

International Comparative Legal Guides

Anti-Money Laundering 2026

A practical cross-border resource to inform legal minds

Ninth Edition

Contributing Editors:

Stephanie Brooker & M. Kendall Day

Gibson, Dunn & Crutcher LLP



iclg

Expert Analysis Chapters

- 1** Top Developments in Anti-Money Laundering Enforcement in 2025
M. Kendall Day, Stephanie Brooker, Ella Alves Capone & Sam Raymond, Gibson, Dunn & Crutcher LLP
- 9** US Toolkit for Addressing Anti-Money Laundering Risks at Non-US Financial Institutions
Brent Wible, Marietou Diouf & Jasmine Chen, White & Case LLP
- 15** Anti-Money Laundering in the Asia-Pacific Region: An Overview
Dennis Miralis, Kartia Zappavigna, Jack Dennis & Phillip Salakas, Nyman Gibson Miralis

Q&A Chapters

- 24** **Australia**
Dennis Miralis, Kartia Zappavigna, Jack Dennis & Phillip Salakas, Nyman Gibson Miralis
- 34** **France**
Thierry Marembert, Cécile Labarbe & Aaron Bass, Kiejman & Marembert
- 42** **Germany**
Dr. Dirk Seiler & Dr. Daisy Hullmeine, Herbert Smith Freehills Kramer LLP
- 51** **Greece**
Ilias Anagnostopoulos & Alexandros Tsagkalidis, Anagnostopoulos
- 60** **Ireland**
Darragh Murphy & Megan Hooper, McCann FitzGerald LLP
- 69** **Isle of Man**
Caitlin Gelder, Kathryn Sharman & Sinead O'Connor, DQ Advocates Limited
- 76** **Liechtenstein**
Dr. Stefan Wenaweser, Dr. Julia Köpf, Katharina Hasler & Julian Maikisch, Marxer Attorneys
- 86** **Malta**
Mario Zerafa & Karl Wismayer, Ganado Advocates
- 94** **Netherlands**
Brendan Newitt, Lisa van der Wal, Jantien Dekkers & Thomas Felix, De Roos & Pen
- 103** **Romania**
Simona Enache-Pirtea & Mădălin Enache, ENACHE PIRTEA & ASOCIATII S.p.a.r.l
- 112** **Singapore**
Gary Low & Terence Tan, Drew & Napier LLC
- 124** **Spain**
Arantxa Geijo & Francisco Estevan, Geijo Estevan Abogados
- 134** **Switzerland**
Cornelia Stengel & Lea Ruckstuhl, Kellerhals Carrard
- 144** **Türkiye**
Dr. Vahit Bıçak, Bıçak Law Firm
- 156** **United Kingdom**
Jonah Anderson & Anneka Randhawa, White & Case LLP
- 168** **USA**
M. Kendall Day, Stephanie Brooker, Ella Alves Capone & Sam Raymond, Gibson, Dunn & Crutcher LLP

Netherlands



Brendan
Newitt



Lisa van
der Wal



Jantien
Dekkers



Thomas
Felix

De Roos & Pen

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at the national level?

The legal authority is the Public Prosecution Service (PPS, *Openbaar Ministerie*).

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

Under Dutch law, the following are considered criminal offences: (i) concealing or disguising the true nature, origin, location, disposition or relocation of an object or concealing or disguising who is the rightful owner or holder of an object; or (ii) acquiring, possessing, transferring, converting, or using an object whilst one knows or should have reasonably suspected that this object derives – partially or wholly, and directly or indirectly – from any felony under Dutch law (*misdrrijf*). The wording of the criminal offences refers to the term “objects”. Objects include all property rights, such as shares, etc.

Money laundering offences are listed in title XXXA of the Dutch Criminal Code (DCC, *Wetboek van Strafrecht*). There are several types of money laundering offences: intentional money laundering (Sections 420*bis* and 420*bis*.1 DCC); culpable money laundering (Sections 420*quater* and 420*quater*.1 DCC); habitual intentional money laundering; and money laundering committed in the course of a business or profession (420*ter* DCC).

As described above, only a felony can be a predicate offence. Minor offences (*overtredingen*) cannot qualify as predicate offences. Tax evasion is a felony and can be a predicate offence for money laundering (Sections 69 and 72 of the General State Tax Act (*Algemene wet inzake rijksbelastingen*)).

If the suspect fails to provide an explanation as to the legitimate origin of the objects, and the facts and circumstances brought forward by the PPS justify the suspicion that there is no other possibility than that the objects were derived from a felony, the court can accept that as proof for the criminal origin of the objects. In addition, the court has to prove the suspect performed one or more actions listed above and that the suspect acted either intentionally or culpably.

