Integrity Supervision in Focus 2025

DeNederlandscheBank

EUROSYSTEEM

Contents

1 Introduction

1.1 Background and purpose of this report

De Nederlandsche Bank (DNB) conducts integrity supervision of banks, payment service providers, insurers, pension funds and trust offices, both in the European Netherlands and on the BES islands. Our integrity supervision consists of monitoring how these financial institutions comply with integrity laws and regulations.[1] To share our insights from integrity supervision more widely, we are releasing this report.

This report aims to assist institutions in adopting a robust and risk-based approach to sound and ethical business operations by providing insight into current developments, findings from our supervision and emerging risks. It contains no new policy statements and is consistent with our previous publications. Supervision in Focus 2024-2025 highlights three key pillars that contribute to effective supervision. Our Supervisory Strategy 2025-2028 sets out our risk-based approach and elaborates on the focal points of our supervision. Supplementing these publications, this report presents an integrated overview of integrity risks inherent in the various sectors, and of our supervision. The following topics are covered in this publication:

- **Review of 2024**
  Section 2 describes our activities in the past year, as an integrity supervisor, in terms of publications, the ongoing dialogue with the financial sector and the adoption of the European AML package. In addition, it highlights our engagement with the sectors about a more focused approach to *Wwft* compliance and related initiatives in 2024.

- **Sector-specific feedback from our integrity supervision and integrity risks**
  Sections 3 to 9 discuss, for each sector, the findings from our integrity supervision and identify key integrity risks. Here we offer general feedback on the positive developments and vulnerabilities we have identified in supervised institutions' management of integrity risks. This feedback is primarily based on the results of supervisory examinations conducted in 2024. It also outlines the main integrity risks from the sector analysis. In the sector analysis, the risks identified in the National Risk Assessment (NRA), other national and international sources[2], and information from supply chain partners are analysed. We assess supervised institutions' exposure to integrity risks for each sector using the supervisory information that is available to us, including information from our integrity risk survey (IRAP). This analysis offers insights into the main challenges faced by financial institutions when fulfilling their role as gatekeepers of the financial system. We aim to provide supervised institutions support in further developing a targeted and risk-based approach.

1 Our integrity supervision covers the following laws and regulations: the Financial Supervision Act (*Wet op het financieel toezicht – Wft*), the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft*), the Sanctions Act (*Sanctiewet 1977 – Sw*), the Act on the Supervision of Trust Offices (*Wet toezicht trustkantoren – Wtt 2018*), the Pensions Act (*Pensioenwet – Pw*), the Financial Markets (BES) Act (*Wet financiële markten BES – Wfm BES*) and the Anti-Money Laundering and Anti-Terrorist Financing (BES) Act (*Wet ter voorkoming van witwassen en financieren van terrorisme BES – Wwft BES*), as well as delegated regulations.
2 Examples include the Dutch Banking Association's (NVB) "*Financial Crime Threat Assessment of The Netherlands 2023-24*" and various analyses by FIU-NL.

by identifying sectoral trends and risk themes. Many of the risks identified may be relevant to multiple sectors.

- **Measures taken by DNB**
  This section shows how we have used our supervisory tools to support necessary remediation at supervised institutions.

Many of the risks identified may be relevant to multiple sectors. More and more risks are cross-sectoral. For example, the payment chain, which includes all parties involved in payment transactions, is becoming increasingly complex and opaque. This makes it more difficult to maintain a clear overview of transaction flows, especially when transactions span multiple countries, sectors (such as correspondent banks, payment service providers and crypto service providers) or payment methods. Criminals exploit this complexity to hide illicit funds by using intermediaries and third-party structures and converting funds into crypto assets. This requires that all gatekeepers in the chain be always adaptable and vigilant.

2024 was the last year for our integrity supervision of crypto asset service providers. Pursuant to the Markets in Crypto-Assets Regulation (**MiCAR**), this supervision will be transferred to the Dutch Authority for the Financial Markets (AFM). We do not, therefore, discuss crypto service providers in this report. Our supervision of crypto service providers was largely dominated by the transfer to the AFM in the past year. We also conducted two examinations of the crypto sector, one of jointly with the AFM.

2 Retrospective

DNB publications

In 2024, we published several policy statements. In April 2024, the DNB Wwft Q&As and Good Practices was published. This document aims to provide an up-to-date and convenient overview of the obligations under the *Wwft*. It should also assist institutions in designing their risk management in a proportionate manner and provide guidance on how to apply a risk-based approach to customer due diligence and ongoing transaction monitoring.

In addition, in 2024, the DNB SIRA Good Practices and the Good Practices Wtt 2018 (Dutch) were put out for consultation. The new SIRA Good Practices provide supervised institutions with a practical guide for conducting their systematic integrity risk analysis (SIRA). The Good Practices *Wtt* 2018 provides trust offices with an up-to-date overview of their obligations under the *Wtt* 2018, as well as guidance in applying the relevant standards.

Dialogue with the sector

Ongoing dialogue with sectors and representative organisations

We maintain an ongoing dialogue with the institutions we supervise, and we adapt our supervisory activities based on the input and reports we receive. On several occasions in 2024, we discussed with various banks and the Dutch Banking Association (NVB) how transaction monitoring systems could be made more effective. These talks will continue in 2025. We are also involved in several joint bank-led initiatives to enhance the effectiveness of the entire anti-money laundering chain. In addition to institutions and representative organisations, we also consult other stakeholders, for example when preparing the publications cited above. Moreover, we share our knowledge in public-private contexts, including through the Financial Expertise Centre (FEC).

Round-table sessions

Application of the risk-based approach occupies an important place in our dialogue with the sector, especially on the effectiveness of the anti-money laundering chain. In that context, a series of round-table sessions held in 2023 were continued in 2024. An important topic of discussion was discrimination. Studies by DNB and others show that the application of the *Wwft* and the Sanctions Act can result in instances of discrimination: excessive questioning or indeed exclusion of certain customers, without their risk profiles warranting such drastic measures. This issue was discussed in-depth with representatives of banks and payment institutions during the round-table sessions. Representatives of the AFM, the Netherlands Institute for Human Rights (College voor de Rechten van de Mens) and the National Coordinator against Discrimination and Racism also contributed to the sessions. We will continue to emphasise this topic in 2025.

Publication of the European AML package

We are committed to further strengthening the anti-money laundering chain in 2025. A relevant development is the adoption of the new EU AML framework. A comprehensive package of new EU anti-money laundering legislation was adopted in 2024. It contributes to a level playing field across Europe, given that most of its rules are now included in a Regulation, which has direct binding effect, rather than in a Directive. The establishment of a new EU anti-money laundering authority (AMLA) will provide even more impetus. AMLA will gradually grow over the next few years to a workforce of 430 by 2028. From 1 January 2028, it will directly supervise 40 financial institutions, including at least one Dutch institution. In addition, AMLA has various mandates to draft further AML regulations and policies, and to

conduct indirect supervision. Some of these regulations are currently being prepared by the European Banking Authority (EBA), and the first drafts are expected to be put out for consultation in mid-2025. We are playing an active role in AMLA's establishment, while aiming for adoption and strengthening of a risk-based approach.

The introduction of the Anti-Money Laundering Regulation (AMLR) and the imminent arrival of AMLA are expected to require a significant investment in our supervisory capacity.

3 Banks

3.1 Introduction

Over the past year, the banking sector made good progress in improving its integrity risk management. Remediation processes at several institutions were successfully completed or entered their final stages. However, a number of banks still need to take significant steps to reach the required level. For the sector as a whole, it is important to capture the progress made and avoid backsliding: integrity risks such as money laundering and terrorist financing are constantly evolving, which means managing these risks requires continued attention.

Banks should adopt a risk-based approach, while making allowance for their risk appetite. That means they should do less where possible - conducting less intensive controls for low risks - and do more where needed. Resource allocation should focus on where the risks of money laundering or terrorist financing are high. We realise it is not always easy to make such distinctions, often for fear of overlooking specific aspects. But continuing to strive for "a complete as possible picture" uses up scarce time and energy that is better deployed elsewhere.

The sector is taking positive initiatives to further implement the risk-based approach, such as the Industry Baselines published by the Dutch Banking Association (NVB) and the NextGen Gatekeepers initiative. We have published the *Wwft* Q&A and Good Practices and have put out the SIRA Good Practices for consultation.

3.2 The Dutch banking sector in figures

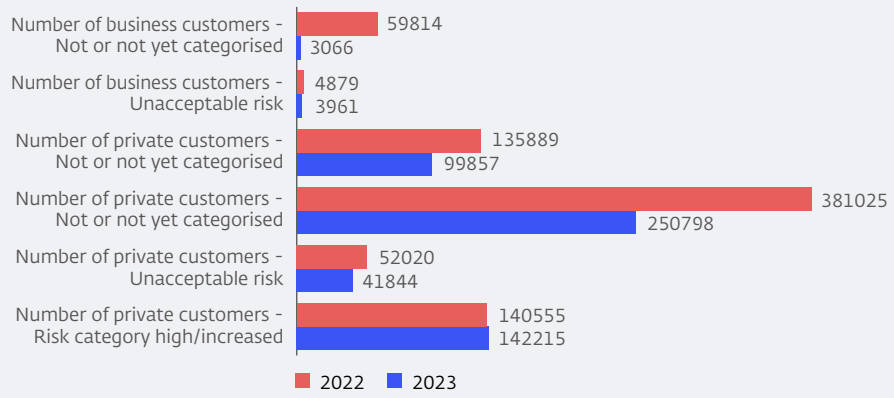
In 2024, 83 banks submitted their 2023 annual integrity risk assessment (IRAP), against 80 in 2023. The sector's reported volume of outbound transactions shows a decline, from €69,213 billion in 2022 to €59,438 billion in 2023. The reported volume of inbound transactions likewise shows a decline, from €65,605 billion in 2022 to €55,309 billion in 2023. The top three countries for cross-border transactions with the Netherlands remained unchanged: the United States, the United Kingdom and Germany. However, both inbound and outbound transactions to and from high-risk jurisdictions increased in 2023 compared to 2022. It should be noted that the value of inbound transactions was 40 times higher than outbound transactions (€906 million and €22 million, respectively).

The figures reflect the progress made by banks. The number of uncategorised customers fell from 440,000 to 254,000. The decline is greatest among corporate customers, which tend to have the higher risks. The number of customers incommensurate with the banks' risk appetite also fell, from 57,000 to 45,000.

The number of unusual transactions reported to FIU-NL increased from 1.1 million to 1.3 million. About half of the reports are based on objective factors. The same applies to the increase, which is largely attributable to new reports made by a limited number of institutions.

Interestingly, reported direct staff costs incurred for first-line anti-money laundering activities showed a slight decrease, from €1.18 billion in 2022 to €1.06 billion in 2023.

Number of customers (high and unacceptable) riskcategory



3.3 Integrity supervision findings for 2024

3.3.1 Money laundering risk management

This section sets out the main findings from the supervisory examinations we conducted at banks in 2024. To determine compliance with the *Wwft* and the Sanctions Act in 2024, we carried out individual deep dives or on-site or off-site examinations at 12 banks, thematic examinations at 11 banks, and we conducted risk identification interviews with 9 banks. In addition, we monitored remediation processes at several other banks. During these activities, we paid particular attention to the integrity risk analysis (referred to below as "risk analysis") and transaction monitoring.

SIRA

From our examinations and risk identification interviews, we found that banks have recently made progress in terms of risk analysis. An increasing number of institutions are using granular and often data-driven portfolio analysis, allowing them to better identify their key top risks. We also find, however, that some institutions are still lagging behind in this regard. Their risk analysis remains superficial or mostly theoretical, providing little practical guidance in managing integrity risks.

Understanding top risks - both during remediation processes and in day-to-day operations - is crucial for effective risk management. By focusing on specific risk themes, institutions can lay a solid foundation for their approach and allocate their resources where the risks are highest. Importantly, transaction monitoring (TM) systems must be closely aligned to the top risks identified in the SIRA. A robust feedback loop in the organisation helps to continuously learn and design AML/CFT activities more efficiently and effectively.

Despite sector-wide progress, some institutions still need to take substantial steps in monitoring and mitigating risks. We find that management information is often strongly process-oriented rather than risk-oriented. As a result, specific risk priorities and targeted actions are not given the attention they deserve. It is important that management information enables board members to effectively manage the risk areas identified in the SIRA, including oversight of foreign entities. To help institutions further improve their risk analysis, we drafted a new SIRA Good Practices document in 2024, replacing the first version from 2015.

Transaction monitoring

Our thematic examinations at 11 institutions have revealed that the majority have transaction monitoring processes and systems in place that are roughly adequate. We did, however, identify several points for improvement. For instance, the necessary link between the identified top risks and transaction monitoring is often lacking, and institutions are unable to explain which business rules or models cover the key risks. This picture also emerges from several individual examinations of TM systems. Next year, we will also focus on whether banks are able to explain how their TM system mitigates the key risks in their portfolio, or what other mitigating measures they have taken. We will also look at how banks periodically test their TM system to boost its effectiveness.

3.3.2 Sanctions Act

In 2024, we did not carry out any examinations specifically focusing on the Sanctions Act at banks, but we did discuss it during risk identification interviews and while monitoring ongoing remediation processes. Banks still make sanctions reports to DNB on a daily basis. We have noted progress with regard to the reports made – banks seem to be more aware of what they must report under the Regulation on Supervision pursuant to the Sanctions Act 1977 (*Regeling toezicht Sanctiewet* 1977), and the quality of their reports continues to increase. However, this area warrants continued attention. Following up on examinations carried out in 2022, we will therefore conduct another examination of the effectiveness and efficiency of banks' sanctions screening systems in 2025.

3.3.3 Discrimination survey

In 2024, we published the survey report entitled "Countering discrimination by banks in compliance with the Wwft (Dutch). The outcome of the survey and of the NVB's self-assessment and the Ministry of Finance's survey on perceived discrimination call for action.

Our key findings show that approaches to discrimination vary widely between banks in terms of specificity and focus. Many banks consider discrimination to be mainly a risk of exclusion, while the concept also encompasses putting customers at a disadvantage and treating them differently. For this reason, we stressed the need for banks to take a more comprehensive view when designing their processes so as to not only prevent exclusion, but also to actively counter discrimination in all forms and shapes. We have asked banks to perform a risk analysis to bring this issue into sharper focus. We organised a round-table session on this topic in late 2024 and will conduct a follow-up examination in 2025.

3.4 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 and that arose as part of our broader insights from integrity supervision.

3.4.1 International payment flows

TBML and SBML
Trade-Based Money Laundering (TBML) and Service-Based Money Laundering (SBML) are methods by which criminals misuse international trade and services to hide and legitimise illicit proceeds. In TBML, trade activities are used to mask the origin of criminal funds, for example by manipulating invoices or over- or understating the value of traded goods. SBML uses services, such as legal or financial advisory services, to launder illicit funds.

A specific TBML technique is the use of third-party payments for goods or services. Third-party payments typically involve one or more non-cash payments covering all or parts of the invoice, often originating abroad and are made either directly or through a Dutch intermediary. If a financial institution cannot find a plausible explanation for the payment, it may decide to classify it as unusual.

In addition, a trend can be discerned in which criminals, partly due to the heightened attention to large cash payments in exports of products and services, are more frequently using non-cash payments through third parties. Non-cash payments are increasingly being used for purchases of export products. This shift from cash to non-cash payments is likely to be a long-term trend requiring adjustments in processes and systems.

High-value products
Illegally obtained money can be integrated into the financial system through the purchase, rental or (operating) lease of high-value products, such as cars, gold, watches, jewellery or art. A shift can be seen from buying to renting or leasing these high-value goods and services. Examples include renting (luxury) cars, concert and wedding venues, as well as purchasing certain services, such as plastic surgery. A key feature is that the rental payments are often made in cash.

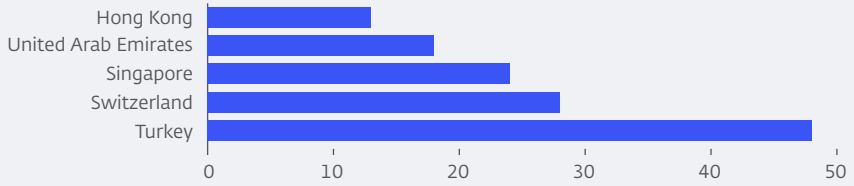
Criminals find this method attractive, as lessors of high-value products are not obliged to report high-value transactions under the *Wwft*. Moreover, the government's proposed limits on cash payments (e.g. a ban from €3,000) apply to goods, but not to services. Having no limit on cash payments for services makes this sector potentially attractive for money laundering.

This shift from buying to renting high-value products calls for additional attention for lessors and other service providers that make disproportionate use of cash payments. Financial institutions should adjust their risk assessments and transaction monitoring to effectively detect and mitigate the risk arising from these trends.

Correspondent banking
Money laundering and terrorist financing through correspondent banking (COBA) remains a major concern, given the inherent complexity and lack of transparency in this type of transaction. Especially when transaction volumes are disproportionate to trade with high-risk jurisdictions (as defined at European level), they require special attention.

In 2024, the European Commission found that financial institutions increasingly opt to de-risk rather than manage risks inherent in COBA. This means banks prefer to terminate relationships with specific customers or in specific regions to avoid risks, rather than managing these risks effectively. Data from 2022 and 2023 support this observation, revealing a decrease in the total volume of COBA transactions.

It is important that institutions strike a balance between managing risks and avoiding unnecessary exclusion of certain customers or regions. Effective risk assessment and management are essential to safeguard the integrity of the financial system and maintain access to financial services.

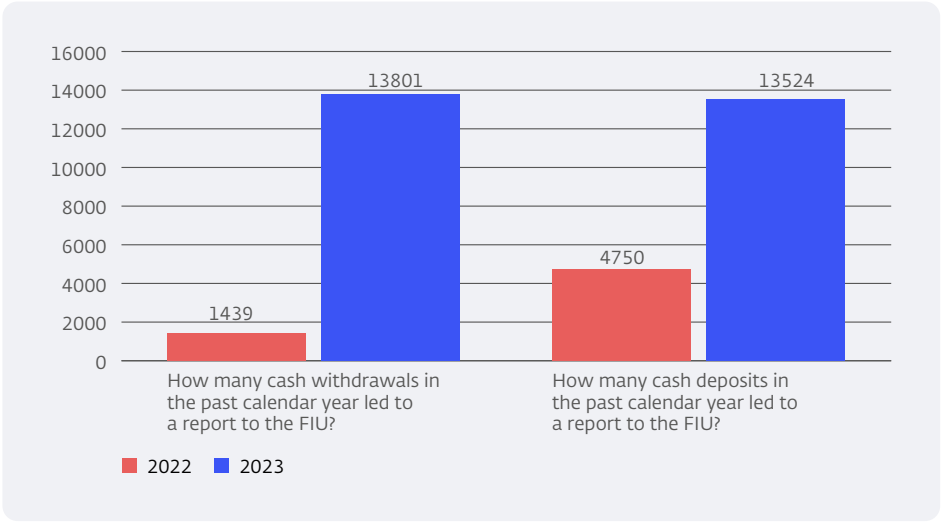


Top 5 high-risk jurisdictions in terms of total volume of inbound and outbound COBA transactions in 2023

3.4.2 Cash

Cash is frequently used as a means of payment, and its legitimate use should not be obstructed. Its use does require banks to be alert to increased risks of misuse for money laundering and other illegal activities. The number of reports of unusual cash transactions by Dutch banks to the Financial Intelligence Unit (FIU-NL) increased strongly in 2023 compared to preceding years.

This increase may be related to the extensive remediation processes under the *Wwft* carried out by several banks in recent years. In addition, improved portfolio analytics and more sophisticated transaction monitoring systems have made customer categories featuring high-risk cash use more visible.



High cash use by retail customers

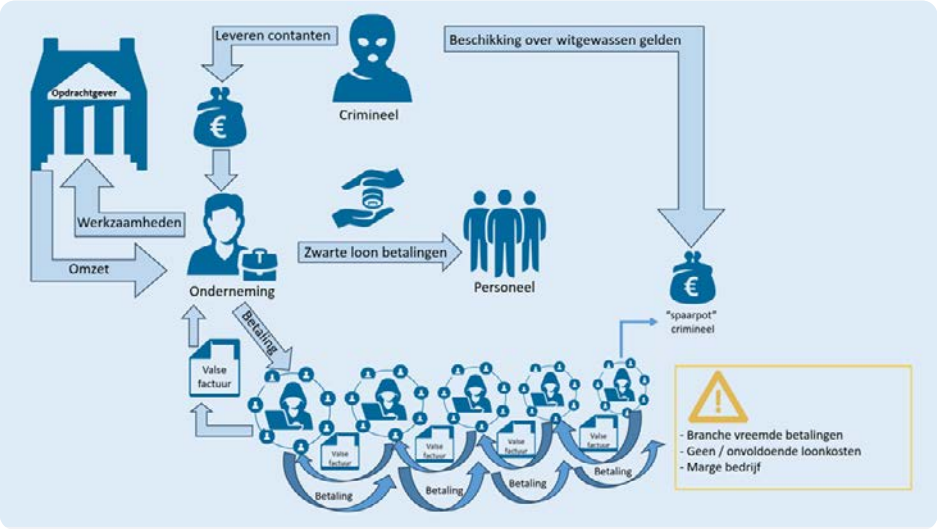
The annual integrity risk survey shows that a significant number of retail customers are characterised by remarkably high cash use. Better understanding of these customer categories and their cash transactions is needed to determine whether unusual activities are involved. Retail customers with annual cash volumes between €20,000 and €50,000 together accounted for a total volume of €3.5 billion. In addition, individual retail customers who carried out cash transactions in excess of €50,000 each together accounted for over €800 million in cash volume.

Cash use by corporate customers

The data show that businesses with annual cash use of more than €250,000 together accounted for €19 billion. The risks of cash use by businesses were recently addressed by FIU-NL in its cash compensation model. This model illustrates how criminals systematically provide cash to firms in labour-intensive sectors, which then compensate for the cash by means of (fake) invoices and non-cash payments. In its 2023 annual report, FIU-NL reports that sectors such as construction, transport, temporary employment agencies, infrastructure and logistics are particularly vulnerable, partly due to the frequent use of subcontractors. We ask banks

to devote attention to this risk and include it in internal analyses and surveys on cash use.

Below is a diagram illustrating the cash compensation model:



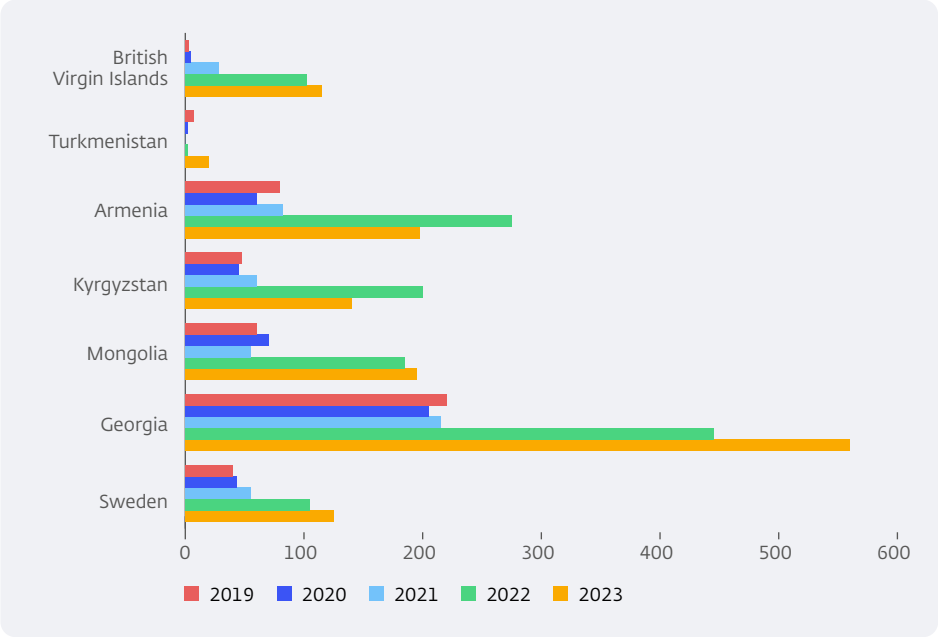
Source: The need for cash in labour-intensive sectors: the Cash Compensation Model | AMLC (Dutch)

3.4.3 Sanctions avoidance

Banks must be able to verify on an ongoing basis whether any party with whom they have a relationship appears on any sanctions lists, and whether services provided or transactions conducted are within the scope of sanctions regulations. We also specifically call attention to the risk of sanctions avoidance, in which prohibited activities or trade with sanctioned parties are continued, circumventing sanctions. The "Financial Crime Threat Assessment of The Netherlands 2023-24" by the Dutch Banking Association (NVB) places sanction avoidance in the top 20 biggest current financial crime threats. The SIRAs of banks under our supervision also identify sanctions avoidance as a top risk.

Inbound transactions from jurisdictions such as the British Virgin Islands, Turkmenistan, Armenia, Kyrgyzstan, Mongolia, Georgia and Sweden increased sharply, especially after the outbreak of the war in Ukraine. This increase, ranging between 100% and more than 600%, may indicate sanctions avoidance. It is therefore crucial that banks know their customers and understand and can explain the reasons behind changes in transaction patterns.

Incoming transaction volumes (in millions)



3.4.4 Terrorist financing

Terrorist financing can be defined as the provision or collection of funds by any means, directly or indirectly, with the intention or knowledge that they will be used, in whole or in part, to carry out terrorist acts, by terrorist organisations or by individual terrorists. This can range from providing money for subsistence and attack preparations, to funding the operating expenses of terrorist organisations. Besides financial support, it also includes providing goods or services, such as fundraising, providing information on financing and making funds available for an attack.

In the "Financial Crime Threat Assessment of The Netherlands 2023-24", the Dutch Banking Association identifies both terrorist financing and extremism as two of the biggest threats. In addition, fraud involving public funds, including healthcare fraud, is mentioned as an issue potentially related to terrorist financing. For banks, detecting terrorist financing remains a challenge as the signals are often subtle and complex. We have therefore compiled the following list of indicators based on insights from our supervision and cooperation with our FEC partners, which can be used in risk analysis of possible terrorist financing. The list is not exhaustive and is intended as guidance for banks in identifying possible terrorist financing. It is essential that banks assess each situation separately and assess risks carefully. An additional challenge here is the importance of an inclusive financial system and the risk of discrimination in applying these indicators. Discrimination is incompatible with an inclusive financial system, and is prohibited by law. This calls for these factors to be handled with great care.

- **Cash transactions:** Frequent cash deposits and withdrawals, especially in sectors where the use of cash is common, such as repatriation, funeral insurance premiums, meat trading, small travel agencies and foreign aid.
- **Situations that also involve subsidised activities:** Involvement in subsidised activities, such as healthcare or language teaching, if there are suspicions of fraud. There are indications that link healthcare fraud to terrorist financing.
- **Family ties:** Owners or directors who are related and carry out unclear transactions among themselves.
- **Transactions with high-risk jurisdictions:** Relationships or transactions with high-risk jurisdictions, whether bordering conflict areas or not.
- **Links to terrorist organisations:** Individuals who have or had a relationship with members of a terrorist organisation, or who are or were in touch with them.
- **Conduct on social media:** Individuals who present themselves on social media by, for example, showing weapons or making statements may suggest sympathy for terrorist organisations and/or endorse their views.
- **Foundations with unclear money flows:** Foundations that transfer funds to accounts of individuals, other foundations or unexplained individuals or organisations.
- **Exchange of denominations:** Directors of foundations exchanging small denominations for €500 or €200 notes, possibly in preparation to reduce their physical volume and export the currency undetected.
- **Charities not registered as Dutch public benefit organisations (ANBI):** Entities that present themselves as charities but are not listed in the ANBI register to avoid supervision.
- **International money transfers:** Foundations acting as international hubs for transferring funds received from other countries.

3.4.5 Illegal financial service provision

The rise of illegal financial services providers continues to be an area of concern, especially given the challenges in detecting them. Banks can play a role in identifying these illegal parties. One possible indicator of such activity that banks could look out for is funds that remain in an account for a short time and are then transferred in full to a subsequent account. This pattern may indicate attempted money laundering, where money is moved quickly to hide its origin.

In addition, referral fees that service providers receive from providers of domicile[3] may be an indication of illegal practices, such as cutting up trust services. In practice, it is common practice for domicile providers to pay part of their own fees as a referral fee to service providers who have referred customers. While this may be a legitimate business practice in itself, it is important for financial institutions to be alert to unusual or excessive referral fees, as these may indicate attempts to mask illegal activities.

3 Domicile provision means making a physical or postal address available professionally or commercially.

Thorough due diligence investigations and continuous monitoring of such transactions are essential to ensure the integrity of the financial system.

3.4.6 Money mules

The use of money mules is a common method used by criminals to mask illicit financial flows. This can take different forms, such as:

- **Straw men:** Individuals who launder money through their business, on the instruction of criminals, by feigning revenues.
- **Money couriers:** Individuals who physically move cash, often abroad.
- **Individuals making their bank accounts or debit cards available:** Increasingly, young people are being asked on social media to make their bank accounts or debit cards available to criminals in exchange for a fee. This allows criminals to remain anonymous and mask their illicit financial flows.

The use of money mules remains a relevant and topical issue. We therefore continue to urge banks be alert to this phenomenon, especially those whose services are at a higher risk. The annual IRAP shows that banks regularly encounter money mules. Fortunately, most are aware of this risk and take appropriate action when detecting a money mule.

In addition, banks, through the Dutch Banking Association, launched the awareness campaign 'Recognise fraud, prevent fraud', explicitly calling attention to the issues surrounding money mules. We endorse the importance of the campaign and encourage this and similar initiatives.

3.4.7 Virtual IBANs

In May 2024, the European Banking Authority (EBA) published a report on the issues surrounding virtual IBANs (vIBANs). The report discusses the various ways in which vIBANs are provided and the associated risks. A key challenge is the fact that financial institutions and investigative authorities cannot distinguish vIBANs from regular IBANs. As a result, an account holder may seem to be domiciled in the country where its master account was opened, whereas this may not be the case.

In addition, the sixth Anti-Money Laundering Directive (AMLD 6), which came into force on 19 June 2024, requires vIBANs to be made available for the Banking Information Reference Portal. It is important that institutions providing vIBANs do so.

3.4.8 Environmental crime

Environmental crime, such as illegal mining, waste scams and overfishing, poses a significant risk due to the damage it inflicts on the environment, the threat to biodiversity and the link to serious crime, such as drug trafficking and human rights violations. As an international trade hub, the Netherlands is at additional risk of involvement in these practices, especially through complex supply chains.

Environmental crime indicators that institutions should look out for are:

- Unusual transactions in high-risk sectors such as mining, fishing and logging.
- Sudden sales growth or changes in payment patterns at businesses in high-risk sectors.
- Payments to countries known for wildlife trade.
- Unusual cash payments, especially in sectors where this is uncommon.

Cooperation with government agencies and civil society organisations is essential if environmental crime and related violations are to be tackled effectively.

3.5 Outlook

In 2025, we will continue to focus on promoting robust risk management at banks, expecting banks to focus on the top risks they have identified and, where necessary, getting the basics right. We expect institutions to continue the improvements initiated in 2024 and further develop their risk-based approach. The emphasis should be on efficient and proportionate resource allocation, deploying less resources if risks are low and exercising closer scrutiny if they are more significant. Some banks still have a long way to go. Finding the balance between doing less where possible and doing

more where necessary is not only desirable but also necessary to manage integrity risks effectively. We remain committed to dialogue with the sector to help banks strike the right balance.

In addition, next to monitoring individual remediation programmes, our supervision programme will specifically focus on refining transaction monitoring systems, enhancing the effectiveness of sanctions screening systems and addressing the risk of discrimination in applying the *Wwft* and the Sanctions Act. To get a fuller overview of the risks inherent in vIBANs, we will launch a project in 2025 in tandem with FEC partners. We will coordinate the project, which is part of the FEC Annual Plan.

4 Trust offices

4.1 Introduction

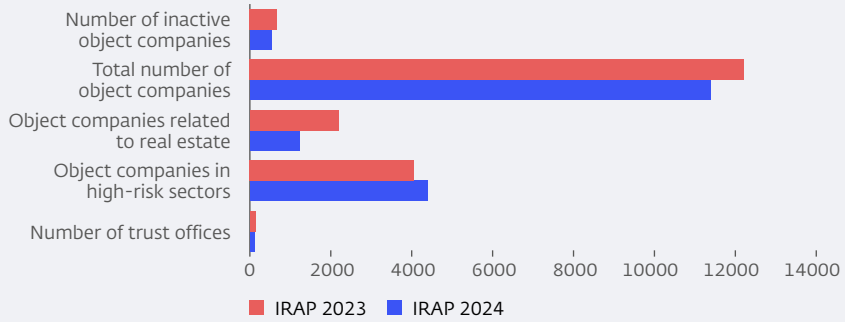
Since the *Wtt 2018* entered into force, we have seen an overall improvement in the way trust offices conduct their customer due diligence. However, some of our examinations - including 8 on-site inspections - and enforcement processes have also revealed that various shortcomings persist at both large and small trust offices. Effective translation of policies and procedures from the board level to the rest of the organisation is a key area of concern. Identifying and effectively managing integrity risks at object companies and customers remains of great importance and warrants continued attention. Similarly, not all trust offices appear to have set up independent and effective compliance and audit functions. We expect trust offices to be committed to complying with their obligations and fulfilling their gatekeeper role.

In addition, we are continuing our dialogue with the trust sector. For example, in March 2024, we hosted a round-table session on the *Wtt*, which was attended by the representatives of the industry associations Holland Quaestor and the Dutch Association of Trust Offices, as well as participants from several trust offices and the Ministry of Finance.

4.2 The trust sector in figures

The number of Dutch trust offices fell from 136 in 2022 to 120 in 2023, reflecting a contraction in the sector. However, the number of object companies in high-risk sectors went up from 4,057 to 4,390. The top 3 high-risk sectors were unchanged: i) commercial real estate, ii) oil, gas and energy, iii) commodities, minerals and mining. The number of object companies related to real estate decreased from 2,197 to 1,224, a 56% decline compared to 2022. The total number of object companies decreased from 12,214 to 11,391, and the number of inactive object companies also fell, from 673 to 538. The number of object companies for which trust offices did not have insight into transactions fell from 259 to 54[4], marking a significant improvement.

In spite of the decrease in the total number of object companies, total trust and other services revenue increased from €288 million in 2022 to €327 million in 2023. The number of reports to FIU-NL also rose, from 89 to 123. However, we observed a significant decrease, from 16 to 5, in reports based on the subjective indicator 'tax avoidance and evasion'.



4.3 Integrity supervision findings

This section sets out the main findings from the supervisory examinations we conducted at trust offices in 2024. To determine compliance with the *Wtt 2018*, the *Wwft* and the Sanctions Act, we carried out an examination covering many trust offices in 2024. We performed deep dives at eight trust offices. Furthermore, there were two thematic examinations: one focusing on incident reports that involved nine offices, and one on the effectiveness and independence of the compliance and audit functions at eight offices. Lastly, in our pilot study 'Fit For Future', we explored the extent to which supervised institutions are future-proof in terms of the governance of their organisation. To this end, we examined three trust offices in more detail. The validation examinations of trust offices for which we had previously found non-compliance revealed that the institutions in question were making gradual progress in the area of sound and ethical business operations, more specifically in drawing up policies and procedures and conducting customer due diligence investigation.

4.3.1 Money laundering risk management

Customer due diligence

Our deep dives concentrated on elements of customer due diligence that trust offices must conduct. In particular, we zoomed in on accurate identification and documentation of an object company's integrity risks, the origin of an object company's assets and the asset position of ultimate beneficial owners (UBOs). Key aspects that recurred in all examinations were to the depth with which customer due diligence was carried out how its results were documented.

In terms of depth, two situations can broadly be distinguished. In one situation, the customer files we reviewed contain the required information, but none or only some of it was considered in the integrity risk analysis.

4 If a trust office has no insight into an object company's transactions, it cannot comply with the obligations under the *Wtt 2018*.

In the other situation, information needed to perform customer due diligence is lacking or insufficient and therefore cannot be considered in customer due diligence. As a result, a trust office runs the risk that certain integrity risks are not or insufficiently considered when conducting customer due diligence. Depth of the customer due diligence conducted and the documentation of its results therefore remain key areas for attention.

4.3.2 Sanctions Act

In 2024, we did not carry out any examinations specifically focusing on the Sanctions Act at trust offices, but we did touch on it during our examinations and while monitoring ongoing remediation processes. Trust offices make few sanctions reports to DNB. Our examinations do reveal, however, an ongoing focus among trust offices on amendments to sanctions regulations and relevant changes to the *Wtt 2018*. In 2025 we will again examine the effectiveness and efficiency of sanctions screening systems at trust offices. The inherent risks of sanctions avoidance in the trust sector remain high, given the number of object companies forming part of structures in high-risk sectors, including the energy sector. Besides high-risk sectors, we also note the share of high-risk jurisdictions in structures served by trust offices, which pose inherent risks of sanctions avoidance.

4.3.3 Results of thematic examinations

Effectiveness and independence of the compliance function

In the past year, we conducted a thematic study on the effectiveness and independence of the compliance and audit functions at eight trust offices. We found shortcomings in the compliance functions of several of the trust offices we examined. They mainly concerned monitoring by compliance, which was insufficiently structural and was lacking depth, inadequate management reporting, the absence of annual work programmes and failure to align the weight prominence of the compliance function with the number of customers, the nature of their activities and the associated integrity risks. We also found that trust offices outsourced their compliance function[5].

Incident reports

In early 2024, we launched a thematic examination into trust offices' incident reports. A key finding is that it is insufficiently clear in the sector what exactly is meant by an incident. In addition, we found that there is a certain fear with regard to reporting incidents to us because of the risk of facing enforcement action. In part, we rely on incident reports to get a comprehensive picture of potential risks and vulnerabilities in the sector. It is therefore important that the trust offices comply with their obligation to report incidents without delay.

It is primarily for the institution to assess which cases involve a serious danger. It may wish to take its cue from its internal escalation procedures. For example, when an incident is reportable to the Management Board or Supervisory Board, it is often also relevant to DNB.

4.4 Sector-specific integrity risks

In this section, we discuss the main trends and sector-specific integrity risks relevant to the trust sector that we identified in the annual integrity risk survey and that arose as part of our broader insights from integrity supervision.

4.4.1 Money laundering through foreign bank accounts

The risk of money laundering through foreign bank accounts is particularly pertinent if a trust office has insufficient insight into object companies' bank accounts. In practice, we often see this risk in, for example, complex structures that involve many legal entities in different potentially high-risk jurisdictions, in which many intra-group transactions take place. In addition,

5 A trust office is not allowed under the *Wtt 2018* to outsource its compliance function.

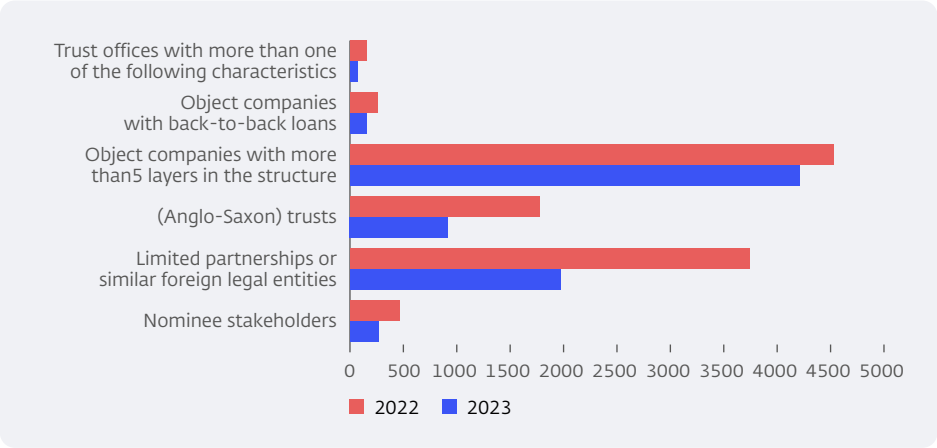
this risk could arise in the case of object companies that have many customers, suppliers or other business relationships in high-risk jurisdictions that do not seem to have a direct link to the object company's sector and/or operations.

One aspect which plays an important role in this regard is the full picture a trust office must have of an object company's business relationships as well as related transactions. Such a full picture must be reflected, among other things, in the transaction profiles to be prepared. These profiles must be up-to-date and specific to ensure adequate ongoing monitoring.

4.4.2 Money laundering through foreign (offshore) structures and less transparent Dutch legal entities

Money laundering through foreign (offshore) structures and less transparent Dutch legal entities is a key risk in the trust sector. The tiered nature of many international group structures plays an important role in this regard. In total, across the Dutch trust sector, 4,205 object companies are served that are part of a structure involving more than five tiers. Such structures may lack the required transparency.

High risk characteristics



Nevertheless, the number of risk-increasing characteristics of corporate structures in the trust sector fell between 2022 and 2023. The number of object companies that have nominee shareholders declined from 461 to 266, while those involving limited partnerships (*commanditaire vennootschap*) or comparable foreign legal entities decreased from 3,744 to 1,969. The number of object company structures involving (Anglo-Saxon) trusts likewise fell, from 1,779 to 918. The number of object company structures involving more than five tiers fell from 4,529 to 4,205. Furthermore, the number of object companies that use back-to-back loans decreased from 262 to 156. All in all, this warrants the tentative conclusion that Dutch licensed trust offices are gradually parting ways with customers that have high-risk structures.

A further key characteristic relevant to the above-mentioned money laundering risk is the presence of a UBO in a less transparent jurisdiction. Jurisdictions such as these are less cooperative in terms of tax transparency and fair taxation. If the UBO is resident in such a jurisdiction, there may be an increased risk of money laundering. In total, there are 61 UBOs in jurisdictions with limited transparency (Andorra, UAE, Monaco, Malta, Mauritius and the Cayman Islands). Particularly prominent are Andorra, UAE and Malta, with 49 residing there.

4.4.3 Trade-based and service-based money laundering

Trade-Based Money Laundering (TBML) and Service-Based Money Laundering (SBML) are methods by which criminals misuse international trade and services to hide and legitimise illicit proceeds.

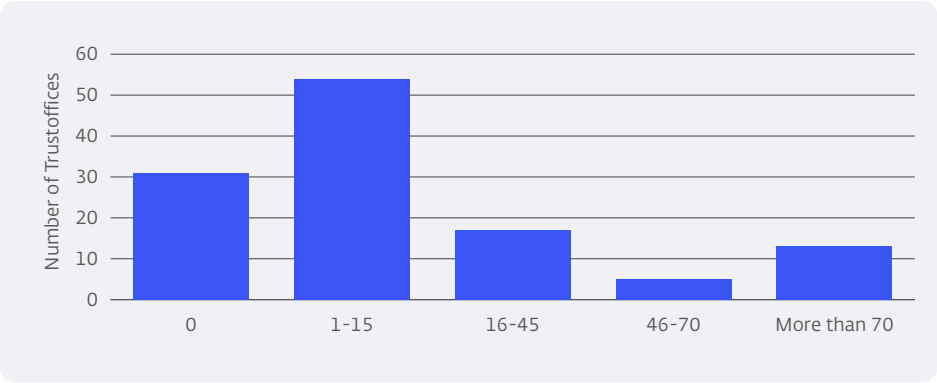
TBML and SBML risk seems to be becoming increasingly relevant for the Dutch trust sector. This is particularly true given that various institutions are increasingly noting a shift from classically tax-driven structures to structures geared to operational activities. Among other things, it is therefore important to gain an understanding and knowledge of object companies engaged in importing and exporting goods and/or services. Also, it requires trust offices to gain more sector-specific knowledge to better assess the integrity risks associated with the services they provide. The number of object companies in high-risk sectors went up from 4,057 to

4,390 in 2023, while the number of object companies in the trust sector as a whole declined by some 10%. This implies that insight into an object company's bank accounts must be a key aspect of customer due diligence and ongoing monitoring. Unlike other financial institutions, trust offices do not provide their own financial products to customers and object companies; they rely on the financial products provided by other financial institutions. This means it is important that they have insight into these products to perform adequate customer due diligence and, more particularly, to prepare transaction and integrity risk profiles and exercise ongoing monitoring.

4.4.4 Money laundering through real estate

Money laundering through real estate is a relevant risk for the trust sector. We have seen a decrease in the number of object companies served by trust offices that operate in real estate from 2,197 in 2022 to 1,224 in 2023 (56% of the number in 2022). The majority of trust offices (89) serve object companies operating in commercial real estate. In addition, 10 trust offices report serving object companies that use back-to-back loans. Combined with complex property structures, such loans can significantly increase the risk of money laundering.

Number of object companies operating in real estate



4.4.5 Money laundering through professional service providers or intermediaries

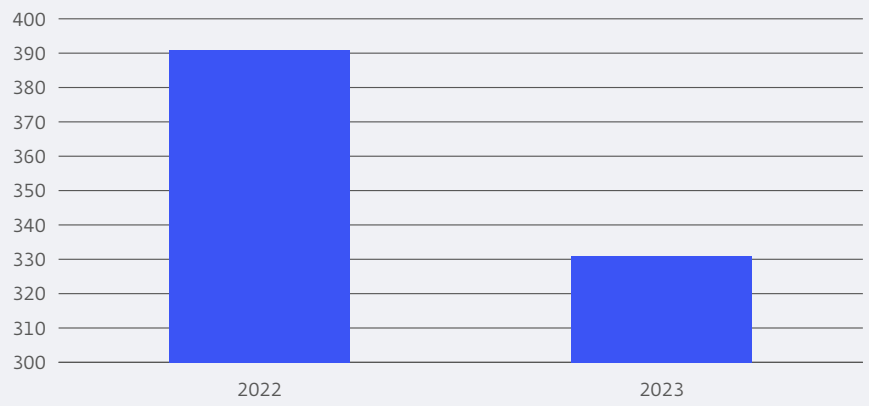
Despite a decrease in the number of object companies having one or more risk-increasing characteristics, the risk of money laundering through professional service providers or intermediaries remains an important one for the trust sector. A trust office may become involved in money laundering if it provides services in situations where high-risk structure aspects are present such as nominee shareholders and limited partnerships.

Overall, 30 trust offices do not serve object companies that could indicate abuse by straw men or money mules, while the majority (90 out of 120) serve between 1 and 25 object companies with these indicators. Only 28 trust offices serve more than 25 object companies with these characteristics, with some outliers such as one trust office that serves more than 440 object companies. As the number of object companies with these indicators increases, a trust office will need to put more effort into complying with its statutory obligations.

4.4.6 Money laundering through corruption and PEPs from high-risk jurisdictions

The risk of money laundering through corruption is closely related to the presence of a politically exposed person (PEP) in a high-risk jurisdiction. A large proportion of trust offices (101) do not serve PEPs in high-risk jurisdictions. 19 trust offices do serve one or more PEPs in high-risk jurisdictions, which total 61. In 2022, there were still 391 UBOs of object companies across the trust sector who were PEPs. In 2023, this number fell to 331.

Decrease in the number of UBOs which are also PEPs



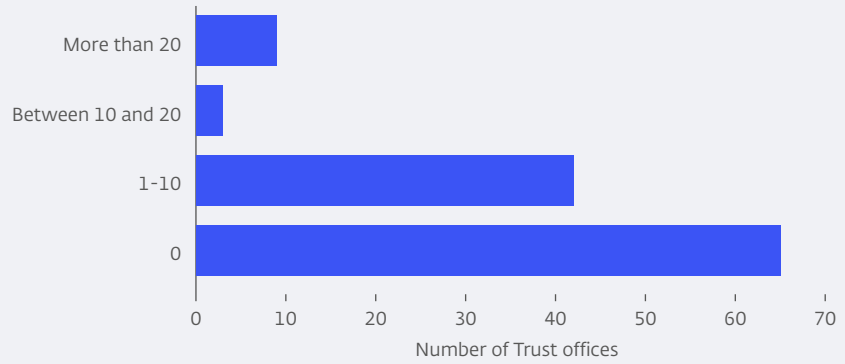
4.4.7 Terrorist financing

The risk of terrorist financing may be related to the results of the sector's screening against sanctions lists. The number of sanctions screening hits in the trust sector totalled 92. Strikingly, they are spread across just 16 trust offices. 104 trust offices did not find any screening hits, and most trust offices do not, or no longer, serve any UBOs in high-risk sanctioned jurisdictions. Most reports related to UBOs and sanctions concern UBOs that are not from high-risk sanctioned jurisdictions.

4.4.8 Tax abuse

Although trust services are less and less sought for tax optimisation purposes, tax avoidance and evasion through object companies remains a relevant risk for the trust sector. Key features, as mentioned above, are the presence of an Anglo-Saxon trust in the structure, a tiered structure and the object's legal form and use of a back-to-back loan. Due to data availability restrictions, it is not possible to identify how many object companies meet all risk-increasing characteristics. However, a total of 69 trust offices serve object companies that meet more than one of them. The 2023 IRAP shows that there were still 152 in 2022.

Number of UBO's in HR country sanctions



4.5 Outlook

We will follow up on our thematic examination of the independence and effectiveness of the compliance and audit functions in 2025. The Fit For Future pilot will also be continued Furthermore, we will include a large number of trust offices in the cross-sector examination into the effectiveness of sanctions screening systems. In 2025, we also expect to conduct several validation examinations at institutions for which we previously identified shortcomings, and also their wider risk assessments. Trust offices are expected to lay a solid groundwork for further integrity risk management by increasing the depth of their customer due diligence. We will also pay specific attention to transaction monitoring and the reporting of unusual transactions in our supervision programme, hosting a round-table session in 2025. As mentioned previously, a key development in the trust sector is the shift from classically tax-driven structures to more operationally focused companies that are part of an international structure. As described above, this may have implications for the way integrity risks can be managed. We will take this development into account in our supervisory activities for 2025.

Following the DNB *Wwft* Q&As and Good Practices, we recently put the policy statements Good Practices Wtt 2018 out for consultation. Also, the consultation version of the SIRA Good Practice was released in November 2024. This new policy statement aims to present good practices to provide trust offices with further guidance on their statutory obligations.

5 Payment institutions (incl. MTOs), electronic money institutions and exchange institutions

5.1 Introduction

Several payment and e-money institutions have made progress over the past year in managing their integrity risks. Following earlier findings, several completed their remediation processes. As such, institutions are taking more significant steps in documenting and tracking the outcomes of their customer due diligence. As a result, institutions are better able to establish risk and transaction profiles, which contribute to enhanced ongoing monitoring of business relationships. At the same time, for much of the sector, there is still much work to be done in terms of managing integrity risks. Many institutions still need to take significant steps to reach the required level. We identified most of the major shortcomings in the area of transaction monitoring. Overall, institutions have not yet adequately designed their transaction monitoring systems, resulting in potential integrity risks being insufficiently managed. In 2025, this will be the subject of renewed focus, and we will monitor how previously examined institutions follow-up on this issue.

We will also continue our dialogue with the sector. We hosted a seminar for payment and electronic money institutions in June 2024, for instance, during which we elucidated the new Q&A and Good Practices on the *Wwft*. We also hold periodic meetings with the sector organisations VBIN and NVGTK.

5.2 The sector in figures

In 2024, 75 payment institutions and 17 e-money institutions submitted their 2023 annual IRAP. In 2023, 73 payment institutions and 11 electronic money institutions reported for 2022. The number of reporting exchange institution remained unchanged at four. Direct staff costs for first-line AML activities went up from €28 million to €42 million, reflecting the steps the sector is taking to bring its risk management up to standard, as noted earlier.

The total transaction volume for merchants in 2023 was €377 billion, edging down from €385 billion in 2022. A sharp decline was seen for debit and credit card transactions, whereas domestic payments outside the Netherlands (e.g. Bancontact and Sofort) grew strongly. The top three countries from and to which transactions are effected remained unchanged: the United Kingdom, the Netherlands and Ireland.

The number of reports made to FIU-NL for these sectors increased from 479,000 in 2022 to 533,000 in 2023. The ratio between objective and subjective reports remained the same at 50-50.

5.3 Integrity supervision findings

5.3.1 Introduction

This section sets out the main findings from the supervisory examinations we conducted at payment institutions and electronic money institutions in 2024. In December 2024, we conducted 23 examinations into compliance with the *Wwft* and the Sanctions Act, 9 of which were on-site inspections. In addition, we completed our involvement in a number of large-scale remediation projects. Based on the insights we gained, we find that institutions are making progress in documenting and tracking the outcomes of their screening processes. As a result, institutions are better able to establish risk and transaction profiles, which contribute to better ongoing monitoring of business relationships. Besides these positive developments, our examinations have also identified areas of concern as explained below.

5.3.2 Money laundering risk management

5.3.2.1 SIRA

Our examinations reveal that the risk analysis often does not sufficiently reveal the risks associated with (outsourcing) partners, agents, sub-merchants and other (end) customers acquired through third parties. In addition, in the case of payment institutions and electronic money institutions, the risk analysis lacks considerations about risks associated with fraud, money laundering through cross-border payments and integrity risks associated with transaction flows to and from high-risk jurisdictions outside the EEA, e.g. in the context of sanctions circumvention. As a result, institutions have insufficient insight in how these risks may arise and how they can be mitigated. As a result, the policies and procedures in place are not geared towards the management of these risks.

5.3.2.2 Customer due diligence

In many of our examinations, we found that the risk profile assessment lacked sufficient depth or that its development is incompletely documented. Customer files often lack substantiation on how the institution arrived at the customer's risk profile, and many do not specify what factors were considered in the assessment. We also found that ongoing transaction monitoring often is insufficiently commensurate with the level of maturity we would expect from institutions. We will elaborate on this in the next section.

5.3.3 Results of thematic examinations

Transaction monitoring conducted by payment and electronic money institutions

In last year's thematic examination on transaction monitoring we found that institutions had not adequately designed their transaction monitoring, potentially insufficiently managing their integrity risks. In the policies and procedures examined we specifically found the following:

- Institutions could not always clearly explain why a particular set of business rules had been selected and whether they adequately mitigate the risks.
- Institutions could not clearly explain why certain thresholds were selected and how they adequately mitigate risks.
- There were insufficient concrete policies and procedures that adequately ensure transaction monitoring, including adequate alert handling.
- Quality assurance was insufficiently organised to ensure that the effectiveness of transaction monitoring processes and systems is tested on an ongoing basis and, if necessary, improved.
- There was insufficient governance, with all duties and responsibilities for the proper execution of continuous monitoring being allocated to a sufficiently committed Management Board member, compliance expert and audit expert.

We often see that the shortcomings listed above are rooted in the fact that no link is made between the risks identified in the SIRA and how transaction monitoring is designed. Our supervision will again devote attention to compliance with the standards related to ongoing monitoring next year.

MTO agent integrity

In 2024, we held a thematic risk identification examination into agent integrity in the Dutch money transfer organisation (MTO) sector. We look at whether the sector, by design, adequately addresses the money laundering risks involved in conducting business transactions and using payment service agents. It shows that MTOs conducting business transactions fail to devote sufficient attention to the specific risks associated with business transactions during risk analysis and alert handling. A further finding is that if MTOs exclude business transactions as a matter of policy, they fail to devote sufficient attention during risk analysis to preventing them from being carried out inadvertently. We have brought this to the institutions' attention.

With regard to oversight on payment service agents, we found MTOs to devote insufficient attention to the risk of mixing funds originating from agents' other business activities with the flows of (cash) funds for money transfers. In 2025, we will examine the effectiveness of agent integrity oversight at a number of MTOs in closer detail.

Exchange institutions

With regard to exchange institutions, the past year also saw examination into, among other things, how exchange institutions deal with PEPs and sanctions and how they conduct their transaction monitoring. This did not result in any significant findings.

5.4 Sector-specific integrity risks

In this section, we discuss the main trends and sector-specific integrity risks relevant to payment institutions (including MTOs), electronic money institutions and exchange institutions that we identified in the annual integrity risk survey and that arose as part of our broader insights from integrity supervision.

In last year's Integrity Supervision in Focus, we highlighted the cross-sectoral trend of the payment chain becoming increasingly non-transparent. Among PSPs, we see increasing fragmentation of the payment service chain across different payment service providers, as well as increasing segmentation of transactions in the payment chain. We therefore added questions to the IRAP at the beginning of 2024. The IRAP results and examinations we performed in 2024 testify to the provision of ever more varied types of services, such as those targeting sub-merchants and providing (virtual) IBANs. A further observation is that institutions collaborate with various intermediaries or partners to provide combined payment services. They may have a variety of reasons to do so.

- One of the partners may lack the required licence.
- One of the partners may lack the technical infrastructure.
- An institution may seek access to an (alternative) payment method.
- An institution may seek to reduce costs, e.g. by outsourcing CDD.
- An institution may wish to acquire new customers.

Mapping these circumstances, considered together, will help institutions to complement their SIRA. We recommend that they consider this when preparing their risk analysis.

5.4.1 Sanctions

For payment service providers and e-money institutions, increasing non-transparency also heightens the risk of processing transactions for sanctioned parties, as institutions are more distant from the end users of their services (including customers of their partners and in the context of outsourcing customer screening) or rely on a partner's sanctions screening. Following up on examinations carried out in 2022, we will conduct another examination of the effectiveness and efficiency of sanctions screening systems in 2025.

5.4.2 Payment chain non-transparency

As part of our sector analysis, we highlight the following specific risks in terms of payment chain non-transparency:

POS terminals (PIN terminals)

POS terminal payment processing gives rise to money laundering risks because three components of money laundering can be exploited – placement, layering and integration – making this service particularly attractive for abuse by criminals. This risk arises in particular in payment processing for merchants in high-value (luxury) goods and if (foreign) prepaid/debit cards are accepted. We will therefore devote additional attention to this as part of our supervision.

Cash withdrawals through ATMs

We are observing a money laundering risk related to cash withdrawals for payment service providers participating in an ATM network. This risk arises if ATMs are placed at a retailer's premises, allowing the retailer to replenish the machine. Accordingly, it is important for the payment service providers involved to have a clear view of their mutual agreements and responsibilities regarding the controls on the use of these ATMs and to adjust these where necessary.

Virtual IBANS

The European Banking Authority (EBA) issued a report in 2024 on the money laundering and trade finance risks of virtual IBANs, and the Dutch Banking Association and DNB have also previously mentioned vIBANs as part of the risk posed by the current fragmentation of the payments landscape. Among other things, a vIBAN allows account holders – both individuals and businesses – to settle payments using a bank account number with an IBAN code from another country, impeding identification of the payee. This makes vIBANs attractive to criminal end users. We will devote attention to this issue in 2025 in the form of an FEC project[6] to help us gain insight into the main money laundering and trade finance risks emerging from vIBAN issuers in the Netherlands and institutions operating from abroad. The project's exact scope, objective and activities are to be determined in 2025.

White-labelling/L.a.a.S

Licensed institutions that make their platform available to other financial service providers (partners) and their customers/end-users, e.g. for providing IBANs to non-residents, run the risk of lacking the required knowledge of such customers. Especially if the partners are also responsible for accepting these customers and maintaining relationships with them without the institution being involved, while the institution also serves these customers. In cases like these the institution must be involved in decision-making on these customers' acceptance, risk profiles and potential exit. It is obliged to perform its own reviews of these customers.

6 See the FEC Annual Plan 2025.

5.4.3 Money laundering through licensed MTOs

Agent integrity
The inherent risk of MTOs becoming involved in money laundering and terrorist financing is high, given that transactions are often carried out in cash and destination countries often face increased risks due to the lack of financial infrastructure. The majority of remittances go through authorised agents, making it important for MTO providers to be alert to agents at which unusual transactions take place, agents that conduct many transactions to high-risk jurisdictions or that use multiple MTO providers.

5.5 Outlook

In 2025, next to monitoring individual remediation programmes, our supervision programme will again focus on transaction monitoring, enhancing the effectiveness of sanctions screening systems and addressing the risk of discrimination in applying the *Wwft* and the Sanctions Act. In addition, we will focus on the topic of agent integrity at MTOs. To get a fuller overview of the risks inherent in vIBANs, we will launch a project in 2025 in tandem with FEC partners. We will coordinate the project, which is part of the FEC Annual Plan.

6 Insurers

6.1 Introduction

In 2024, we took several initiatives to further strengthen integrity risk management in the insurance sector. Our focus was mainly on compliance with the Sanctions Act and the *Wwft* and managing the risk of conflicts of interest. The examinations we conducted in 2024 show that, overall, many insurers manage integrity risks adequately and that they take a risk-based approach where possible. Particularly in the area of *Wwft* compliance, we see insurers taking a more risk-based approach, deploying fewer resources if risks are low and exercising closer scrutiny if they are more significant. Significant strides have also been made in complying with the Sanctions Act compared to previous years. Nevertheless, the outsourcing of sanctions screening and the use of external screening systems remain vulnerabilities that we will continue to address. Furthermore, in recent years insurers seem to have been increasingly heeding our calls through thematic examinations and news releases for attention to the risk of conflicts of interest.

6.2 The sector in figures

The number of life, health and (in-kind) funeral services insurers and reinsurers submitting the annual IRAP has remained stable over the past two years. Non-life insurers showed a slight decrease, however: from 76 in 2022 to 73 in 2023.

The volume of surrendered insurance policies rose significantly, from €3 billion in 2022 to €5 billion in 2023. The volume of new single-premium policies likewise increased: from €587 million in 2022 to €1 billion in 2023.

The highest revenues were achieved in the high-risk sectors of transport, construction and engineering, and real estate.

In 2023, the number of secondary positions in the sector showed a remarkable increase, doubling from the previous year. The total number of registered secondary positions held by second-tier officers, management board members, and supervisory board and supervisory council members went up from 907 in 2022 to 1,864 in 2023. Among management board members, secondary positions increased from 217 in 2022 to 424 in 2023. Among supervisory board and supervisory council members, the increase was even more pronounced – from 461 in 2022 to 815 in 2023. In particular, growth in secondary positions among supervisory board and supervisory council members at other insurers was a major contributor to this increase.

Lastly, the number of FIU-NL reports by life insurers fell sharply, from 42 in 2022 to 15 in 2023.

6.3 Integrity supervision findings

In 2024, we conducted examinations among insurers focusing on the management of risks related to conflicts of interest and compliance with the Sanctions Act. In addition, an exploratory examination addressed incident reporting. The key findings are set out below.

6.3.1 Results of thematic examinations

Sanctions avoidance
Last year's thematic study on sanctions revealed that many insurers blindly rely on their sanctions screening systems or on those of the parties they have outsourced sanctions screening to. They do not test or monitor the accuracy of these systems and the sanctions lists used by these systems. As result, insurers runs the risk that screening is insufficient. In addition, not all insurers have documented which relationships must be screened. This carries the risk of incomplete screening.

Incident reports
Our exploratory examination reveals that insurers do not always report an incident to us. Insurers experience reluctance in classifying and reporting an event as an incident. This is partly due to the open definition of the term 'incident', which allows room for interpretation. It is primarily up to the institution to assess which cases involve a serious danger. It may wish to take its cue from its internal escalation procedures. For example, when an incident is reportable to the Management Board or Supervisory Board, it is often also relevant to DNB.

Also, it is insufficiently clear to institutions what follow-up action DNB undertakes in response to a report. Institutions perceive a risk that, after they have reported an incident to us, we might take action without given them the opportunity to resolve it first. As a result, institutions are more likely to report the incident at a later stage. However, in part, we rely on incident reports to get a comprehensive picture of potential risks and vulnerabilities in the sector. It is therefore important that insurers comply with their obligation to report incidents without delay.

Perceived conflicts of interest
In 2024, also further to previous examinations into conflicts of interest and past incidents, we examined how the risk of conflicts of interest is managed in the case of directors enjoying broad powers of representation for amounts in excess of €10 million. A survey of 10 insurers and an in-depth

examination among some of them shows that this risk is generally not recognised in the SIRA, and relevant scenarios have not been developed. Moreover, the management of this risk is often inadequately documented in procedures and measures and usually does not receive explicit attention in management board decision-making. Even so, this risk did not materialise at the institutions we examined, as joint decision-making based on predefined principles – especially in the event of important decisions – appeared to be the norm.

6.4 Sector-specific integrity risks

In this section, we discuss the main trends and sector-specific integrity risks relevant to the insurance sector that we identified in the annual integrity risk survey and that arose as part of our broader insights from integrity supervision.

The insurance sector faces a number of specific risks that are not highlighted in the NRA. It is also important to note that only life insurers are covered by the *Wwft*. The biggest risk in the insurance sector relates to actual or perceived conflicts of interest. We found little change in this risk compared to last year's sector analysis, however.

6.4.1 Risk of money laundering through value accumulation products

From a previous examination, we concluded that money laundering at life insurers could mainly occur in the case of policies with value accumulation. This is why, in the latest IRAP for life insurers, we adjusted some of the questions in order to get a better picture of money laundering risk. The IRAP shows that a large proportion of life insurers still have value accumulation products in their portfolios, and some life insurers offer value accumulation products. When a life insurer offers value accumulation products, they run an increased risk of money laundering in payments to and from foreign bank accounts, in receiving premiums through means other than the customer's bank account and in remitting funds to an account other than that of the policyholder.

6.4.2 Investments in high-risk sanctioned jurisdictions

86% of investments by the insurance sector in Q4 2023 came from life insurers. This also puts life insurers at the highest risk of investing in sanctioned individuals and legal entities. In Q4 2023, about €615 million was invested in high-risk sanctioned jurisdictions, representing a slight increase compared to Q1 2023, when the value of investments in high-risk sanctioned jurisdictions was €570 million. Of this amount, investments were mainly in China and Türkiye. Compared to Q1 2023, more was invested in Türkiye and less in China.

6.5 Outlook

In 2025, we will continue to examine compliance with the Sanctions Act, with a particular focus on how insurers conduct their sanctions screening. Regarding compliance with the *Wwft*, we will look specifically at compliance where (parts of) customer due diligence have been outsourced and at how insurers use external software for their CDD activities. There will also be an additional focus on data quality, using the answers given in the annual IRAP as a starting point.

7 Pension funds

7.1 Introduction

In this section, we discuss the main trends and sector-specific integrity risks relevant to pension funds that we identified in the annual integrity risk survey and that arose as part of our broader insights gleaned from integrity supervision.

In 2024, we undertook various initiatives to further improve integrity risk management in the pension sector, with a particular focus on compliance with the Sanctions Act. Apparently, pension funds still face frequent challenges in this regard, especially in the area of outsourcing sanctions screening and monitoring its implementation. We would stress that the ultimate responsibility for proper execution of sanctions screening always rests with the pension fund, even when it has outsourced tasks.

7.2 The sector in figures

As a result of conversions to the new pension system, we decided in 2024 to grant some of the pension funds more time to complete the IRAP. Consequently, it is not possible to compare data between 2022 and 2023, and we have chosen not to present figures for the pension funds.

7.3 Integrity supervision findings

In December 2024, we conducted an examination into compliance with the Sanctions Act. The key findings are summarised below.

Compliance with the Sanctions Act
Following an incident, it was found that an external party to which several pension funds had outsourced sanctions screening did not conduct adequate screening, failing to screen against the National Terrorism Sanctions List. As a result, periodic screening against this list had not taken place for several years. As a result, the pension funds that used the services of this outsourcing partner also failed to screen their members against the National Terrorism Sanctions List. This had been going on since 2008, but it was not detected because pension funds had not monitored screening effectiveness. If a pension fund has outsourced sanctions screening, the outsourcing of tasks (including sanctions screening) does not alter the fact that the responsibility for the proper execution of that task remains with the pension fund at all times.

A thematic examination of pension funds and insurers likewise brought to light that pension funds insufficiently monitoring whether the outsourcing partner actually performs the screening fully and properly. It revealed that pension funds lack the safeguards needed to establish that all members were screened. If effectiveness is verified, this is often limited to requesting statements.

7.4 Sector-specific integrity risks

The pension sector faces a number of specific risks that are not highlighted in the NRA. Moreover, pension institutions are not subject to the provisions of the *Wwft* in this regard. With the conversion to the new pension system making an increased demand on our supervisory capacity, we decided to grant some of the pension funds an exemption for the 2023 IRAP. This means most of the data used in the sector analysis below covers a portion of the pension sector (70 of the 158 pension funds that submitted the IRAP in 2024), and a comparison relative to 2022 is not possible. Based on the completed integrity reports, our examinations and the supervisory incidents in the past year, we see little change in the pension sector regarding integrity risks. However, we have two specific areas of concern, which are verification of sanctions screening in outsourcing relationships (see also the section on integrity supervision findings above) and the management of the risk of conflicts of interest in fiduciary management.

7.4.1 Investments in high-risk sanctioned jurisdictions

The Dutch pension sector invested less in jurisdictions with an increased risk of sanctions avoidance in 2023, €7.2 billion less than in 2022. This decline is mainly due to a reduction in investments in China. In 2023, €7.6 billion less was invested in China than the year before. However, we note that €600 million more was invested in Serbia in 2023 than in 2022, while Serbia is also a high-risk sanctioned jurisdiction.

7.4.2 Verification of sanctions screening in outsourcing relationships

We noticed in the IRAP that over half of the pension funds report they do not periodically verify whether the sanctions lists are up to date. For most pension funds, the outsourcing partner checks this.

7.4.3 Managing the risk of conflicts of interest in fiduciary management

The Dutch pension sector devotes little attention to countering conflicts of interest in fiduciary management. Especially if responsibility for fiduciary management is allocated to the party to which asset management is outsourced, there may be an increased risk of conflicts of interest. We conclude from the IRAP that pension funds using fiduciary management often fail to document secondary positions, gifts and invitations. Furthermore, the remuneration policy of fiduciary managers deserves additional attention.

7.5 Outlook

As in previous years, we plan to conduct examinations into potential vulnerabilities in managing integrity risks in the pension sector in 2025. Particular attention will be devoted to risks such as conflicts of interest, compliance with the Sanctions Act in outsourcing, and how pension funds monitor compliance.

In addition, in 2025, we will devote additional attention to the data quality of responses in the annual IRAP, which is a crucial source of information for identifying and assessing integrity risks.

8 Other financial institutions

8.1 Introduction

In 2024, the European Union adopted a legislative package that will help Member States further counter money laundering and terrorist financing. Within this context, DNB will be obliged to know all institutions it supervises. While we know most of them, because they are licensed or registered to provide their services and offer their products, some we do not yet know. They are banks that fall within the scope of our *Wwft* supervision, but do not provide any of the services listed in Annex I of the Capital Requirements Directive. These 'other financial institutions' include, for example, safe custody service providers, financial lease providers and buy-to-let mortgage lenders. With the Ministry of Finance, we are exploring ways in which we can fully map this section of our supervisory population without causing the institutions concerned to incur excessive compliance costs.

8.2 Outlook

This year, we will conduct our supervision of other financial institutions on a signal basis. In addition, targeted identification research will be conducted on sections of this supervisory population in 2025. If possible, we will again look to cooperate with the chain partners in the Financial Expertise Centre (FEC). In addition, we aim to engage in dialogue with representatives of this supervisory population.

9 Enforcement to end illegal financial service provision

9.1 Introduction

We received more reports of illegal market activities in recent years. Financial service providers are operating in the Dutch market without the required licence or registration. These reports also reflect some trends. We saw an increase in the number of reports regarding trust services being 'cut up'. '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 addition, we are receiving more reports about illegal payment service provision, such as the provision of money transfers by individuals or firms that do not have the required licence or have failed to register with us as exempt payment service providers. If banks, payment institutions and other financial institutions see indications of these or other forms of illegal service provision, they can report them to us using the online form available on the Digital Supervision Portal or by email at handhaving@dnb.nl..

Over the past year, we completed the last examinations into unregistered crypto service providers. The resulting enforcement procedures are expected to be completed in 2025. With the entry into force of the Markets in Crypto Assets Regulation (MiCAR), enforcement of illegal crypto service providers will be the AFM's area of responsibility. Alongside enforcement measures against unregistered crypto service providers, we imposed one fine in 2024 for cutting up trust services.

9.2 Integrity supervision findings

9.2.1 Illegal trust service provision

With regard to illegal trust service provision, we see an increase in the number of reports about the cutting up of trust services. Cutting up trust services means providing a postal or visiting address together with other services, such as performing accounting work or preparing financial statements (trust service b). If a service provider splits these activities, outsourcing them to different service providers, trust services are cut up. In some cases, the initial service provider is paid a fee for outsourcing.

9.2.1 Unlicensed payment service provision

With regard to unlicensed payment service provision, we see an increase in the number of reports about the unlicensed money transfer services. This may be the case, for example, when a service provider receives an amount of money from someone with the sole purpose of forwarding it, often within a short time frame, to a third party.

9.3 Outlook

As the rules aimed at preventing money laundering and terrorist financing become stricter, integrity risks may shift to unlicensed or unregistered financial service providers. For this reason, we are relentlessly continuing our enforcement approach to illegal service providers. Whereas in recent years we deployed much of our capacity on the enforcement of unregistered crypto service providers, from 2025 we will devote more attention to illegal trust service providers and unlicensed payment service providers. This is because we receive many reports about these forms of illegal service provision.

We seek to counter illegal financial services by imposing both informal and formal enforcement measures. In doing so, we work closely with the Fiscal Intelligence and Investigation Service (FIOD), the Public Prosecution Service (OM) and the other chain partners represented in the Financial Expertise Centre (FEC).

10 Measures taken by DNB

This overview shows how DNB has used its supervisory tools to support necessary remediation at supervised institutions. Between 1 January 2024 and 31 December 2024, we took the informal and formal measures listed below in response to non-compliance with integrity regulations by supervised institutions.

Measures imposed on supervised institutions 1 January 2024 – 31 December 2024	
Formal measures	**18**
Issued an instruction	13
Imposed an order subject to penalty	1
Revoked a licence	2
Imposed an administrative fine	2
Informal measures	**15**
Compliance briefing	3
Written warning	12
Total	**33**
Disclosed formal measures	8

Between 1 January 2024 and 31 December 2024, we imposed 18 formal measures and 13 informal measures on supervised institutions for integrity breaches. Most of these were in the trust sector, and some of the instructions were issued to groups comprising several trust entities, each with their own separate licence. In general terms, the enforcement measures were mainly aimed at remedying significant shortcomings in the execution of customer due diligence and the effectiveness of the audit and compliance functions.

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

Follow us on:
Instagram
LinkedIn
X

DeNederlandscheBank

EUROSYSTEEM