Integrity Supervision in Focus 2026

DeNederlandscheBank

EUROSYSTEEM

Contents

Introduction

This is the 2026 edition of our Integrity Supervision in Focus (ISF) report. In this report, we share the insights gained from our integrity supervision of various financial institutions, including banks, payment institutions, insurers, pension funds and trust offices. Our integrity supervision covers both the European Netherlands and the BES islands.

The ISF report is aligned with previous publications and does not present any new policies.[1] Where the Supervision in Focus 2025-2026 report (in Dutch) provides an overview of both prudential and integrity supervision, the ISF report provides information about actual and emerging integrity risks. Next to that, it provides a review of integrity supervision over the past year and looks ahead to relevant developments for 2026. The thematic examinations in this report are based on the sector figures for 2024, which were provided by the sector via the annual integrity risk survey (IRAP) in 2025. The sector figures for 2025 will be available in the second quarter of 2026.

In the 'Cross-sectoral' section, we discuss the following thematic examinations carried out across the wider financial sector: the sanctions screening examination, the follow-up examination on counteracting discrimination by banks and the exploratory survey on the proportionate application of the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wwft*). The next section is our sector-wide outlook for 2026. We also discuss developments in the supervisory landscape, such as the new European Anti-Money Laundering Authority (AMLA) and the use of AI in the financial sector. Next, we take a closer look at the key findings for each sector, paying particular attention to sector-specific risks and challenges.

We also discuss the projects carried out by the Financial Expertise Centre (FEC), in which we collaborate with other partners in the sector.

Finally, the Annex lists an overview of the measures imposed in 2025 on institutions under supervision and those not under supervision. The measures were imposed for non-compliance with the applicable integrity laws and regulations, or on parties operating without a licence issued by DNB.

Figure 1 Number of institutions under supervision by sector in January 2026 compared with January 2025

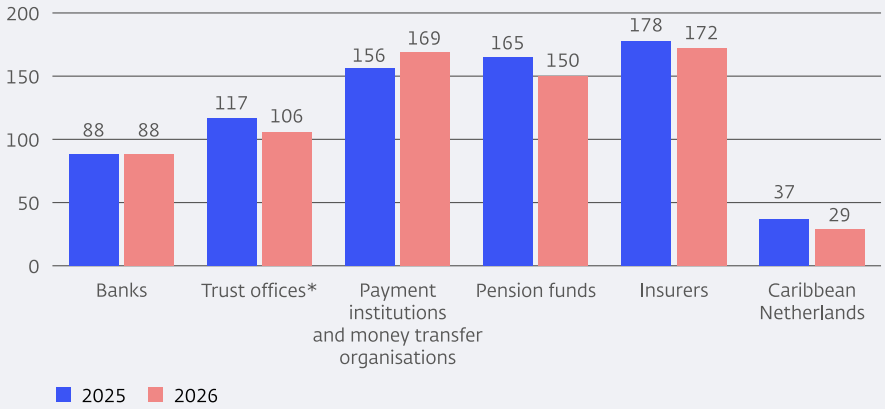


*Figure shows the number of license holders, there are 49 group entities and 68 trust offices in 2025 and 45 group entities and 61 trust offices in 2026.

1 Integrity Supervision in Focus 2024–2025 and Integrity Supervision in Focus 2025.

Cross-sectoral

In this section, we provide feedback on cross-sectoral examinations, focusing on key issues such as counteracting discrimination and the proportionate application of the *Wwft*, and we share information that is relevant to multiple sectors.

The payment chain is becoming increasingly complex and less transparent, making it difficult to effectively monitor transaction flows. Cross-border payments and a variety of payment methods increase the complexity of cash flows. Criminals are taking advantage of this situation, for example by using intermediaries and crypto-assets to conceal criminal flows. This is why all parties involved must remain constantly vigilant, and why we are conducting more cross-sectoral examinations to better identify and tackle suspicious financial flows.

Since the Russian invasion of Ukraine, there has been a significant increase in the number of incoming transactions from countries with an elevated risk of sanctions evasion. Although we have not directly identified any sanctions evasion, there have been notable shifts in transactions at Dutch financial institutions, which may indicate involvement in sanctions evasion. Particularly given the current geopolitical climate, this requires financial institutions to remain vigilant regarding both direct and indirect sanctions risks and changing transaction patterns. A mature sanctions policy requires a thorough assessment of risks and vulnerabilities. Furthermore, an understanding of the underlying motives and structures behind transactions is essential for effective risk management.

Sanctions screening examination

Our thematic examination of sanctions screening systems used test data to assess the effectiveness and efficiency of the systems in place at a number of institutions. In 2022, we found that the systems at a number of banks and payment institutions were not functioning adequately, compelling them to take remedial action. In 2025, we conducted a more comprehensive examination of sanctions screening systems at a total of 59 financial institutions: 21 banks, 10 insurers, 20 trust offices and 8 payment institutions were examined, with each institution receiving individual feedback and recommendations. A total of 15 institutions are implementing remedial measures in response to the findings of the examination. The results show that the effectiveness of the systems at banks and payment institutions has clearly improved since the previous examination. In addition, we have observed that awareness regarding sanctions screening among institutions has improved in recent years. For example, there are more frequent discussions with suppliers of sanctions screening systems to ensure that the configurations and settings of the systems are better suited to the institution's operations. Systems are also being tested more frequently. These are positive developments.

Follow-up examination into banks' approach to combatting discrimination

In September, we published the report Counteracting Discrimination – Actively Addressing the Risk on measures taken by banks and payment service providers to combat discrimination in their compliance with the *Wwft* and the Sanctions Act. Our examination focused on 26 banks and 13 payment service providers, all of whom received individual feedback. In a previous examination, we found that most banks were using a definition of discrimination that was too narrow. This has clearly improved.

The banks have also taken concrete steps in the areas of training and improved communication.

Although the major banks made the most progress – which is a positive and encouraging sign given their significant market share – smaller banks are also showing signs of improvement. For the first time, payment service providers were included in the examination. They have now progressed to a position similar to where the banks were a year ago, demonstrating that they can achieve similar results and further improve their working methods. Identifying and tackling indirect discrimination requires constant attention, commitment and expertise. Indirect discrimination is often less obvious and can arise from policies that appear to be neutral.

Proportionate application of the *Wwft*

We conducted an exploratory survey on the proportionate application of the *Wwft* at a selection of banks. The focus here was on low-risk customers for whom less intensive monitoring should be sufficient. The results of the survey indicate that banks do recognise the importance of applying the *Wwft* in a proportionate manner, but that they are facing challenges in putting this into practice. The survey results were discussed with the banks in September. On December 17th, a news item was published in which the findings were explained in more detail. We observe opportunities to apply the *Wwft* more proportionately through improving knowledge development and increasing the scope for professional judgement, ensuring that measures are better tailored to the actual risk. We encourage supervised institutions to make use of the scope for risk-based judgement when applying standards and risk indicators, and to accept residual risks in a responsible manner. This reduces the burden on customers and minimises inefficiency, while enabling elevated risks to be managed in a more targeted manner.