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

The PPS has extraterritorial jurisdiction for money laundering if a Dutch national (i.e., a Dutch legal entity, a Dutch natural person, a foreign national who became a Dutch national after the offence or a foreign national with a permanent residence or domicile of at least five years in the Netherlands) commits any of the money laundering offences mentioned under question 1.2 in another country, as long as the offence is also punishable in that country (Section 7 DCC). In addition, the Dutch authorities may assert jurisdiction over offences largely committed abroad by using an extensive interpretation of various *locus delicti* doctrines, to place (part of) the acts constituting the offence within the territory of the Netherlands.

The PPS has jurisdiction to prosecute money laundering of objects deriving from both foreign and domestic crimes, even if the statute of limitations for the predicate offence itself has since passed. The Dutch Supreme Court has not yet clarified whether laundering the proceeds of foreign crimes is punishable if the predicate offence is not punishable by law in the foreign state.

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The National Police (NP) and, in more complex cases, the Fiscal Information and Investigation Service (FIOD) are responsible for investigating money laundering criminal offences. The PPS is responsible for prosecution. The PPS has a special branch for complicated fraud cases (*Functioneel Parket*), which often includes money laundering charges.

1.5 Is there corporate criminal liability or only liability for natural persons?

Criminal offences can be committed by natural persons and legal entities (Section 51 DCC). To consider a legal entity as an offender, the offence must be reasonably attributable to the legal entity. That attribution depends on the concrete circumstances of the case, which includes the nature of the prohibited conduct. An important issue in attribution is whether the conduct took place within the “realm” of the legal entity. The circumstances that can be taken into account for this are, among others: whether the criminal offence has been committed by an employee; whether the conduct is in the ordinary course of business or duties of the legal entity; whether

the conduct was beneficial to the legal entity; and/or if the legal entity accepted the criminal offence being committed.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

- Section 420*bis* DCC: six years' imprisonment; and/or community service for a maximum of 240 hours; and/or a fine of the fifth category (up to €110,000).
- Section 420*bis*.1 DCC: six months' imprisonment; and/or community service for a maximum of 240 hours; and/or a fine of the fourth category (up to €27,500).
- Section 420*ter* DCC: eight years' imprisonment; and/or community service for a maximum of 240 hours; and/or a fine of the fifth category (up to €11,000).
- Section 420*quater* DCC: two years' imprisonment; and/or community service for a maximum of 240 hours; and/or a fine of the fifth category (up to €110,000).
- Section 420*quater*.1 DCC: three months' imprisonment; and/or community service for a maximum of 240 hours; and/or a fine of the fourth category (up to €27,500).

If a perpetrator is convicted of several offences at the same time, the aforementioned maximum prison sentences may be raised by a third. Community service and fines can accumulate without such a limitation. Only natural persons can receive a prison sentence or community service. If a legal entity is convicted and the maximum possible fine is deemed insufficient for a suitable punishment, a fine in the next highest category may be imposed (Section 23 DCC). For Sections 420*bis*, 420*ter* and 420*quater* DCC, this increases the potential maximum to €1,100,000 or, if this maximum is deemed insufficient for a suitable punishment, a maximum of 10% of the annual turnover (of the year prior to the verdict).

Finally, under Section 420*quinquies* DCC, natural persons may be removed from the profession during the period in which the money laundering was committed, and certain other civil rights may be denied, such as running for public office.

1.7 What is the statute of limitations for money laundering crimes?

Under Section 70 DCC, the statute of limitations for the aforementioned offences are as follows:

- Section 420*bis* DCC: 12 years.
- Section 420*bis*.1 DCC: six years.
- Section 420*ter* DCC: 20 years.
- Section 420*quater* DCC: six years.
- Section 420*quater*.1 DCC: six years.

The statute of limitations begins the day after the offence was committed. Because possession of an object is often an ongoing event, the limitation period for money laundering of objects still in possession may not start until they are relinquished.

Under Section 72 DCC, any "act of prosecution" (meaning any involvement of a judge in the case at the behest of the prosecutor, such as performing a search of a home, confiscating property with leave of a judge or summoning a suspect to appear in court) interrupts the statute of limitations and commences it anew. However, for felonies, the period of limitation can last no longer than twice the initial statute of limitations.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Enforcement is only at a national level. Please note that the

European Public Prosecutor's Office also has enforcement authority where it concerns money laundering that harms the financial interests of the EU, as defined by Regulation (EU) 2017/1939 and Directive (EU) 2017/1371.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

The NP and the PPS have the authority to attach property for a number of reasons. Objects may be seized in order to ascertain the truth in an ongoing criminal investigation, prove the existence of illegal proceeds from a felony (Section 94 DCC), or ensure that any fines, forfeiture orders or civil damages can be paid (Section 94a DCC). As mentioned under question 1.2, objects entail both goods and all property rights. Furthermore, objects may be seized if they are (in short) illegal or related to a criminal offence (Sections 33a and 36c DCC in conjunction with Section 94 DCC) and may be forfeited. During the investigation and subsequent legal proceedings, the object is typically held by a government custodian until a final judgment.

