the illicit origin, ownership and destination of funds.

E | Predicate offences list

The list contains a total of 23 predicate offences, including both 'proceeds-generating' offences (which produce the illicit funds targeted for laundering) and 'enabling' offences (which commonly facilitate the laundering process).
Of these 23 predicate offences, 21 are listed as 'criminal activity' in the DIRECTIVE (EU) 2018/1673 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on combating money laundering by criminal law [276], a directive that strengthens EU-wide efforts to combat money laundering by harmonising definition of related criminal offences and enhancing penalties.
In the FCTA 2026, the predicate offences 'espionage' and 'sanction evasion' are added based on the feedback during expert workshops to ensure coverage on sanction- and espionage-related threats. The predicate offences are listed in alphabetical order.

Arms trafficking
Arms trafficking refers to the unlawful import, export, sale, delivery, movement, or transfer of firearms, their essential components, or ammunition without proper authorisation. It also includes cases where such items are not properly marked for identification as required by law.

Corruption
Corruption refers to the deliberate abuse of power or position for personal gain, either in the public or private sector. It includes both passive corruption, where an official accepts or solicits undue advantages to act against their duties, and active corruption, where someone offers such advantages to influence an official's actions. Similar conduct in the private sector – offering or receiving undue benefits to breach professional duties – is also considered corruption.

Counterfeiting and piracy of products
Counterfeiting and piracy of products refers to the unauthorised production or distribution of goods that infringe intellectual property rights. This includes counterfeit trademark goods, which bear identical or deceptively similar trademarks without permission, and pirated copyright goods, which are unauthorised copies of protected works made without the consent of the rights holder.

Counterfeiting currency
Counterfeiting currency refers to the fraudulent creation, alteration, or distribution of currency with the intent to deceive and use it as genuine. This includes making or using counterfeit money, importing or exporting it with knowledge of its falsity, and possessing tools or materials specifically designed for counterfeiting.

Cybercrime
Cybercrime refers to criminal acts committed using information and communication technologies, including computers, networks, and the internet. It includes cyber-dependent crimes, such as hacking and ransomware, which target digital systems, and cyber-enabled crimes, like online fraud, piracy, and child exploitation, where traditional crimes are facilitated by digital means. Cybercrime often crosses borders, making international collaboration essential for investigation and enforcement.

Drugs trafficking
Drug trafficking involves the illegal cultivation, production, possession, transport, or sale of narcotic drugs or psychotropic substances as defined by international conventions and EU legislation. It also includes the handling of chemical precursors with the knowledge that they will be used for illicit drug manufacture.

Environmental crime
Environmental crime refers to unlawful acts that harm or are likely to harm the environment or human health or safety, including the illegal discharge of pollutants into air, water, or soil, improper waste management, and illegal shipment of waste. It also includes activities involving hazardous substances, destruction of protected species or habitats, and the use of ozone-depleting substances.

Espionage
Espionage is the covert collection of intelligence (information) or objects (for example products or machines). This information could involve sensitive (personal) data, technology, or state secrets. There are 2 types of espionage vectors: (a) state espionage (intelligence, when state actors are involved) or (b) industrial espionage (when commercial actors are involved).

Extortion
Extortion is a criminal act in which an individual or group unlawfully obtains money, goods, or services from a victim through coercion, threats, or abuse of power. It typically involves the use or threat of violence, causing financial loss to the victim, and may occur repeatedly or systematically, as in racketeering. Forms of extortion include blackmail, kidnapping for ransom, protection rackets and corrupt demands by officials.

Forgery
Forgery is the criminal act of making, copying, or using a false instrument – such as a document – with the intent to deceive someone into accepting it as genuine. The offence requires that this deception causes the person to act or refrain from acting to their own or another's detriment.

Fraud
Fraud refers to any intentional act or omission involving deception – such as presenting false or incomplete information, misusing funds, or concealing facts – that results in unlawful financial gain or damages the financial interests of others. It includes offences like misappropriation of public funds, VAT fraud and payment instrument fraud, as well as digital manipulation to cause unauthorised financial transfers.