In consultation with the Ministry of Finance and the Dutch Banking Association (NVB), we are considering possible follow-up measures to support the sector in these efforts.

Good Practices SIRA

In July 2025, we published an updated version of the Good Practices SIRA document, aimed at providing guidance to supervised institutions for preparing and using a SIRA. Although many institutions now have a SIRA, we see in many cases that it is not (or not sufficiently) used as a dynamic control instrument for identifying, analysing and mitigating integrity risks. This is why we have reviewed and updated the Good Practices SIRA document.

Outlook for 2026

Anti-Money Laundering Authority (AMLA)

The Anti-Money Laundering Regulation (AMLR) and the Anti-Money Laundering Directive (AMLD6) will come into effect on the first of July 2027. The Anti-Money Laundering and Anti-Terrorist Financing Implementing Act (*Iwt*) was drawn up to implement the Anti-Money Laundering Directive in the Netherlands. An implementation assessment of this Act was conducted in 2025. The AMLR and the *Iwt* will replace the *Wwft*. In addition, we are preparing for the arrival of the new European Anti-Money Laundering Authority, AMLA. AMLA is set to transform the regulatory landscape in the years ahead. We are making extensive preparations to ensure we can successfully fulfil our role within the new European supervisory framework.

For example, we are actively contributing to the development of the new supervisory framework, which focuses on risk-based and proportionate supervision. We are also contributing with our expertise to the development of technical standards and guidelines. Our contributions relate to the AMLA supervisory methodology, cooperation between supervisory authorities and the obligations imposed on institutions in the areas of customer due diligence and transaction monitoring. AMLA will issue various regulatory technical standards (RTS) and guidelines in 2026 to further implement the new European anti-money laundering rules.[2]

The AMLA methodology will be used to calculate the risk scores of supervised institutions and it has the goal to eventually replace the current methodology, including the existing IRAP questions. A news item was published in December regarding practical implications for the supervised institutions and the IRAP in 2026 and 2027.

In 2026, financial institutions – including banks, insurers and payment service providers – must prepare for stricter requirements regarding customer due diligence, UBO/PEP assessments, sanctions screening and reporting of suspicious transactions. The RTSs and guidelines will provide further details on these matters and will be binding on the entire sector. The new framework will largely come into force in mid-2027. In the run-up to the new framework and AMLA supervision, our own processes and structures will be adapted, including preparations for participation in joint supervisory teams. In addition, we will invest in collaboration and knowledge-sharing with other national supervisory authorities. By taking part in European consultative structures, we strengthen the connection with our peers and work together to build a more harmonised and risk-based AML supervisory practice.

Through these preparations, we are helping to ensure a smooth and effective transition to the new European supervisory framework, with the aim of making the financial system more resilient to financial crime.

Use of AI in the financial sector

AI is transforming the way money laundering risks can be detected. Under the *Wwft* and the new AMLR, AI offers opportunities to identify suspicious patterns more quickly and accurately. This helps institutions to better substantiate their reports and adopt a more risk-based approach, guided by the principle of 'more when needed, less if possible'. At the same time, AI presents a number of challenges: how can transparency, explainability and privacy be safeguarded? And how can direct and indirect discrimination be prevented? European regulations such as the GDPR, the AI Act and the AMLR impose strict requirements regarding responsible use. The AI Act is expected to enter into force in August 2026. All sectors under our supervision

2 Annex XI of AMLA's Single Programming Document 2026-2028 sets out the timelines for the various mandates.

are actively experimenting with AI. Last year, banks were still in the pilot phase, but major banks in particular have made significant progress. The use of AI requires not only a focus on the technological possibilities, but also on effective risk management, appropriate governance, the explainability of models, and the establishment of proportionate forms of human oversight. How organisations design these elements depends on the impact and risks of the specific AI applications they use. We will continue to engage in dialogue with the sector regarding the responsible use of AI.

RegTech

Regtech refers to the digital processes, tools and systems that help financial institutions with compliance and reporting. The use of RegTech offers opportunities such as faster processes, improved data quality and more sophisticated risk assessments, particularly in the areas of customer acceptance, transaction monitoring and reporting. At the same time, operational risks arise, such as outsourcing without adequate control and automation without effective monitoring. We are seeing an increase in outsourcing of onboarding processes[3], which brings additional risks for the gatekeeper function. Examples are identity fraud and the use of straw men. Even when institutions use AI and technological solutions, they remain responsible at all times.

Terrorist financing

The current geopolitical climate is a major factor in the heightened threat of terrorism. At the end of 2025, the National Coordinator for Security and Counterterrorism (NCTV) maintained threat level four, as the terrorist threat remains substantial and the risk of an attack is seen to be real.

In 2024, Europol published its Terrorism Situation and Trend Report. This revealed that the attack on the 7th of October 2023 and the subsequent developments in the Middle East have had a noticeable impact on extremist and terrorist movements in Europe, with the resulting tensions intensifying the mobilisation and activities of these networks.[4]

Terrorist financing will therefore be a key focus area in 2026. The National Risk Assessment of Terrorism Financing 2023 (NRA) shows that vulnerabilities mainly arise in connection with cash and non-cash transactions via licensed banks and money transfer offices, online payment service providers (PSPs), crypto service providers and unauthorised payment service providers and hawala networks. Elevated risks may arise in relation to funds raised via social media platforms or organisations and foundations with a non-transparent structure. The sector should therefore pay particular attention to newly established organisations or social media platforms, the destination of the funds and/or the involvement of high-risk countries. It is, of course, important to take the context into account when making an assessment and to prevent exclusion or discrimination.

In practice, terrorist financing flows are often a mix of legal sources (such as loans and benefits) and illegal sources, with fraud constituting a major revenue stream. This combination makes detection by institutions more difficult.

The NRA emphasises that financing derived from fraud and other forms of crime poses a significant threat. Within Dutch context, healthcare fraud is regularly mentioned by FIU-NL analyses and case studies as a flow of funds which – whether or not through mixing – contributes to the financing of terrorism.[5]

3 In the case of institutions subject to the Financial Supervision Act (*Wet financieel toezicht – Wft*) where the party effecting the transactions is part of the same group, we maintain our policy that this party may carry out the ongoing monitoring. In doing so, we consider both current and anticipated European legislation and regulations, as well as the safeguards applicable to outsourcing under the *Wft*. See Q&A/GP *Wwft*, p. 44.
4 Europol, EU Terrorism Situation and Trend Report (TE-SAT) 2024
5 See Parliamentary Paper 28 828, No. 124, available (in Dutch) at: https://zoek.officielebekendmakingen.nl/kst-28828-124.pdf.