Currently, no confiscation is possible without a criminal conviction, but a law implementing the EU Confiscation Directive (Directive (EU) 2024/1260) is currently being discussed in parliament. Both the Directive and the Dutch implementation law provide for non-conviction-based confiscation. The Directive instructs Member States to have their national law comply with the Directive ultimately by 23 November 2026.

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

In recent years, several banks entered into out-of-court settlement agreements with the PPS in money laundering cases for substantial amounts. Notable examples are ING Bank N.V. (2018) and ABN AMRO Bank N.V. (2021).

ING Bank accepted a settlement and paid €775,000,000 on charges of culpable money laundering and failure to comply with the Anti-Money Laundering and Counter-Terrorist Financing Act (AML CTF Act, *Wet ter voorkoming van witwassen en financieren van terrorisme*), which we will discuss further in question 2.1. While the PPS dismissed the case against the CEO at that moment, aggrieved parties successfully appealed that decision, resulting in an order by the Hague Court of Appeal in December 2020 to prosecute the CEO. After further investigation into the matter, in which insufficient evidence of personal wrongdoing was found, the PPS requested the Court of Appeal to allow it to decline further prosecution, which the court allowed in December 2025.

ABN AMRO Bank also accepted a settlement and paid €480,000,000 on charges of culpable money laundering and failure to comply with the AML CTF Act. The PPS publicly announced at the time that four (former) executives of ABN AMRO Bank had been formally designated as suspects and that it would continue with its investigation into them. In December 2024, the PPS stated that this investigation had not resulted in evidence of criminal liability of the executives, and declined further prosecution.

In April 2025, the PPS announced that it was planning to take Coöperatieve Rabobank U.A., another Dutch system bank, to

trial on similar charges of failure to comply with the AML CTF Act in the years 2016 through 2021, and possibly also culpable money laundering.

Theoretically, a bank could lose its licence as a result of a conviction, but that is an unlikely outcome if it concerns a system bank.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

The PPS can dismiss a case – either conditionally or unconditionally – if the suspect, for example, has already implemented compliance measures. The PPS can also impose a punishment order (*strafbeschikking*), which can be appealed in court by the suspect. In major cases, however, the punishment order is the result of negotiations between the defence and the PPS and will not be appealed. Finally, the PPS can offer an out-of-court settlement (*transactie*). The records of the facts and terms of a conditionally dismissed case, punishment order or settlement are in general not accessible to the public. However, in high-profile cases or cases that generated publicity, the PPS may issue a press release in which the punishment order or settlement and the settlement conditions are announced, together with an explanation of why there will be no public trial. For the so-called “high-value out-of-court settlements” (in short, those with a fine component exceeding €200,000 or a total value of more than €1,000,000), the PPS, in principle, issues an extensive press release and publishes a detailed statement of facts together with the settlement agreement. Since September 2020, an independent review committee must review proposed high-value settlements and advise on the admissibility of the settlement.

1.12 Describe anti-money laundering enforcement priorities or areas of particular focus for enforcement.

According to the Dutch Strategic Program for Criminal Flows of Funds for 2024–2028, there is currently a particular focus on facilitators of money laundering (both the intentional and unintentional kind) and on the charting of criminal flows of funds and subsequent confiscation.

2 Anti-Money Laundering Regulatory/Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

The most significant Dutch law enacted to counter money laundering is the aforementioned AML CTF Act (see question 1.10), which imposes several obligations on banks, financial institutions and other entities specified in the Act, for example:

- risk management: establish the relevant risks with regard to money laundering and take measures in order to control these risks;
- conducting customer due diligence;

- reporting any unusual transaction after the unusual nature of the transaction becomes known. Please note that contrary to other countries, the AML CTF Act relates to unusual transactions instead of suspicious transactions (see question 3.7);
- adequately training staff about the obligations under the AML CTF Act; and
- keeping records of the risk assessment/customer due diligence for at least five years after the transaction was performed, the business relation ended and/or the unusual transaction was reported.

As stated above, the AML CTF Act obligations apply to banks and a wide range of financial institutions and other entities, for example:

- financial institutions such as investment firms, life insurers and mediators in life insurance, payment service agents/providers, electronic money institutions and currency exchange offices; and
- natural persons and legal entities acting in the context of their professional activities, such as accountants, lawyers, tax advisers, domicile providers, real estate brokers, traders (of, for example, vehicles, art objects, antiques, precious stones and metals and jewellery), brokers in expensive art objects, notaries, pawnshops, cryptocurrency service providers, casinos, appraisers and trust offices.

For lawyers and notaries, the AML CTF Act is only applicable for certain work, such as (in short) providing advice or assistance in the purchase of registered goods or the management of assets, and acting in name and on behalf of a client in a financial or real estate transaction. Note that the AML CTF Act does not apply insofar that the work consists of providing advice regarding legal proceedings or the legal position of the client.