Human trafficking
Human trafficking is the recruitment, transport, transfer, harbouring, or receipt of persons – often through coercion, deception, abuse of power, or exploitation of vulnerability – for the purpose of exploitation. This includes forced labour, sexual exploitation, slavery-like practices, criminal exploitation, or organ removal. Consent is irrelevant if any coercive means are used, and trafficking of children is punishable regardless of such means.

Insider trading & market manipulation
Insider trading involves the use or unlawful disclosure of non-public, price-sensitive information in the acquisition, disposal or recommendation of financial instruments. Market manipulation involves any conduct or trading practice that gives false or misleading signals about the supply, demand or price of financial instruments, or that secures prices at an abnormal or artificial level – including but not limited to wash trades, layering/spoofing, fictitious transactions, pump-and-dump schemes, or the deliberate dissemination of false or misleading information or rumours intended to distort market behaviour.

Kidnapping, illegal restraint and hostage-taking
Kidnapping is the unlawful taking and movement of a person against their will, typically by force or deception, with the intent to hold them for ransom, harm, or otherwise deprive them of their liberty. Illegal restraint involves confining or restricting a person's freedom of movement without lawful authority. Hostage-taking is the act of seizing or detaining a person and threatening to harm them to compel a third-party to act or refrain from acting.

Murder, grievous bodily injury
Murder is defined as the unlawful and intentional killing of one person by another. It involves three key elements: the act of killing (objective), the intent to kill or cause serious harm (subjective), and the fact that the act is punishable under law (legal).

Organised crime
Organised crime means a structured group of more than two persons, established or existing for a period of time and acting in concert with the aim of committing serious offences (as defined in national law) in order to obtain, directly or indirectly, a financial or material benefit. The concept covers participation in, direction of, facilitation of or assisting such groups, including activities to launder or conceal the proceeds of their criminal activities.

Piracy
Piracy consists of illegal acts of violence, detention, or depredation committed for private ends by individuals aboard a private ship or aircraft, directed against another vessel, aircraft, or persons on the high seas or outside any state's jurisdiction. It also includes knowingly participating in the operation of a pirate vessel or facilitating such acts.

Sexual exploitation
Sexual exploitation includes abusing or coercing someone (including through abuse of power) for sexual purposes, including through prostitution or pornography. It also covers acts involving children – for example engaging in sexual activities with a child, recruiting them for pornographic performances, soliciting children online for sexual purposes, or possessing and distributing child pornography.

Smuggling
Smuggling, in the EU context, refers to the intentional facilitation of the irregular movement of persons or the unlawful movement of goods into, through, or within an EU Member State, typically in exchange for financial or material gain. It includes migrant smuggling – providing means, resources or information to enable the irregular entry, transit or residence of a non-EU national, even with the migrant's consent – and goods smuggling, such as the concealment or illicit import/export of contraband (e.g. cigarettes, narcotics, weapons) to evade customs controls, duties, prohibitions or sanctions.

Tax crimes
Tax crimes involve the illegal evasion of direct or indirect taxes, such as income tax or VAT, by concealing income, falsifying records, or misrepresenting financial information, and include offences that obtain tax advantages through illicit means – for example fraudulently claiming tax refunds or orchestrating VAT-repayment schemes.

Terrorism
Terrorism refers to intentional acts – such as violence, destruction, or threats – committed to intimidate a population, coerce a government or international organisation, or destabilise a country's core structures. These acts include attacks on people or infrastructure, use of weapons or hazardous substances, and interference with essential services. Supporting terrorist groups, training, travel, and financing for terrorist purposes are also considered terrorist offences.

Theft (and robbery)
Theft is the unlawful taking of property with the intent to permanently deprive the owner of it, without using force, threats, or deception. It includes offences such as shoplifting, pickpocketing, car or bicycle theft, and animal theft. Robbery, by contrast, involves stealing from a person using physical force, threats, or weapons – for example, in muggings or armed robberies.

Trafficking in stolen goods
Trafficking in stolen goods in the EU refers to the intentional acquisition, possession, use, or transfer of property known to originate from criminal activity. It includes actions aimed at concealing the illicit origin, nature, source, location, or ownership of such property.

Dutch banking association
Gustav Mahlerplein 29-35
1082 MS Amsterdam
www.nvb.nl

strong banks
strong society