Banks

Over the past year, the banking sector has made further progress in implementing a risk-based approach. Banks are increasingly moving towards more proportionate risk mitigation. They are increasingly applying differentiated approaches: less intensive and less burdensome checks for low-risk customers, and conversely, greater capacity, expertise and resources for customers with higher risks of money laundering or terrorist financing.

Effective implementation requires ongoing investment in expertise, sound risk assessment and a thorough understanding of customers. At the same time, it takes time to fully embed a risk-based approach into day-to-day operations. Banks increasingly use typologies and patterns to identify risks more accurately. In practice, however, the depth of customer due diligence is not always sufficient. This is particularly true in more complex situations, where identifying the relevant integrity risks and determining appropriate controls requires expert judgement from staff with the right expertise and experience. The effective implementation of a risk-based approach requires expertise, thorough risk assessments and a clear link between identified key risks and customer due diligence and monitoring.

Supervisory findings

To determine compliance with the *Wwft* and the Sanctions Act in 2025, we carried out on-site or off-site examinations at 9 banks and thematic examinations at 41 banks, and we conducted risk identification interviews with 14 banks. Several banks are still implementing a remediation programme, and we are assessing their progress. Over the past year, we have paid particular attention to the effectiveness of transaction monitoring systems and the quality of EDR processes.

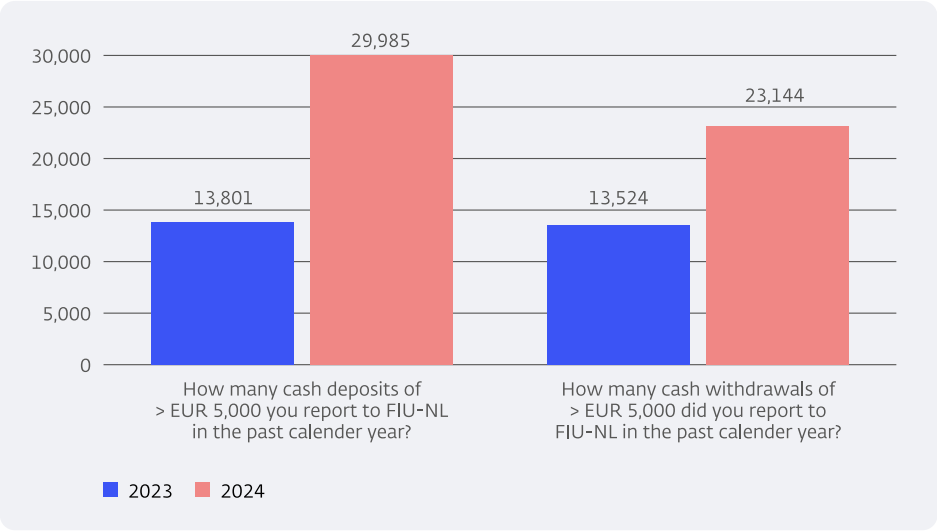
Sector-specific integrity risks

In this section, we discuss the main trends and sector-specific integrity risks relevant to the banking sector that we identified in the annual integrity risk survey (IRAP). In addition to the risks set out in this document, we refer to the Financial Crime Threat Assessment (in Dutch) published by the Dutch Banking Association (NVB) in collaboration with the police, FIOD and FIU-NL.

Cash

Cash is a legal and important means of payment, to which everyone should have unhindered access. At the same time, the use of cash requires vigilance to prevent abuse, such as money laundering and other illegal activities. Dutch banks are also observing this dilemma in practice. In recent years, we have seen an upward trend in the number of notifications to FIU-NL concerning both cash withdrawals and deposits. Inflation is also causing an increasing number of transactions to exceed the reporting threshold. We advise banks to take this into account. The increased number of notifications to FIU-NL is linked to the banks' *Wwft* compliance remediation programmes as well as transactions from previous years that were wrongly not reported. Portfolio analyses are becoming increasingly sophisticated, as are transaction monitoring systems, which provide a clearer picture of high-risk cash usage. Furthermore, as the banks' SIRA show, cash transactions remain a major structural key risk for many banks. With the introduction of a ban on cash payments exceeding €3,000 in 2026, the landscape is set to change for both consumers and banks. The ban is expected to change customers' payment habits, although it is not yet clear exactly how this measure will play out in practice.

Figure 2 Total number of cash withdrawals and deposits that led to a notification to FIU-NL



In addition, a mandatory cash acceptance requirement will be introduced in due course, meaning that certain parties will be obliged to accept cash payments up to the permitted limit. The national implementation of this requirement has been put on hold pending the forthcoming EU legal tender cash regulation. The requirement does not apply to all sectors; landlords, for example, are exempt, which means it is important to be alert to changes in customers' use of cash. Taken together, these developments are prompting banks to review their policies on cash transactions and to assess their potential impact in good time. To ensure the security, transparency and integrity of cash handling processes in this changing environment, the NVB has drawn up a Risk-based Industry Baseline on Cash. It provides banks with a framework for identifying and managing the risks associated with processing, distributing and storing cash.

Sanctions evasion

Since Russia's invasion of Ukraine in 2022, there has been a marked increase in the volume of incoming transactions from countries with a heightened risk of sanctions evasion. The transactions are affected through a wide range of institutions, including major banks, foreign branches and a number of smaller banks. Although we were unable to establish sanctions evasion based on our data on cross-border payment transactions, there have been notable developments in incoming transactions at Dutch institutions that suggest that some of the financial flows involved in sanctions evasion pass through Dutch financial institutions. For institutions, this means that sanctions risks arise not only from direct relationships with sanctioned parties, but also from indirect financial flows and changing transaction patterns. A mature sanctions policy requires an understanding of the organisation's vulnerabilities to evasion, particularly by major players such as Russia. Screening remains important but is on its own not sufficient: understanding the underlying motives and structures behind transactions is essential to effectively mitigating risks.

Discrimination

Preventing discrimination in the implementation of the *Wwft* and the *Sw* is a socially relevant issue that directly affects public trust in banks. Discrimination[6] undermines trust and is prohibited by law. Research findings indicate that, despite banks' efforts to address discrimination, there is still progress to be made. In particular, the risk of indirect discrimination deserves more attention. As part of our regular supervisory practice, we will therefore continue to engage in dialogue with institutions on the unintended side effects of compliance with the *Wwft* and *Sw*.

6 DNB uses the terms direct discrimination, indirect discrimination and perceived discrimination. The definitions of direct and indirect discrimination are used as proposed by the Netherlands Institute for Human Rights (*College voor de Rechten van de Mens*). For perceived discrimination, the definition is used as proposed by Netherlands Institute for Social Research (SCP) in *Ervaren discriminatie in Nederland II, 2020*).