Notable administrative authorities that give guidance on and supervise compliance with the AML CTF Act are:

- The Dutch Central Bank (DNB, *De Nederlandsche Bank N.V.*), which supervises banks, investments institutions and exchange offices.
- The Netherlands Authority for the Financial Markets (AFM, *Autoriteit Financiële Markten*), which regulates organisations that provide financial products, including stock exchanges.
- The Financial Supervision Office (BFT, *Bureau Financieel Toezicht*), a supervisory body that oversees the compliance with laws and regulations by bailiffs and notaries and the compliance with the AML CTF Act by various professional groups.
- The Local Dean (*Deken*) of the Netherlands Bar (NOvA, *Nederlandse Orde van Advocaten*), which supervises lawyers.
- The Financial and Economic Integrity Service (DFEI, *Dienst Financieel-Economische Integriteit*) which supervises, *inter alia*, buyers and sellers of certain goods, real estate agents and real estate appraisers.
- The Netherlands Gambling Authority (KSA, *Kansspelautoriteit*), which provides permits and supervises gambling companies.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

The main AML requirements are laid down in the AML CTF Act, with professional organisations supervising and imposing further specific regulations on their members and/or offering guidelines to aid the professionals to comply with the AML CTF Act, for example: the Royal Dutch Association of Civil-law Notaries (KNB, *Koninklijke Notariële Beroepsorganisatie*); the

mentioned NOVA; and the Royal Netherlands Institute of Chartered Accountants (NBA, *Koninklijke Nederlandse Beroepsorganisatie van Accountants*), for notaries, lawyers and accountants, respectively.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes, see question 2.1.

2.4 Are there requirements only at national level?

Yes, with the national requirements being largely considered as the implementation of the EU Anti-Money Laundering Directives.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? Are the criteria for examination publicly available?

We refer to questions 2.1 and 2.2. On recommendation of the International Money Fund (IMF), the Dutch Ministries of Finance, Justice and Security issued General Guidelines to the AML CTF Act (*Algemene leidraad Wet ter voorkoming van witwassen en financieren van terrorisme*) in order to support the private sector in carrying out their AML obligations.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes. The FIU is the central authority to which unusual transactions must be reported in accordance with the AML CTF Act. The FIU analyses the reported unusual transactions; if these transactions are considered suspicious, they are put at the disposal of various law enforcement and investigative services.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

Enforcement of the AML CTF Act can take place through the criminal justice system or the administrative justice system. Administrative fines can be imposed until five years after the violation (Section 5:45 of the General Administrative Law Act (GALA, *Algemene wet bestuursrecht*)). Failure to comply with certain Sections in the AML CTF Act is also a criminal offence under the Economic Offences Act (EOA, *Wet economische delicten*). The statute of limitation for criminal offences with regard to violating the AML CTF Act varies from three to 12 years (Sections 6 EOA and 70 DCC).

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

In administrative proceedings, failure to comply with the AML CTF Act may result in a fine in the range of €10,000 to (in case of repeated offences) €10,000,000 (Section 31 AML CTF Act).

Furthermore, financial institutions such as banks may be fined up to 20% of their annual turnover.

In criminal proceedings, failure to comply with the AML CTF Act may result in imprisonment of up to four years, community service of 240 hours and/or a fine of up to €1,100,000 or 10% of the annual turnover (Sections 1 and 6 EOA and 23 DCC).

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

There are several other types of penalties that may be imposed under the DCC, the EOA, the AML CTF Act and the GALA, such as total or partial closure of the company for a maximum of one year, publication of the court ruling, forfeiture of objects, the removal from office and cessation of the legal entity. Furthermore, administrative regulators may impose a penalty payment order subject to penalty (*dwangsom*), give an administrative order (*last onder bestuursdwang*) and publish the fines imposed.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

See question 2.8. The penalties can be administrative and criminal. Do note that if an institution failed to comply with the AML CTF Act and that resulted in damages to an aggrieved party, that party can file a civil claim for damages.

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

If an administrative agency wants to impose an administrative fine, it usually draws up a penalty report. If the administrative agency shares the penalty report with the offender, the offender can submit his view. Not all resolutions of penalty actions are public; resolutions are only public if the administrative agency decides to publish the fine.

If the administrative agency fines the offender, it can file an objection with the administrative agency involved, after which a review takes place. If the administrative agency upholds its decision, an appeal can be lodged at the District Court. Verdicts by the District Court can often be challenged in appeal at an Administrative Appeal Court.

Financial institutions have, in the past, successfully challenged penalty assessments in judicial and administrative proceedings.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and non-financial businesses and professions are subject to anti-money laundering requirements? Describe any differences in the anti-money laundering requirements that each of them are subject to.

See question 2.1.

3.2 Describe the types of payments or money transmission activities that are subject to anti-money laundering requirements, including any exceptions.

As mentioned under question 2.1, the AML CTF Act applies to institutions as a result of the activities performed by that institution. For the purposes of the AML CTF Act, under Section 1 AML CTF Act, a transaction is defined as any (combination of) act(s) performed by or on behalf of the client that has come to the attention of the institution on account of its services rendered to the client. See also question 3.7. For lawyers and notaries, the AML CTF Act is only applicable for certain work and does not apply insofar that the work consists of providing advice regarding legal proceedings or the legal position of the client.

3.3 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry? Describe the types of cryptocurrency-related businesses and activities that are subject to those requirements.

Until recently, only providers of custodial crypto-asset wallet services and crypto-asset to fiat exchange services fell under the remit of the AML CTF Act. With the Dutch implementation of the EU Markets in Crypto Asset Regulation (MiCAR, Regulation (EU) 2023/1114) and the Anti-Money Laundering Directive (Directive (EU) 2015/849), nearly all types of crypto-asset service providers now qualify as an institution in the sense of the AML CTF Act, and must adhere to the AML/CTF obligations contained therein. Currently, the providers of the following crypto-asset services fall under the AML CTF Act:

- providing custody and administration of crypto-assets on behalf of clients;
- operation of a trading platform for crypto-assets;
- exchange of crypto-assets for funds;
- exchange of crypto-assets for other crypto-assets;
- execution of orders for crypto-assets on behalf of clients;
- placing of crypto-assets;
- reception and transmission of orders for crypto-assets on behalf of clients;
- providing advice on crypto-assets;
- providing portfolio management on crypto-assets; and
- providing transfer services for crypto-assets on behalf of clients.

3.4 To what extent do anti-money laundering requirements apply to non-fungible tokens (“NFTs”)?

As NFTs are (when they are not factually interchangeable), in principle, not regulated by the MiCAR, and as the AML CTF Act derives its definition of a crypto-asset service provider from the MiCAR, NFT service providers are arguably not directly covered as crypto-asset service providers by the Dutch AML requirements. There is, however, not yet any case law available on this issue. In addition, the AML CTF Act may still be applicable to those who trade in NFTs, especially if the NFT in question is a work of art. Natural persons and legal entities that professionally act as a buyer or seller of art objects for an amount exceeding €10,000 are subject to the obligations under the AML CTF Act as described in question 2.1, as are natural persons and legal entities that professionally mediate in the buying and selling of art objects (Section 1a AML CTF Act).

3.5 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

As mentioned in question 2.1, an institution has to establish risks with regard to money laundering, take the necessary measures to mitigate risks, perform customer due diligence and train employees. Under Section 2d AML CTF Act, institutions with two or more policy makers must also appoint a day-to-day AML CTF Act policy maker who is responsible for compliance with the AML CTF Act.

3.6 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

See question 2.1 for the requirements with regard to recordkeeping and question 3.7 for reporting currency transactions.

3.7 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

The AML CTF Act requires financial institutions to report unusual transactions to the FIU (Section 16 AML CTF Act). Transactions may be considered unusual if objective and/or subjective indicators are present. The indicators are listed per type of institution in the Implementing Decree for the AML CTF Act (*Uitvoeringsbesluit Wwft 2018*). An objective indicator can be, for example, a cash exchange of €10,000 or more, a credit card or prepaid card transaction of more than €15,000 or more, or a money transfer of €2,000 or more. A subjective indicator can be anything that gives occasion to assume that a transaction is related to money laundering or terrorist activity.

3.8 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

The scope of the AML CTF Act is not limited to national transactions. Cross-border transactions – transactions to and from the Netherlands – fall within the scope of the AML CTF Act and must be reported by the institution to the FIU if they are unusual. The report to the FIU must contain the information stated in Section 16 under 2 AML CTF Act, such as the identity of the client and the ultimate beneficiary owner (UBO), the time and place of the transaction and why the transaction is deemed unusual by the institution.

3.9 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

The AML CTF Act provides for three procedures of customer identification and due diligence: simplified; standard; and enhanced.

For low-risk clients or transactions, the simplified level, involving basic due diligence based on the matter at hand, is sufficient.

The standard procedure involves identification and verification of the client and its representative, identification and (if reasonable) verification of the UBO, establishment of the purpose and nature of the transaction and, if needed, research into the source of the funds, verifying whether the client is acting as an intermediary, etc.

For high-risk clients (such as politically prominent persons) or high-risk transactions, the enhanced procedure must be followed, which may include, for example, more research into the origin of the funds involved, etc.

3.10 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Section 5 AML CTF Act prohibits banks and other financial institutions entering into or continuing a correspondent relation with a shell bank, or with a bank or other financial institution that is known to allow a shell bank to use its accounts.

3.11 What is the criteria for reporting suspicious activity?

See question 3.7. Note that the threshold for the obligation to report a transaction is lower than “suspicious”, given that the current Dutch criterion for reporting is whether the transaction is “unusual” (Section 16 AML CTF Act). The FIU will determine if a reported transaction is actually suspicious.

It is important for institutions to record the (subjective) reasons for reporting a transaction. If an unusual transaction is reported in good faith and in line with the duties under the AML CTF Act, the notifying institution is exempt from criminal or civil liability for damages caused to the client as a result of the notification (Sections 19 and 20 AML CTF Act).