International payment flows

Correspondent banking is important for the international financial system, but managing money laundering risks is a complex matter. In the ISF 2025, we noted a decline in the volume of correspondent banking transactions, which appeared to indicate de-risking. More recent figures show that this decline has halted. Through the IRAP, we will continue to monitor developments in this area. In addition, we will continue to emphasise the importance of adequate risk management in correspondent banking relationships in 2026.

Payment fraud

Payment fraud – such as phishing, bank helpdesk fraud, dating fraud or investment fraud – is a growing social issue.

It is estimated that 1% of the Dutch population falls victim to this every year, resulting in total losses of approximately 375 million euro. The emotional damage is also considerable. In addition to the financial and emotional damage, fraud has wider implications, such as money laundering risks and loss of confidence in the payment system. Fraud is a criminal offence that generates illegally obtained money and can therefore constitute a predicate offence for money laundering. Transactions relating to this offence must therefore be regarded as unusual transactions under the *Wwft* and reported to FIU-NL. According to the FATF and the recent NRA, proceeds from fraudulent activities account for a substantial proportion of the total amount of laundered money. Fraud is one of the integrity risks that banks must take into account under the *Wft* and the *Bpr*.

PSD3 and PSR will impose further obligations relating to the prevention of fraud. In 2026, we will conduct a thematic examination into fraud risk, and fraud risk management.

Tax evasion and tax avoidance

As gatekeepers of the Dutch financial system, trust offices have an important role to play in combating tax evasion and tax avoidance. At present, the vast majority of banks generally take tax considerations into account in their integrity risk profile. We note that some banks take a more sophisticated approach by considering more specific forms of risk, such as Dividend Arbitrage, Transfer Pricing Manipulation, Base Erosion and Profit Shifting, misuse of the Participation Exemption, and Circular Lending. We believe there is still room to elaborate tax compliance risks associated with the customer portfolio in the SIRA in more detail. Another area that warrants more attention is the systematic provision of adequate education and training to ensure that all staff can continue to improve their knowledge of tax risk management.

Transaction monitoring at banks

As part of monitoring remediation programmes, we examined the operation and effectiveness of transaction monitoring systems (TM systems) at several banks. The examination showed that the banks have made efforts to improve and refine the design of these TM systems, as well as their integration into the organisation. However, banks must continue to improve their TM systems by assessing their effectiveness, clarifying processes, and making the necessary adjustments. Finally, we note that banks are now also exploring various forms of AI applications and models to make systems more efficient and to support their analysts in areas such as alert handling. Further development of these initiatives could make the overall TM process more efficient and effective. DNB remains in dialogue with the sector regarding the functioning and effectiveness of TM systems.

AI in the banking sector

In the broadest sense, banks view AI as a potentially powerful technology that enable faster analyses, with increased consistency and a possibility to reproduce them. At the same time, banks still rely heavily on traditional business rules. However, the will to innovate is growing. In practice, we observe the greatest added value at present lies primarily in AI-powered support applications, such as tools that help analysts find and assess relevant documentation more quickly, or better document and organise their findings. These applications improve the efficiency and quality of work, without directly making decisions about customers or transactions. In addition, a small number of banks are exploring AI models that contribute to risk detection, for example in transaction monitoring, customer due diligence or anomaly detection in dataflows.

It is important that banks remain vigilant regarding risks associated with AI. Just like in non-AI systems and in people, a risk of bias with AI is present. Bias can arise from incomplete or non-representative data, or because models inadvertently use correlations that may act as proxies for sensitive personal characteristics. Transparency, explainability and robust model management therefore remain crucial prerequisites for responsible use. We see that banks are drawing on their experience with models from other areas, such as credit risk, to ensure these new models are properly integrated into the existing governance framework. We will continue our dialogue with banks regarding the responsible and transparent use of AI in customer due diligence and transaction monitoring.

Outlook for 2026

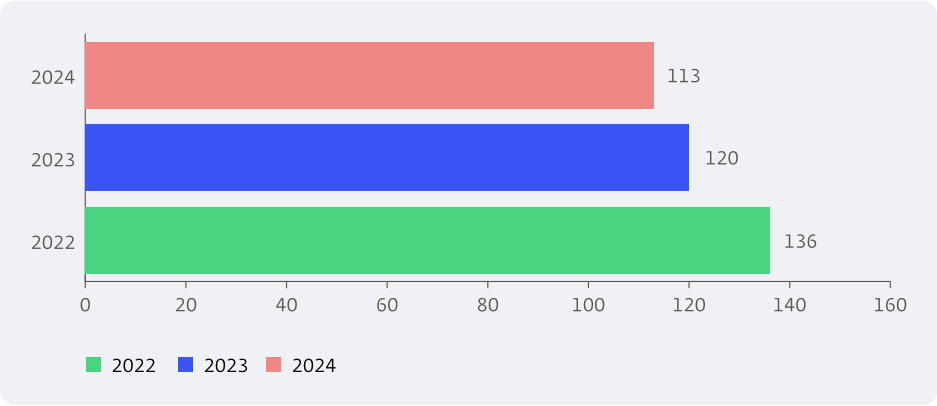
This year, we will be conducting several validation examinations, supplemented by targeted monitoring of ongoing remediation programmes. In addition, we are launching a cross-sectoral examination into remote onboarding and fraud, involving banks and other institutions, with the aim of gaining a clearer picture of sector-wide risks. We are preparing for the changes that the introduction of AMLA will bring, so we can respond promptly to new regulatory requirements and work processes. In addition, we will continue to actively engage in dialogue with the sector – as we have done more intensively this year, including our participation in the NVB's Financial Crime Threat Assessment (FCTA) – and we will continue discussions on a regular basis in the coming year in order to identify developments at an early stage and further strengthen our supervisory role.

Trust offices

The trust sector faces a structurally higher inherent integrity risk, which implies trust offices must have a robust framework of control. We welcome the fact that trust offices are increasingly meeting this demand. In our supervision, we are committed to an open and meaningful dialogue with the sector.

Since 2024, we first discuss supervisory findings with relevant trust offices and explain them in detail before sending them in writing. Both before and during examinations and remediation programmes, we are in increased contact with relevant offices. By engaging in additional dialogue with the trust sector, we aim to improve compliance with the Act on the Supervision of Trust Offices (*Wet toezicht trustkantoren – Wtt 2018*). However, the responsibility for compliance and structural improvement remains with trust offices themselves.

Figure 3 Number of licensed trust offices



Supervisory findings

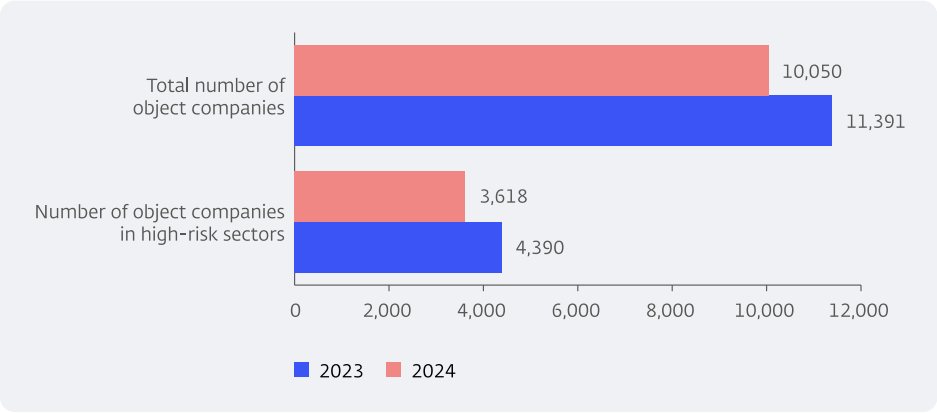
The number of licensed trust offices and the number of object companies they serve is declining. The share of object companies in high-risk sectors has fallen slightly. Although an increasing number of trust offices have their basic procedures in order, our examinations still reveal variations in the thoroughness and quality of customer due diligence and its documentation. These differences relate in particular to the verifiable evidence of the origin of the object company's assets and those of the UBOs, the ability to understand the relevant aspects of the structure, and the identification and management of integrity risks. As a result, some trust offices are unable to manage their risks or cannot manage them effectively. The number of object companies that do not have insights in their bank account fell from 259 in 2022 to 10 in 2024. This reflects a clear improvement in structural access to banking data. Nevertheless, we observe transaction monitoring is not always effective. Among other reasons this is because of limited transaction histories and account information not always being up to date. This creates a risk of unusual transactions not being identified and reported in a timely manner, which undermines sound and ethical operational management.

In 2025, we conducted a further in-depth thematic examination of the compliance and audit function at trust offices. Compared with 2024, it is more often organised in an independent and effective manner, as might be expected under the *Wtt 2018*. At 9 trust offices we examined, the scope of the compliance and/or audit function was still found to be too limited; remedial action has been initiated or implemented in these cases. In two cases, the situation was resolved because we withdrew the licence at the request of the trust offices concerned.

Following reports we received, we also launched a thematic examination into the fragmentation of trust services in 2025.

Fragmentation means the risk that activities requiring a licence may be split up or effectively carried out outside the scope of supervision, which could lead to increased integrity and money laundering risks. We expect to complete this examination in 2026. In addition, we contributed to an FEC project designed to raise awareness of fragmented trust services, with the aim of enabling warning signs to be identified and addressed more effectively in practice.

Figure 4 Total number of object companies, and those operating in high-risk sectors



Sector-specific integrity risks

Foreign bank accounts, foreign offshore structures and less transparent Dutch legal entities

The trust sector remains at risk of being exploited for money laundering purposes, as it is often part of complex international legal and financial structures. This risk is particularly prevalent in relation to cross-border cash flows, foreign bank accounts, offshore structures and less transparent legal structures.

In this context, transparency regarding ownership or the origin of assets and transactions may be limited, which makes it more difficult to identify and manage integrity risks.

Complex structures

The complex and multi-layered structures within the trust sector can increase the risk that money-laundering schemes are not adequately identified, particularly where the reason for using a particular structure is unclear, where there is no structural access to account information, or transaction monitoring is not carried out effectively enough. Although 2024 saw a number of positive developments, such as a decline in the number of high-risk structures, the risk of money laundering remains.

This risk is linked to the international and often complex nature of structures within the trust sector. In some cases, existing relationships between object companies may not be immediately apparent, such as structures involving back-to-back loans. This requires ongoing attention to gain an understanding of the specific money laundering risks associated with each object company and of the extent to which the trust office manages these risks.

Tax evasion and tax avoidance

The risk of tax evasion and avoidance remains a significant concern in the trust sector. Although the use of trust services for tax optimisation has declined, the associated risk has not disappeared. In 2024, more notifications were submitted to FIU-NL on the basis of the subjective indicator of tax evasion or tax avoidance. At the same time, we are seeing a decline in the number of object companies with structures traditionally associated with higher tax risks.

For object companies with a higher tax risk, an independent and objective substantiation of the commercial rationale behind the structure and proposed transactions is required. This must be accompanied by an assessment of whether tax evasion or tax avoidance is involved. If this substantiation is lacking, there is a risk that tax risks will not be adequately identified and managed.

Sanctions screening at trust offices

The thematic sanctions screening examination at 20 trust offices (representing a third of the sector) in 2025 shows that sanctions screening in the trust sector is generally adequate. With a few exceptions, the trust offices examined effectively identify sanctioned entities and transactions, and their performance in this regard is comparable to that of other financial institutions. The downside is that this effectiveness comes with a relatively high number of false positives and more manual work, meaning that sanctions screening requires more resources.

Outlook for 2026

In 2026, we will carry out several validation examinations and monitor the ongoing remediation programmes. In addition, we are conducting a thematic examination on transaction monitoring.

AMLR

The entry into force of the Anti-Money Laundering Regulation (AMLR) also has implications for the trust sector. We expect that trust offices complying with the *Wtt 2018* will only need to make minor adjustments, since in many cases, the AMLR aligns with existing requirements and contributes to further harmonisation with other financial institutions.

Geopolitical developments

Due to the international nature of the trust sector, it is relatively sensitive to geopolitical developments and the associated integrity risks. As a result, trust offices may be more likely to be affected by incidents relating to the circumvention of sanctions or other prohibitions. They are expected to manage these risks on an ongoing basis, particularly in the areas of risk assessment and transaction monitoring. This will be a key focus of our examinations.

DNB Good Practices *Wtt 2018*

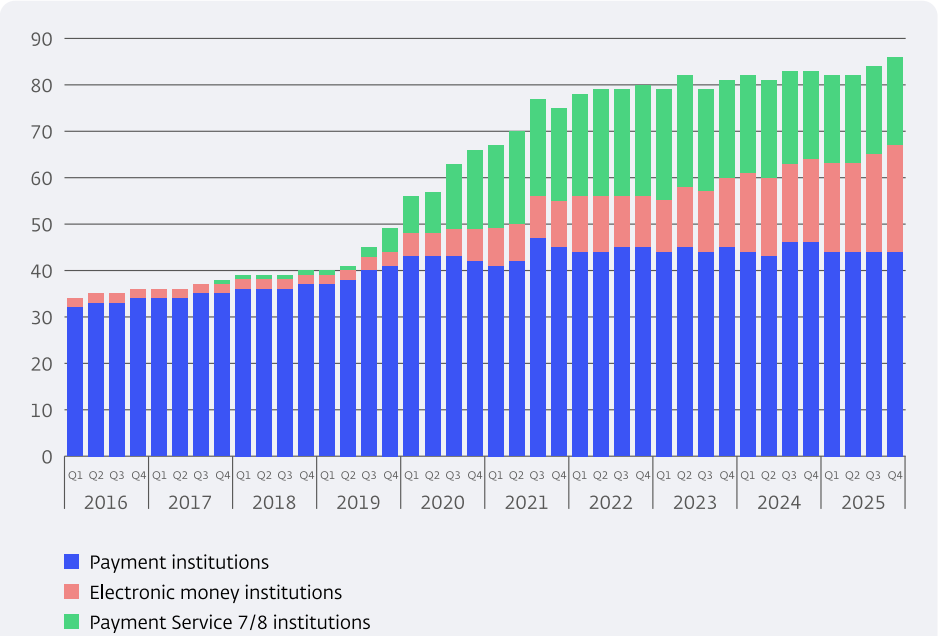
To provide practical guidance on the implementation of the *Wtt 2018*, we published the Good Practices *Wtt 2018* in November 2025. This document provides new guidance and also consolidates several previous policy statements, while preserving room for institutions to apply their individual interpretation of open standards.

Payment institutions and electronic money institutions

The payment sector is in a state of flux. Over the past year, we have seen a marked increase in both the complexity and the volume of payment transactions. New services and combinations of services were introduced, with innovation and digitalisation playing a major role.

For example, the use of virtual IBANs and white labelling has increased significantly. In addition, the use of various RegTech applications is becoming increasingly widespread. These developments offer opportunities for greater efficiency, but at the same time increase the complexity and lack of transparency in the sector.

Figure 5 The number of institutions has grown significantly since 2016



The growing number of institutions and their increasing involvement in transactions (such as vIBAN and white labelling) raise new supervisory concerns and require a more rigorous approach to risk management. We regularly engage in dialogue with the sector to explain legislation and regulations and to draw attention to emerging vulnerabilities.

In November 2025, we organised a seminar for payment institutions and electronic money institutions, focusing on topics such as transaction monitoring and our examination into countering discrimination in relation to compliance with the *Wwft* and the *Sw*. In addition, we hold regular meetings with the sector organisations VBIN and NVGTK.

Supervisory findings

In its Report on ML/TF risks associated with EU Payment Institutions (16 June 2023), the EBA notes that the management of integrity risks in the payment services sector – comprising payment institutions and electronic money institutions – lags behind that of other financial sectors. The EBA notes, among other things, that institutions in these sectors often fail to adequately identify and manage ML/TF risks, that internal controls are frequently inadequate, and that supervisors relatively often identify weaknesses. As a result, this sector is more vulnerable than other sectors. Our supervision confirms these observations. We have identified shortcomings at a significant number of institutions, particularly in the areas of transaction monitoring and the underlying SIRA and CDD processes. Given the nature and scale of these shortcomings, a large share of the sector is running excessive risk. We have imposed remedial measures on the individual institutions where shortcomings have been identified.

In addition to institution-specific examinations, we also conducted sector-wide thematic examinations into compliance with the *Wwft* and the *Sw* in 2025. Based on the insights gained, we find that institutions are making progress in documenting and tracking the outcomes of their customer due diligence processes. Nevertheless, many institutions still need to make further improvements in order to meet the required standards. Below is an explanation of the thematic examinations

Transaction monitoring at payment and electronic money institutions

Over the past two years, our thematic examination on Transaction Monitoring revealed that many payment institutions do not have their core processes in order. Their fundamental controls are inadequate, which means that significant integrity risks may persist. Despite earlier warnings and interventions, this remains a recurring problem in the sector. We have imposed punitive and remedial measures on a number of institutions where our examination revealed that insufficient progress was being made. One shortcoming we frequently encounter is that institutions do not pay sufficient attention to the risk of third parties (such as online shop customers) misusing their payment services.

Agent integrity at money transfer offices

In 2025, we conducted an in-depth thematic examination into agent integrity at money transfer offices (MTOs). We examined whether the sector takes sufficient account of the money laundering risks associated with the use of payment service agents (primarily retailers who offer money transfer services as a secondary activity).

We found that MTOs generally pay sufficient attention to agent integrity. They have generally put appropriate measures in place, including a risk-based internal audit system, policies and procedures focused on agent integrity, and regular review and monitoring of agents' conduct.

Sector-specific integrity risks

In this chapter, we discuss the key trends and sector-specific integrity risks relevant to payment institutions (including MTOs), electronic money institutions and exchange institutions. In both the 2025 Integrity Supervision in Focus publication and the 2024–2025 edition we highlighted the growing lack of transparency in the payment chain. This trend was also evident last year.

Virtual IBANs

A vIBAN is an identification code that looks like an IBAN and directs payments to another payment account (the master account) with a different IBAN. To third parties and payers, a vIBAN looks like a standard IBAN and could be compared to using an alias: while the funds seem to be transferred to this account number, the funds are actually held in a different account. In 2025, the FEC launched a project, coordinated by DNB, to assess the vIBAN phenomenon and the associated risks. As part of this project, discussions are being held with vIBAN service providers and institutions that offer master accounts. In 2026, we intend to issue a report for the sector on useful indicators to detect misuse of vIBANs.

White labelling

Licensed institutions that make their platform available to other financial service providers (e.g. for issuing IBANs to non-residents or holders of crypto wallets) run the risk of having insufficient insight into the ultimate customers and end-users. This risk increases when third parties, without the institution's involvement, carry out customer onboarding and customer management independently. In most cases, these end users are formally considered customers of the licensed institution. This means that despite making its platform available to other financial institutions, the institution remains responsible for all final decisions regarding customer acceptance, risk profiles and the potential termination of customer relationships.

The institution is also required to carry out its own customer reviews. Where necessary, we have requested MTOs to implement remedial measures.

Money laundering through licensed MTOs

The majority of money transfers are cash based and are executed by authorised agents, this makes it important for MTO providers to be alert to agents where unusual transactions occur, to agents that conduct many transactions to high-risk jurisdictions or agents that use multiple MTO providers. In the latter case, larger transactions are split up to remain below the reporting threshold, making detection difficult for institutions (smurfing).

Outlook for 2026

This year, we will be conducting several validation examinations, supplemented by targeted monitoring of ongoing remediation programmes. We are also continuing the FEC project on vIBANs, and in addition to risk identification examinations, we will conduct three thematic examinations on white labelling, remote onboarding and fraud. PSR, PSD3, AMLR, AMLD6 and amended sanctions regulations will bring about significant changes to the supervision of payment institutions and electronic money institutions in the years ahead. We are closely involved in the European and national preparations and are anticipating the implementation of these reforms,

to ensure that our supervision remains timely, proportionate and future proof. We will also continue to actively engage with the sector to discuss how the regulations can be implemented in practice and how we intend to supervise compliance.

Financial Expertise Centre

The Financial Expertise Centre (FEC) is a partnership between authorities with a supervisory, monitoring, prosecution or investigative task in the financial sector and has been established to strengthen the integrity of this sector. DNB is an active partner in the FEC. The FEC also involves a public-private partnership (PPP) with the NVB and the four major banks as permanent partners.

Pension funds

Integrity risks in the pension fund sector remain generally low and well under control. For this reason, we are reducing the intensity of our supervision of institutions in the lowest impact category: 137 pension funds will now have to submit an IRAP once every three years instead of annually. Sanctions evasion and conflicts of interest remain the most significant integrity risks in this sector, with recent supervisory examinations showing that the outsourcing of sanctions screening in particular is subject to systemic vulnerabilities.

Supervisory findings

We have identified shortcomings in sanctions screening in the pension fund sector, particularly where pension funds outsource these activities. Although outsourcing is permitted, pension funds themselves remain ultimately responsible for compliance with the Sanctions Act. Incidents in 2019, 2023 and 2025 show that several pension administration organisations failed to perform sanctions screening against comprehensive and up-to-date sanctions lists for extended periods, meaning that sanctions screening was inadequate at many pension funds. In addition, they often also lacked adequate controls to identify or report shortcomings in a timely manner.

A thematic examination conducted in 2025 among eight pension funds reveals that guidelines for sanctions screening are frequently absent from the pension funds' own policies. The same applies to service agreements with pension administration organisations. Furthermore, pension funds often have a limited understanding of the matching parameters used and rely heavily on reports from service providers. As pension funds do not carry out their own verifications and there is no independent review of sanctions screening – for example through audits or spot checks – there is an increased risk that the sanctions screening is not sufficiently effective and sanctioned persons or entities are not identified in a timely manner.

In light of the incidents identified and the findings of the thematic examination, we have reminded pension funds of their responsibilities. This emphasises the importance of pension funds always remaining responsible for compliance with sanctions regulations, even when they outsource activities. We require the pension funds to ensure their knowledge, management and controls are in order. As part of our regular supervision, we will monitor their timely and thorough follow-up of the identified areas for attention. In case of incidents, we will implement additional supervisory measures.

At the same time, compared with the previous year, there have been improvements in the way pension funds manage sanctions risk. For example, more pension funds now periodically review the risk analyses of their outsourcing partners, incidents are reported more promptly, and some pension funds receive ISAE 3402 Type II reports, which can provide additional assurance regarding the control of outsourced processes.

Sector-specific integrity risks

According to our sector analysis, integrity risks in the pension fund sector remain low and manageable, with the main risks still being sanctions evasion and conflicts of interest. Pension funds outsource many operational tasks, such as pension and asset management, to pension administration organisations and external managers. The main risks are indirect exposures, limited transparency and complex fund structures in the investment chain, combined with rapidly changing sanctions regimes. As a result, there is a risk that sanctioned parties will not be identified as such in good time.

The risks are lower in pension funds' member administrations, but regular screening remains necessary to prevent unintended pension benefit payments. In addition, conflicts of interest are an inherent risk due to pension funds' complex governance structures and the involvement of various parties.

Outlook for 2026

In 2026, we will continue our risk-based approach to supervision. We have revised our impact classification, and as a result institutions in the lowest impact class no longer have to submit the IRAP annually. We will continue to pay particular attention to the outsourcing of sanctions screening and related activities. In the event of repeated or similar instances of non-compliance, we may decide to impose formal enforcement measures in addition to existing supervisory measures.

Insurers

Our recent IRAP data and previous examinations show that insurers generally manage their integrity risks effectively and, where possible, in a risk-based manner. As with pension funds, we have lowered the impact class for insurers due to the limited risks in the sector. As a result, institutions in the lowest impact class (118 insurers) now have to submit an IRAP every three years instead of annually.

Supervisory findings

Integrity monitoring in the sector shows a largely stable picture. In 2025, we conducted a cross-sectoral examination at ten insurers to assess the effectiveness and efficiency of sanctions screening. The examination shows that sanctions screening is often outsourced and that many institutions use external systems and applications, while their understanding of how these systems work and are used is frequently inadequate. Furthermore, the operation of the screening systems is not always systematically tested. At two insurers, we assessed the effectiveness and efficiency of sanctions screening as inadequate. Institutions remain fully responsible for compliance with the Sanctions Act, even when they use external systems. Monitoring the use and operation of screening systems therefore requires ongoing attention.

Sector-specific integrity risks

According to our sector analysis, integrity risks in the insurance sector remain low and well under control. The risk of money laundering and terrorist financing at life insurance companies is generally considered to be low, and compliance with the *Wwft* is, as a rule, adequately organised. Insurers themselves state that external fraud, particularly insurance fraud, poses the greatest integrity risk within the sector.

In addition, internal fraud is becoming an increasingly important area of concern: there has been a distinct rise in the number of reports of internal fraud. Potential conflicts of interest also remain a relevant risk. In practice, the risk of sanctions evasion in both the life and non-life insurance sectors appears to be limited, partly due to the nature of the products and the limited scope for abuse. Insurers' sanction hit notifications usually relate to invested assets or, to a lesser extent, to the misuse of insurance products.

Outlook for 2026

We have revised our impact classification in the context of risk-based supervision, and as a result institutions in the lowest impact class no longer have to submit the IRAP annually. In 2026 we will be conducting a thematic examination into internal fraud at non-life, life and health insurers. This examination addresses the integrity risks previously identified within the sector and aims to provide greater insight into how insurers manage this risk. In addition, we have selected two life insurers for a cross-sectoral thematic examination into remote onboarding, which will be conducted in 2026.

Caribbean Netherlands

Certain institutions based in the Caribbean Netherlands are subject to integrity supervision by DNB. The Caribbean Netherlands is a rapidly developing, cash-intensive society. This makes the area vulnerable to money laundering risks, for example through the real estate sector, the hospitality industry, international financial flows and foreign investment.

With Venezuela as a neighbour and growing US attention, geopolitical risks – and, in that context, compliance with sanctions regulations – are becoming increasingly important. Furthermore, the Caribbean Netherlands is a relatively small community with limited training opportunities in the areas of compliance, integrity and financial crime. Conflicts of interest also pose a risk. There has been a positive trend in the professionalisation of compliance. Supervised institutions are becoming increasingly capable of implementing controls, while we continue our efforts to improve understanding of specific integrity risks.

Following to the National Risk Assessment, the topic of 'money laundering and real estate' received additional attention in 2025. We have sought cooperation on this matter with the other supervisory authorities responsible for supervising compliance with the *Wwft* BES and the partners in the chain. Among other things, this has led to a seminar on this topic in October 2025. Together with other partners possibilities will be explored on how this matter can be taken forward in 2026. We intend to make the SIRA our key theme for 2026.

Other financial institutions

The *Wwft* applies not only to licensed institutions, but also to other financial institutions, such as providers of loans, financial leasing, safe deposit box rental and buy-to-let mortgages. We take a risk-based approach to our supervision of this diverse sector.

With the introduction of new European regulations (AMLR, AMLD6), the requirements for the sector will also change. We are working with the Ministry of Finance to ensure that these requirements are structured in a proportionate manner, so that effective risk management can be achieved without creating unnecessary administrative burdens.

Money laundering risks in the real estate sector and reports we had received regarding this risk have led to the launch of an examination into buy-to-let mortgage lenders in 2025. This examination shows that the sector still has work to do in identifying and mitigating money laundering risks. In 2026, we will continue to focus on this sector and, where possible, seek to collaborate with our supply chain partners within the FEC. In addition, we remain committed to maintaining a constructive dialogue with representatives of this sector.

Reports of illegal activities

The number of reports on illegal market activities increased in 2025. This concerns indications of financial service providers operating in the Dutch market without the required licence or registration.

Following the entry into force of MiCAR, the enforcement of regulations against illegal crypto service providers has largely been transferred to the Dutch Authority for the Financial Markets. As a result, the number of reports we have received concerning illegal crypto service providers has fallen. However, due to an increase in the number of reports of illegal activity in other sectors, the total number of reports has risen.

Figure 6 Number of new reports of unlicensed service provision in 2024 and 2025

Sector	New reports of unlicensed service provision in 2024	New reports of unlicensed service provision in 2025
Trust offices	37	44
Banks	7	31
Payment service providers	16	27
Insurers	2	11
Crypto service providers	30	6
Electronic money institutions	8	4
Exchange institutions	7	0
Total	**107**	**123**

In 2025, the highest number of reports concerned the unlicensed provision of trust services, particularly those relating to 'cut up' trust services. 'Cutting up' means that a service provider outsources domiciliation and additional services – such as keeping accounting records or filing tax returns – to separate providers, with the aim of evading the obligations of the *Wtt 2018*. In 2025, we launched a thematic examination into this form of illegal service provision, which we expect to complete in 2026.
This may lead to enforcement measures. In addition, we are receiving significantly more reports about unlicensed providers of banking services: institutions that accept repayable funds from the public or use the name 'bank' without a licence. The latter refers to individuals or organisations that present themselves online as reliable and legitimate banks. However, they do not hold a licence issued by DNB, and in many cases, they are not registered with the Chamber of Commerce or provide incorrect or incomplete contact details. Their websites contain misleading information, which could put consumers at a disadvantage. That is why we are launching a project in 2026 to investigate and address this phenomenon further. Finally, we have observed an increase in reports of illegal payment services, such as money transfers carried out by individuals or companies that do not hold the required licence. In 2025, we launched a project to investigate unlicensed entities offering money transfer services via apps.

Banks, payment institutions and other financial institutions can report these or other forms of illegal service provision to us using the online form available in the Digital Supervision Portal or by email at handhaving@dnb.nl.

Annex 1 Measures imposed by DNB

Below is an overview of the supervisory measures we imposed on supervised and non-supervised institutions (entities operating without the required licence issued by DNB) for non-compliance with integrity regulations. Between 1 January 2024 and 31 December 2025, we applied both informal and formal measures, ranging from remedial interventions to punitive sanctions.

Measures imposed on supervised institutions	2024	2025
Formal measures	**18**	**7**
Issued an instruction	13	1
Imposed an administrative fine	2	5
Licence withdrawal following enforcement procedures	2	1
Imposed an order subject to penalty	1	-
Informal measures	**15**	**11**
Compliance briefing	3	3
Issuing a written warning	12	8
Final total	**33**	**18**

Measures imposed on NON-supervised institutions	2024	2025
Formal measures	**6**	**5**
Issued an instruction	-	-
Imposed an administrative fine	2	3
Licence withdrawal following enforcement procedures	-	-
Imposed an order subject to penalty	3	1
Reported to Public Prosecutor's Office	1	1
Informal measures	**10**	**6**
Compliance briefing	-	-
Issuing a written warning	10	6
Final total	**16**	**11**

Abbreviations

Abbreviation	
AFM	Dutch Authority for the Financial Markets
AI	Artificial Intelligence
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
AMLA	Anti-Money Laundering Authority
AMLD6	Anti-Money Laundering Directive 6
AMLR	Anti-Money Laundering Regulation
Caribbean Netherlands (BES)	Bonaire, Sint-Eustatius and Saba (BES)
Bpr	Decree on Prudential Rules for Financial Undertakings *(Besluit prudentiële regels)*
CDD	Customer Due Diligence
DNB	De Nederlandsche Bank
EBA	European Banking Authority
EDR	Event Driven Review
EGI	Electronic money institution
FATF	Financial Action Task Force
FCTA	Financial Crime Threat Assessment
FEC	Financial Expertise Centre
FIOD	Fiscal Investigation and Detection Service
FIU-NL	Financial Intelligence Unit
GDPR	General Data Protection Regulation
ISF	Integrity Supervision in Focus
IRAP	Integrity Report *(integriteitsrapportage)*
Iwt	Implementation Act on the Prevention of Anti-Money Laundering and Anti-Terrorist Financing
KYC	Know Your Customer
MiCAR	Markets in Crypto-Assets Regulation

Abbreviation	
ML/TF	Money Laundering / Terrorist Financing
MTO	Money Transfer Organisation
NCTV	National Coordinator for Security and Counterterrorism
NRA	National Risk Assessment
NVB	Dutch Banking Association
NVGTK	Dutch MTO association
PEP	Politically Exposed Person
PPS	Public Prosecution Service
PUO	Pension administration organisation
PSD3	Payment Services Directive 3
PSP	Payment Service Provider
PSR	Payment Services Regulation
RegTech	Regulatory Technology
RTS	Regulatory Technical Standards
SiF	Supervision in Focus
SIRA	Systematic Integrity Risk Analysis
Sw	Sanctions Act (*Sanctiewet 1977*)
TM	Transaction monitoring
UBO	Ultimate Beneficial Owner
UT	Unusual transaction
VBIN	Association of Dutch Payment Institutions
vIBAN	Virtual IBAN
Wft	Financial Supervision Act *(Wet op het financieel toezicht)*
Wwft	Anti-Money Laundering and Anti-Terrorist Financing Act *(Wet ter voorkoming van witwassen en financieren van terrorisme)*
Wtt 2018	Act on the Supervision of Trust Offices 2018 *(Wet toezicht trustkantoren 2018)*

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
The Netherlands
+31 (0) 20 524 91 11
dnb.nl/en

Follow us on:

Instagram
LinkedIn
X

DeNederlandscheBank

EUROSYSTEEM