The notifying institution and its employees must maintain confidentiality regarding notifications (Section 23 AML CTF Act), which means tipping off the client is not allowed.

3.12 What mechanisms exist or are under discussion to facilitate information sharing 1) between and among financial institutions and businesses subject to anti-money laundering controls, and/or 2) between government authorities and financial institutions and businesses subject to anti-money laundering controls (public-private information exchange) to assist with identifying and reporting suspicious activity?

Since 2025, the sharing of information between public and private parties to combat organised crime, fraud and money laundering is regulated by the Data Processing by Partnerships Act (*Wet gegevensverwerking door samenwerkingsverbanden*). This Act and its related Decree prescribe under which circumstances information can be exchanged between private and public parties to combat, *inter alia*, money laundering.

The Data Processing by Partnerships Act and its related Decree contain various legal provisions to protect privacy and personal data rights. For example, partnerships must establish advisory committees, independent privacy audits are mandatory, and there must be a point of contact where citizens can exercise their GDPR rights. Participating parties are designated as joint controllers within the meaning of the GDPR, with the associated obligations.

The European Anti-Money Laundering Package (EU AML Package), which will enter into force in 2027, will lead to alterations in the Data Processing by Partnerships Act. As the EU AML Package arguably narrows the room for voluntary sharing of information between financial institutions subject to AML controls, certain private initiatives, such as the initiative by certain Dutch banks to jointly monitor transactions (Transaction Monitoring Netherlands), are being wound down and/or reorganised to fit the coming legal framework.

3.13 Is adequate, current, and accurate information about the beneficial ownership and control of legal entities maintained and available to government authorities? Who is responsible for maintaining the information? Is the information available to assist financial institutions with their anti-money laundering customer due diligence responsibilities as well as to government authorities?

In accordance with the Fourth Anti-Money Laundering Directive, the Netherlands has a UBO register in which organisations are obligated to register its UBOs with the Dutch Chamber of Commerce (*Kamer van Koophandel*). This obligation is implemented in the Trade Register Act 2007. General public access to the UBO register is no longer unavailable due to a ruling of the Court of Justice of the European Union (ECLI:EU:C:2022:912). Government authorities such as the PPS and the FIOD are able to consult the UBO register. Private organisations that are obliged to perform due diligence under the AML CTF Act or the Sanctions Act can currently consult the most important information about the relevant UBO (being the UBO’s date of birth, nationality, state of residence, the nature of the economic interest held by the UBO and the extent of this interest). A delegated regulation is currently being prepared regarding the access to the UBO register of other third parties with a legitimate interest to access UBO information, such as journalists.

3.14 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions? Describe any other payment transparency requirements for funds transfers, including any differences depending on role and domestic versus cross-border transactions.

Under Section 4 of the EU Transfer of Funds Regulation (Regulation (EU) 2023/1113), which has direct effect in the Netherlands, the payment service provider of the payer must ensure that transfers are accompanied by identifying data regarding the payer and payee, specifically:

- the payer’s and payee’s name and account number;
- the payer’s address, official personal document number and customer ID number or date and place of birth; and
- the payer and payee’s legal entity identifier (LEI) or equivalent (if applicable)

Before transferring funds, the payment service provider of the payer must verify the accuracy of this information unless the (aggregated) transfer of funds does not exceed €1,000 and the funds were not made available in cash (or anonymous electronic money), and no other reasonable grounds for suspecting money laundering exist.

If, with regard to a transfer, all payment service providers in the payment chain are within the EU, the payment service provider can suffice with adding the bank account number of the payer and the payee. (Further information must be made available only upon request.) Similarly, (aggregated) transfers

of funds destined outside the EU that do not exceed a value of €1,000 need only be accompanied by the names and account numbers of the payer and payee.

Under Section 14 of Regulation (EU) 2015/1113, crypto-asset service providers have similar obligations regarding crypto-asset transfers, where every transfer must be accompanied by:

- the names of the initiator and beneficiary of the transaction;
- the distributed ledger address of the initiator and beneficiary and/or their cryptocurrency account numbers;
- the initiator's address, including their country and official ID number or client identification number, or their date and place of birth; and
- if possible and applicable: the LEI.

It is noteworthy that the previously mentioned threshold of €1,000 applies only to fiat money transfers by regular (non-crypto) payment service providers. The Transfer of Funds Regulation has not included such a threshold for crypto-asset service providers. A similar exception was initially considered for crypto-asset service providers but was ultimately not incorporated into the regulation. The preamble justifies this difference by stating that, compared to money transfers, crypto-asset transfers can move more rapidly across multiple jurisdictions due to their global reach and technological characteristics, and it is easier to break large crypto-asset transfers into many smaller ones.

3.15 Is ownership of legal entities in the form of bearer shares permitted?

Under Dutch law, bearer shares can only be issued through a global certificate (*verzamelbewijs*), which must be held at the central institute or an intermediary (such as a bank). Any trade can only take place through a brokerage account. By means of the brokerage account or the shareholders register of the company, it can be determined who owns a share. Consequently, it is not possible to transfer bearer shares anonymously.

Physical bearer certificates representing ownership of individual shares were abolished in 2019. Bearer shares that had not been registered by 1 January 2020 were automatically converted to registered shares.

3.16 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Yes, see question 2.1. The non-financial institutions to which AML requirements apply are listed in Section 1a par. 4 AML CTF Act. Since 1 January 2026, the Act contains a specific prohibition for any pawnshops or professional traders in goods or art to provide or accept payment in cash above the current amount of €3,000.

3.17 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

If the AML CTF Act is applicable to an institution (see question 2.1), the geographic area can be a factor in establishing the required level of customer due diligence. Free trade zones are typically regarded as a factor to consider a client or transaction high-risk.

3.18 Are there government initiatives or discussions underway regarding how to modernise the current anti-money laundering regime in the interest of making it more risk-based and effective, including by taking advantage of new technology, and lessening the compliance burden on financial institutions and other businesses subject to anti-money laundering controls?

The Dutch Implementation Act for the Prevention of Money Laundering and Terrorist Financing is currently in preparation. This new act implements Directive (EU) 2024/1640 (the Sixth Anti-Money Laundering Directive) and Regulation (EU) 2024/16242 (the Anti-Money Laundering Regulation), which form part of the new EU AML Package for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. This new Dutch Act is meant to enter into force by 10 July 2027, and will replace the current AML CTF Act. The new Act will remain risk-based. One of the main guiding principles stated by the government in the draft explanatory memorandum to the implementation of the EU AML Package is that the implementation, where room exists, will be performed with minimal unnecessary compliance burdens for both citizens and institutions.

Since a Dutch court ruled in 2021 that Bunq Bank was not out of line by performing certain AML due diligence with the aid of machine learning technology, many Dutch institutions have started using some form of technology to assist their AML compliance obligations. In a 2022 publication, the DNB took a generally positive stance towards the use of Artificial Intelligence (AI) technology in certain AML/CTF compliance matters, but we note that the use of such AI must in principle adhere to the EU AI Regulation (Regulation (EU) 2024/1689).

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

As alluded to above, the Dutch Implementation Act for the Prevention of Money Laundering and Terrorist Financing is currently in preparation, which will, by implementing the EU AML Package, largely overhaul the current system and replace the AML CTF Act. The EU AML Package is meant to introduce the same rules for combating money laundering and terrorist financing throughout the EU. The EU AML Package will, *inter alia*, bring compliance obligations to certain new businesses such as crowdfunding providers, soccer clubs and soccer agents. The threshold for the obligation to report a transaction will be whether a transaction is "suspicious", and no longer when a transaction is simply "unusual". In addition, Regulation (EU) 2024/1620 establishes a new European-wide Anti-Money Laundering Authority (AMLA), which will provide guidelines on what factors to take into account when deciding whether a transaction is suspicious. The EU AML Package should be fully implemented by 10 July 2027.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

See question 4.3.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

The latest mutual evaluation of the Netherlands by the FATF was published in August 2022. The FATF concluded that measures to combat money laundering and terrorist financing were delivering good results, but the Netherlands needed to do more to prevent legal persons from being used for criminal purposes, strengthen risk-based supervision, and ensure that sanctions for money laundering were proportionate and dissuasive. The Netherlands was considered “largely compliant” to “compliant” regarding most FATF recommendations, and “partially compliant” with regard to “Correspondent banking” and “New technologies”. This last issue pertained to only two types of crypto-asset service providers being subject to the AML CTF Act in 2022 (custodian wallet services and services that exchanged between crypto-assets and fiat currency). As the Netherlands has since implemented the MiCAR, which brings most types of crypto-asset service providers under the AML CTF Act, the “partially compliant” verdict regarding “New technologies” has been updated to “largely compliant” in the 2025 FATF follow-up report. The “partially compliant” verdict remains regarding the issue of “Correspondent banking”, as mandatory enhanced due diligence measures regarding correspondent banking relationships apply only to respondent institutions outside the European Economic Area.

4.4 Please provide information on how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

Unfortunately, not all materials are available in English.

All aforementioned Dutch laws and Decrees can be accessed through: <https://wetten.overheid.nl> (Dutch only).

All EU Regulations and Directives can be accessed in English through: https://european-union.europa.eu/index_en

The General Guidelines to the AML CTF Act of the Ministries of Finance, Justice and Security can be accessed through: <https://open.overheid.nl/documenten/5c9a55d8-a924-4fca-8f0b-3637f96b9932/file>

The specific guidance for each reporting group can often be found through the websites of the supervisory authorities. For example, the AML CTF Q&A from the DNB can be downloaded in English from: <https://share.google/7Yg1K2msPPiVcuT2i>

The website of FIU Netherlands provides extensive and detailed information about the applicable law and regulations for each reporting group, including hyperlinks to the relevant websites of the authorities for each of the different types of institution. The website of the FIU is available in English, and can be found at: <https://www.fiu-nederland.nl/en>



Brendan Newitt, LL.M., assists companies, non-governmental organisations and (leading) individuals in white-collar matters. As a lawyer, he has been involved in many large-scale (international) fraud, corruption and bribery cases and advises companies regarding (international) financial-economic criminal law. He is a leading individual in the fields of cybercrime, cryptocurrency, digital rights and (international) digital investigation measures, in which role he advises various large ISPs in the Netherlands and abroad about their rights and obligations in cyberspace. In addition, he assists both suspects and victims of large-scale international cybercrimes. He is a member of the Advisory Committee on Criminal Law of the Netherlands Bar Association.

De Roos & Pen
Sarphatistraat 600
1018AV Amsterdam
Netherlands

Tel: +31 652 361 174
Email: newitt@deroosenpen.nl
LinkedIn: www.linkedin.com/in/brendan-newitt-12349b4b



Lisa van der Wal, LL.M., has extensive experience in providing legal aid in large and complex (international) fraud cases. The fraud cases in which she acts as a defence lawyer relate to money laundering, confiscation of proceeds of crime, forgery of documents, fiscal fraud, corruption and financial fraud. Van der Wal also advises about criminal liability with regard to these topics. She represents companies, directors, shareholders and employees, as well as (employees) of financial institutions and trust offices, accountants and tax advisers. Van der Wal also assists companies and financial institutions who have been victims of fraud, aids them in the filing of a criminal complaint with the public prosecution office and represents their interests during the trials.

De Roos & Pen
Sarphatistraat 600
1018AV Amsterdam
Netherlands

Tel: +31 620 490 433
Email: vanderwal@deroosenpen.nl
LinkedIn: www.linkedin.com/in/lisa-van-der-wal-b118167



Jantien Dekkers, LL.M., is a passionate attorney specialised in criminal law. Her practice is a combination of complex fraud and money laundering cases, including Fiscal Intelligence and Investigation Service (FIOD) investigations, and other challenging criminal law cases. She represents individuals and companies in investigations into, amongst other things, corruption, embezzlement, deceit, money laundering, forgery and tax fraud. She also has a great deal of experience with internal investigations and confiscation of proceeds of crime. Dekkers distinguishes herself by a thorough analysis of the casefile, creative thinking and plain language. She has the discipline to work through elaborate reports and administration (financial or otherwise), in full detail if necessary.

De Roos & Pen
Sarphatistraat 600
1018AV Amsterdam
Netherlands

Tel: +31 647 009 227
Email: dekkers@deroosenpen.nl
LinkedIn: www.linkedin.com/in/jantien-dekkers-a7666882



Thomas Felix works primarily within the financial and economic criminal law practice. He advises companies and individuals on compliance issues. He has a broad experience as a defence lawyer during (internal) investigations and prosecutions. His clients are (amongst others) business leaders, register accountants, notaries and lawyers often involved in sensitive cases. As a defence lawyer, Felix has been involved in many complex fraud cases. Before joining De Roos & Pen in 2012, Felix gained valuable experience in the field of criminal law. He worked for three years as a criminal defence lawyer at Sjöcrona Van Stigt in The Hague and was a clerk for the investigative judge of the Court of First Instance of Curaçao.

De Roos & Pen
Sarphatistraat 600
1018AV Amsterdam
Netherlands

Tel: +31 648 935 153
Email: felix@deroosenpen.nl
LinkedIn: www.linkedin.com/in/thomasfelix

De Roos & Pen is one of the oldest criminal law firms in the Netherlands, and specialises in financial economic and criminal tax law. It is recognised both internationally and within the Netherlands as an authority in its field. With a long-standing fixture in the top tier of *The Legal 500* rankings for fraud and white-collar crime in the Netherlands, the office has a great deal of expertise and experience in handling complex bribery and corruption cases, as well as matters related to cybercrime. Lawyers from De Roos & Pen have assisted a variety of (leading) individuals, companies and NGOs in large (international) bribery and corruption investigations. Additionally, lawyers from De Roos & Pen conduct internal investigations, often on behalf of the financial sector, and offer advice about compliance and corporate governance. As a result of this specialisation, De Roos & Pen frequently serves international (often

American) companies that have interests in the Netherlands or elsewhere in Europe. Thanks to the scale of the firm and the available expertise, the office is always ready to put together a reliable team of lawyers for every acute criminal law problem.

www.deroosenpen.nl/en

**DE ROOS
& PEN**



The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 59 practice areas.

Anti-Money Laundering 2026 features three expert analysis chapters and 16 Q&A jurisdiction chapters covering key issues, including:

- The Crime of Money Laundering and Criminal Enforcement
- Anti-Money Laundering Regulatory/Administrative Requirements and Enforcement
- Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses