Financial Intelligence Unit -
the Netherlands

Annual review FIU-the Netherlands 2025

Table of Contents

2025 in review

As I write this, only one month has passed since I started work at FIU-the Netherlands. I am truly impressed by the important work being carried out here. This is where intelligence, investigation, international work and both public and private collaboration come together; it is a dynamic, ambitious environment where I feel completely at home. FIU-the Netherlands plays a key role in the financial security sector: on the one hand, we pick up signals about potential criminal activity, while on the other hand, we ensure that this information reaches the places where it can make a difference. I see it as an honour to be able to continue this work as Acting Head.

At the same time, we find ourselves in challenging times. The world is rapidly evolving, and today's news could be out of date by tomorrow. It is against this backdrop that we are preparing for one of the biggest transitions of recent years: the introduction of the comprehensive European anti-money laundering package, which is due to come into force in just over a year's time. This legislation will have an impact on the entire system, from obliged entities to public partners. For FIU-the Netherlands, 2025 was therefore a year of intensive preparation and close collaboration within the sector. More on this in Chapter 3.

Chapter 1 focuses on the figures. Here, we examine the number of unusual and suspicious transactions, placing that development within the correct context. Chapter 2 centres on the results of our analysis. In previous years, the first part of Chapter 2 was roughly divided between money laundering and predicate offences, followed by a section on terrorist financing. The rest of the chapter would then discuss some major trends and notable results. This year, we have decided to take a different approach, focusing less on categories of offences and more on thematic clusters that reflect our working practices. These themes include corruption, fraud and terrorist financing. This new structure results in a more transparent approach and demonstrates the breadth of our analysis, without compromising the required diligence and discretion.

This annual review clearly illustrates all that FIU-the Netherlands achieved in 2025 under the leadership of my predecessor Hennie Verbeek-Kusters. I am proud and grateful to take over the reins from her, and I am inspired to continue building the future of this organisation with the same conviction and energy.

In 2025, FIU-the Netherlands took significant steps towards safeguarding the integrity of the financial system, in collaboration with our public and private partners. Combatting money laundering, underlying crime and terrorist financing requires ongoing commitment from everyone in this field. It is only together that we see more.

I hope you enjoy reading our 2025 annual review.

Lisette Heerze
Acting Head, FIU-the Netherlands

Chapter 1

The figures

This chapter presents the figures behind the work of FIU-the Netherlands in 2025. Under the Money Laundering and Terrorist Financing (Prevention) Act (Wwft), obliged entities are required to report suspicious transactions (STRs). These entities are also referred to as ‘gatekeepers’ and play a key role in safeguarding the integrity of the Dutch financial system. As experts in their field, they are expected to identify irregularities in transactions in a timely manner.

The *figures*

92,043
suspicious transactions

945
FIU requests top 3:
1. Police
2. Fiscal Information and Investigation Service
3. The Royal Netherlands Marechaussee

2,849
Article 17 requests[1]

Top 3 reporting groups with the highest number of reports

1. PSP's[2]	1.386.790
2. Banks	630.461
3. Virtual currency exchange service	327.826

1,779
institutions
reported at least one transaction

77
Financial Intelligence Reports
(FIR's)

15,068
case files
on suspicious transactions

613 incoming requests

Top 5:
1. Finland
2. Italy
3. Germany
4. Spain
5. Luxembourg

794 outbound requests

Top 5:
1. Germany
2. Belgium
3. Spain
4. United Arab Emirates
5. Lithuania

51%
of all transactions
have no sender or recipient with a Dutch connection

3,055,362
unusual transactions
40% of which were reported based on the subjective indicator

[1] *Article 17 of the Money Laundering and Terrorist Financing (Prevention) Act (Wwft) empowers FIU-the Netherlands to request data and intelligence from reporting entities. Furthermore, it allows FIU-the Netherlands to access the Banking Information Reference Portal. In 2025, FIU-the Netherlands accessed this portal 4,434 times.*
[2] *In 2025, as many as 90% of unusual transactions reported by PSPs had no connection with the Netherlands.*
51% of all transactions have no direct link to the Netherlands in terms of the sender or recipient.

1.1 Objective versus subjective

If a gatekeeper suspects a case of money laundering, predicate offences or terrorist financing, the unusual transaction must be reported to FIU-the Netherlands. FIU-the Netherlands receives UTs in a highly secure database and subjects them to further analysis. If the analysis reveals sufficient investigative interest or clear links to money laundering, predicate offences or terrorist financing, these transactions are declared suspicious (STR). The suspicious transactions are compiled into case files that FIU-the Netherlands then makes available to the relevant investigative, intelligence and security services so that they can conduct further investigations based on their own priorities.
This chapter examines the key trends in the 2025 figures. It also explains a number of key concepts that regularly appear in the tables and analysis, such as the objective and subjective indicators on which an unusual transaction may be based.

Objective indicators

Objective indicators are fixed threshold values. If these values are exceeded, the obliged entity must report the transaction. There are several objective indicators, which vary by reporting group. For example, all credit card payments exceeding €15,000 must be reported. These reports usually contain little context, and on their own, often do not provide a direct starting point for analysis. However, they are valuable as a supplement to ongoing analysis, for example to gain insights about financial positions and specific purchases. Of all of the unusual transactions that we received in 2025, 60% were reported based on an objective indicator.

Subjective indicator

The subjective indicator applies to all reporting groups. An obliged entity must report a transaction if it suspects that it is associated with money laundering, predicate offences or terrorist financing. In the transaction description, the institution explains the reason for that suspicion. The content of transaction descriptions and the obliged entities' own investigations prior to a report vary. However, they give FIU-the Netherlands more frequent cause to launch an analysis or manage an ongoing analysis than is the case with objective indicators. Of all of the unusual transactions that we received in 2025, 40% were reported based on the subjective indicator.

Differences by reporting group

The focus varies depending on the reporting group. Last year, accountants based virtually all of their reports on the subjective indicator, whereas payment service providers (PSPs) did so in only 11% of cases. These differences stem from sector-specific indicators and the characteristics of the type of service provided. The breakdown by reporting group is provided in Annex I, Table 7.

1.2 A nuanced assessment of the figures

The figures in this annual review are a snapshot of the reports of unusual transactions received. They do not provide a comprehensive picture of money laundering activities in the Netherlands. This partly depends on the way in which obliged entities submit their reports, the international nature of the Dutch financial system and, occasionally, on guidance provided by supervisory authorities. This is explained in more detail below.

It is worth noting that some obliged entities bundle 100 transactions into a single report, stating only the amount of the first or last transaction. As a result, the total value in the statistics may appear lower. The same applies to transactions in the crypto sector. Suppose someone purchases €100,000 worth of cryptocurrency and then uses that cryptocurrency to make a purchase. An obliged entity may then report both transactions to FIU-the Netherlands, which may declare both transactions to be suspicious. Two transactions, together worth €200,000, are then declared suspicious, while actually only one €100,000 payment was made. The transaction is counted twice, which distorts the total amount. Examples such as this show that determining the value of suspicious transactions requires a much more nuanced assessment.

Individual reports vs. aggregate reporting

The way in which institutions reports also has a major impact on the figures; in particular, whether or not to submit a single aggregate report warrants further explanation. The reporting method can significantly affect the number of reports and applies to several reporting groups. What does aggregate reporting mean in practice? Suppose a criminal defrauds a victim through 100 transactions each worth €1,000. One bank reports this as a single aggregate transaction of €100,000 because each transaction involves the same sender and beneficiary accounts. However, another bank may choose to report 100 separate transactions. Though both reporting methods are permitted, it does result in huge differences in the number of reports between banks. We observe a similar effect among other reporting groups; for example, among trust offices, the number of reports rose from 39 to 281, while among investment firms, the number rose from 168 to 512.

Through the Netherlands, not in the Netherlands

The international nature of our payment transactions could also mislead readers of our annual figures. Anyone looking at the 1.4 million reported unusual transactions from the PSP sector might think that these are all Dutch transactions, but that is not the case.
A significant proportion of the unusual transactions reported to FIU-the Netherlands are international transactions. These transactions can be divided into two categories. On the one hand, there are international transactions where the sender or beneficiary has a link to the Netherlands. On the other hand, there are transactions where neither the sender nor the beneficiary has a direct link to the Netherlands, but where the payment does pass through the Dutch financial system.
Example: suppose an Italian online shop engages a PSP based in the Netherlands to process online payments. When a German customer subsequently makes a purchase, the payment goes through the Dutch PSP. The PSP carries out transaction monitoring in accordance with the Wwft and may conclude that an unusual transaction has taken place. In line with the current legislation and regulations, the Dutch PSP then reports this to FIU-the Netherlands. Naturally, this transaction is included in all of our analysis. In such cases, we share these transactions with the FIUs of the countries concerned; in this example, Italy and Germany.

Within the PSP sector, over 70% of the 1.4 million unusual transactions in 2024 had no direct link to the Netherlands. Of all of the unusual transactions that we received in 2024, approximately 40% had no direct Dutch link in terms of sender or beneficiary.
In 2025, the international nature of the PSP sector increased even further: as many as 90% of the suspicious transactions reported by PSPs were found to have no link to the Netherlands. For the total number of transactions, that percentage stands at 51%. This highlights just how international our financial system is, and therefore, that the total value of suspicious transactions does not provide a comprehensive picture of the money laundering threat within the Netherlands.

Guidance from supervisory authorities

Besides whether reports are aggregated, there is another factor behind significant fluctuations in numbers. For instance, guidance published by supervisory authorities can result in an increase in reports. Following the release of such guidance, institutions may report transactions retrospectively, which often leads to a large volume of additional reports. In 2025, we observed this among credit card companies that reported fraud. These reports may include transactions from previous years that were only reported in 2025, following guidance published by a supervisory authority.

1.3 The major decreases

In 2025, FIU-the Netherlands received reports of over 3 million suspicious transactions. This represents a decrease compared to 3.5 million reports in 2024. One of the main reasons for this lies in the number of reports concerning credit card transactions, of which there were over 420,000 in 2024; in 2025, that number fell to around 191,000. Although this appears to be a significant decrease, it in fact signifies a return to normal levels as the number of reports in 2024 was exceptionally high. In 2023, for example, there were only 10,771 reports.
The sharp rise in 2024 had one clear cause: the Wwft supervisory authority for this sector, the Dutch Central Bank (DNB), instructed these institutions to report all forms of fraud. Where necessary, they were also required to do so retrospectively. As a result, the unusual transactions reported by this group in 2024 largely comprised fraud-related transactions linked to this catch-up exercise. In 2025, the institutions continued to report consistently on all forms of fraud.

The crypto sector

The second explanation for the decrease in the number of unusual transactions lies in the legislative changes affecting the crypto sector. Whereas crypto service providers reported 578,312 unusual transactions in 2024, this figure fell to 327,826 reports in 2025, which is a decrease of 44%. The decrease in the number of reports in this sector has several causes, all of which are linked to new legislation.
Since 30 December 2024, MiCAR (Markets in Crypto Assets Regulation) has applied to crypto service providers in the Netherlands. MiCAR is a European regulation governing the crypto market. It is the first EU-wide legislation for crypto services, setting out rules on transparency, consumer protection and financial stability. Before MiCAR came into force, a crypto service provider operating in several countries simultaneously had to apply for a licence in

each country. This meant that the service provider had to deal with different legislation and regulations in each country. MiCAR has rectified this, which, for parties operating in multiple EU countries, represents a significant simplification. Previously, these parties had to meet separate registration requirements in each country, which was both time consuming and costly. Now, the home country (the EU country in which their head office is located) determines which supervisory authority grants the licence. With a single national licence, they can operate legally in all 27 EU countries.
A consequence of these new legal frameworks is that many crypto service providers that are active in the Netherlands but do not have their head office here are no longer obliged to report in the Netherlands. This significantly reduces the number of reports here.
In addition, an objective indicator for certain transactions in the crypto sector has been abolished due to introduction of the European regulation. Previously, all crypto-related transactions of €15,000 or more had to be reported. The removal of this obligation is a second key reason for the decrease in the number of reports from this sector. The decrease does not, however, mean that our intelligence position has deteriorated, as European FIUs continue to exchange relevant transactions with one another.

Remote gambling

We observe another notable decrease among remote gambling providers. The number of reports from that sector fell by 68%, from 30,553 in 2024 to 9,828 in 2025. Since the Remote Gambling Act (Wet Kansspelen op afstand, Koa) came into force in 2021, remote gambling providers have been subject to stricter regulation by the Netherlands Gambling Authority. The legal gambling market has shrunk in value. In addition, net deposit limits have been in force since 1 October 2024 (€700 per month for adults and €300 for young adults), meaning that the objective indicator of €15,000 is no longer consistently being met. The low deposit limit also makes online gambling less appealing, as reflected in the number of people using these services.

Foreign intelligence

The third category showing a decrease is that of foreign intelligence. The number of reports fell from 191,000 in 2024 to 146,000 in 2025. By ‘foreign intelligence’, this report means intelligence from foreign FIUs, such as reports that are shared through a link with another European country, or analysis that is exchanged in which the Netherlands plays a key role, sometimes even beyond Europe.

The vast majority of reports in the first category originate from a relatively small number of European countries, which sent fewer reports to the Netherlands in 2025 compared to 2024. This is reflected in the table below, and there is no clear explanation for it.

Table 1: Foreign intelligence

2024		2025	
Country	Number	Country	Number
Italy	174,106	Italy	133,638
Ireland	8,905	Ireland	3,545
Luxembourg	7,793	Luxembourg	1,619
Total	**190,804**		**141,417**

1.4 The major increases

Looking at the reporting groups for which the number of reports rose in 2025, there are several that clearly stand out. For example, the number of reports from electronic money institutions rose from 7,034 to 22,496. An electronic money institution (EMI) is a financial undertaking that issues virtual IBANs and electronic money. This is digital value, for example on a prepaid card, which represents a claim on the EMI and can be used to make payments to third parties. One EMI grew rapidly in 2025, and that market share led to additional reports.

Banks also saw an increase of 96,358 reports in 2025, due to a number of banks having expanded their services in the Netherlands. In addition, banks are increasingly reporting suspected fraud at transaction level, whereas money laundering is often reported in a more aggregated manner. Reporting individual transactions leads to an increase in the overall number of reports.

The ‘non-bank leasing’ reporting group shows an increase in reports from 87 in 2024 to 389 in 2025. This increase is caused by a single specific reporting body that reported a major fraud case comprising over 350 transactions. The information in Section 1.1 regarding aggregate reports is also reflected in the number of reports from trust offices, lawyers and investment firms. This number shows a relatively large increase, which is due to the fact that several unusual transactions within a large series of transactions were reported to FIU-the Netherlands by a few obliged entities as individual transactions.

A clear increase in the number of reports is also evident within the PSP reporting group. This increase is largely attributable to a single money transfer agency, which has designated two new countries as high risk in its monitoring rules. As a result, all transactions related to these countries had to be reported as unusual retrospectively.

1.5 Suspicious transactions

FIU-the Netherlands receives reports of unusual transactions. We then analyse those reports and establish whether the transactions are suspicious. If they are found to be suspicious, we share them with investigative, intelligence and security services. In this way, the entire Wwft chain enhances the integrity of the financial system. The table below shows the numbers of suspicious transactions in 2024 and 2025.

Table 2: Number of STRs and case files

	transactions 2024	transactions 2025	files 2024	files 2025
Own investigation	61,410	37,545	2,994	2,537
• Of which based on foreign FIU’s	2,869	3,351	178	236
FIU request	3,618	7,451	317	388
Match Investigation and Prosecution[3]	53,380	47,047	12,995	12,143
Total	**118,408**	**92,043**	**16,306**	**15,068**

Table 2 shows that in 2025, 92,043 suspicious transactions in 15,068 case files were shared with the relevant investigative, intelligence and security services in the Netherlands and abroad. In 2024, there were 118,408 suspicious transactions. The 2025 figure therefore represents a 22.3% decrease. The number of suspicious transactions per year is inherently volatile.

[3] *As part of the Match Investigation and Prosecution initiative, FIU-the Netherlands makes available case files containing suspicious transactions that relate to individuals already under investigation.*

Other case files

Table 2 also includes case files based on FIU requests. These are case files arising from requests by special investigative services to conduct a targeted analysis as part of an ongoing criminal investigation. The 'Match Investigation and Prosecution' category relates to case files containing suspicious transactions made available by FIU-the Netherlands concerning individuals registered as suspects with investigation services. Although these individuals are already under scrutiny, the financial intelligence service regularly provides valuable new insights. For example, it may emerge that, in addition to known bank accounts, a suspect holds assets in other places of which the investigation team was previously unaware. It could also emerge that the suspect maintained financial relationships with parties that had not yet come to light. Table 3 shows the breakdown between objective and subjective reports within these various workflows.

Table 3: Proportion of objective and subjective reports within the STRs

Workflow	Propotion of subjective (%)	Propotion of objective (%)
Own investigation	87%	13%
• Of which based on information requests from foreign FIUs	90%	10%
FIU request	81%	19%
Match Investigation and Prosecution	88%	12%

Own investigations

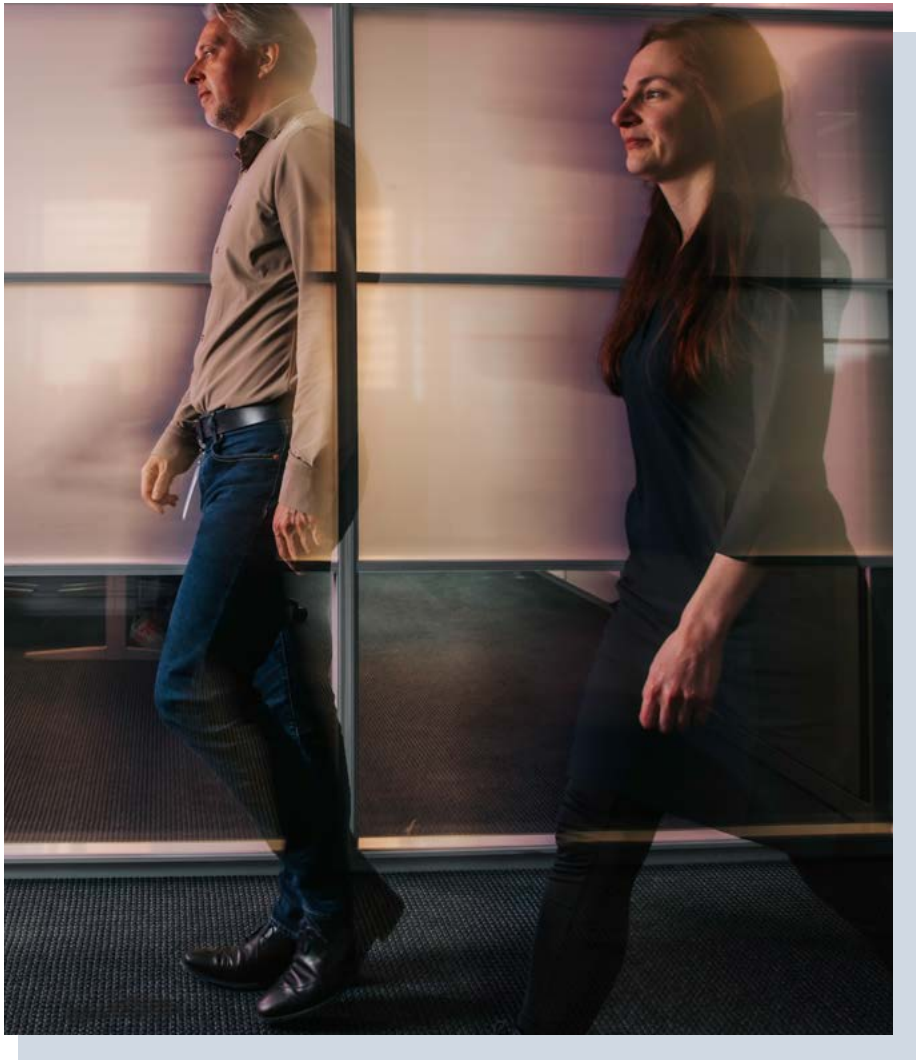
In 2025, the number of case files arising from our own investigations has fallen. By 'own case files', we mean case files launched based on intelligence, thematic searches in our database and requests from abroad. This analysis is often more complex, as reflected in the higher number of transactions per case file. This category accounts for only 17% of the case files submitted by FIU-the Netherlands, but it does contain 41% of all suspicious transactions for the year.
The number of case files produced by FIU-the Netherlands from its own investigations always fluctuates. Unlike organisations with a uniform, predictable caseload, each case file has its own complexity and scope. Therefore, output cannot be predicted based on capacity alone. For example, the number of transactions per case file can vary greatly, from just one to thousands.
The amount of time required to analyse any given transaction can also vary significantly.
The decrease in the number of case files can also be partly explained by the departure of experienced investigators, the induction of new investigators into complex matters and the implementation of new analytical tools that require testing capacity from investigators.

Recipients

Table 4 shows where our own investigation files 'end up'. The two largest recipients are the Dutch National Police and the Fiscal Information and Investigation Service (FIOD). Case files in the 'other' category are sent to authorities such as the Netherlands Food and Consumer Product Safety Authority, the Human Environment and Transport Inspectorate and the Royal Netherlands Marechaussee.

Table 4: Case file recipients

Case file recipient	Proportion
National Police	50%
FIOD	43%
Other	2%
Netherlands Labour Authority	5%
Total	**100%**



Suspicious transactions by reporting group

Looking at Table 9 (provided in the annex) for the numbers of suspicious transactions per reporting group, it is striking that a significant decrease can be observed among custodial wallet providers, virtual currency exchange services and remote gambling providers alike. The explanations for this are consistent with the causes of the decrease in the number of UTs from these reporting groups, as explained in Section 1.3. A sharp decrease in the number of STRs is also evident among PSPs compared to 2024, while the number of UTs has remained virtually unchanged. It was noted above that fewer PSP reports in 2025 relate to the Netherlands, resulting in fewer transactions being declared suspicious.
In addition, gambling is becoming less appealing due to government policy, as reflected in the halving of the number of suspicious transactions at gambling casinos. In contrast, foreign intelligence has seen an increase. The number of STRs rose from 457 in 2024 to 1,345 in 2025. This can be explained by one specific case file involving an exceptionally high number of foreign reports declared suspicious (over 1,100).

Chapter 2

Interpretation

FIU-the Netherlands works using thematic clusters that bring together intelligence and analysis relating to specific money laundering and terrorist financing risks. These clusters have been selected based on the priorities of the investigative services, the objectives of the collaborations in which FIU-the Netherlands participates, the findings of the National Risk Assessment (NRA) on money laundering and terrorist financing and the priorities of the Financial Action Task Force (FATF). This chapter reports on the work and analysis carried out by FIU-the Netherlands within these themes in 2025, providing a coherent picture of the trends, phenomena and risks that were the focus of our work.

2.1 Criminal money flows

Organised crime is widespread. Criminals line their pockets through activities such as drug trafficking, human trafficking, fraud and money laundering. These activities are often accompanied by intimidation and serious violence.

Suspicious transactions are extremely valuable to investigations into criminal money flows. In addition to providing information about criminal proceeds, underground banking, money laundering schemes and facilitators, they offer opportunities to tackle the criminal business process. Suspicious transactions contain valuable information for criminal investigations into virtually all types of crime. Money laundering, fraud and drug trafficking are obvious examples. But the analysis also sheds light on related criminal activities such as attacks involving illegal fireworks, contract killings and facilitating logistical operations for organised crime groups. In addition to financial information, FIU-the Netherlands case files contain a wealth of tactical information that can help identify modus operandi, suspects and locations. On more than one occasion, it has become apparent that our case files can link various investigations in ways that were previously unrecognised without these case files.

Table 5: The number of STRs and case files from the Criminal Money Flows cluster in 2025

Subdivision	Number of STRs	Proportion (%)	Number of case files	Proportion (%)
Hard drugs	946	33.68%	87	35.51%
Fraud	283	10.07%	11	4.49%
Money laundering	1,561	55.57%	143	58.37%
Other	19	0.68%	4	1.63%
Total	**2,809**		**245**	

Explanation of the table

- The majority of case files concern multiple forms of crime in combination with money laundering. These include violence, human trafficking, people smuggling, burglaries, hard drugs, synthetic drugs, fraud and underground banking.
- Case files related to money laundering in combination with fraud, money laundering or hard drugs have been classified under the other category rather than under ‘money laundering’.
- By ‘other’, this report means burglaries, human trafficking, violence and embezzlement.

Transit accounts

What stands out in our analysis is the extensive use of transit accounts, which are bank accounts used by criminals to quickly move illegally obtained money. The aim is to conceal the origin and destination of the money and hinder detection. The money usually only remains in the transit account for a short period of time and is transferred almost immediately.
A facilitating group enables transactions to take place at the request of various criminal networks. These clusters of companies and accounts are used for various payments. Examples include:

- channelling the proceeds of fraud;
- paying for front companies;
- purchasing luxury goods;
- paying for confiscation claims and lawyers.

Analysis of the modus operandi of transit accounts

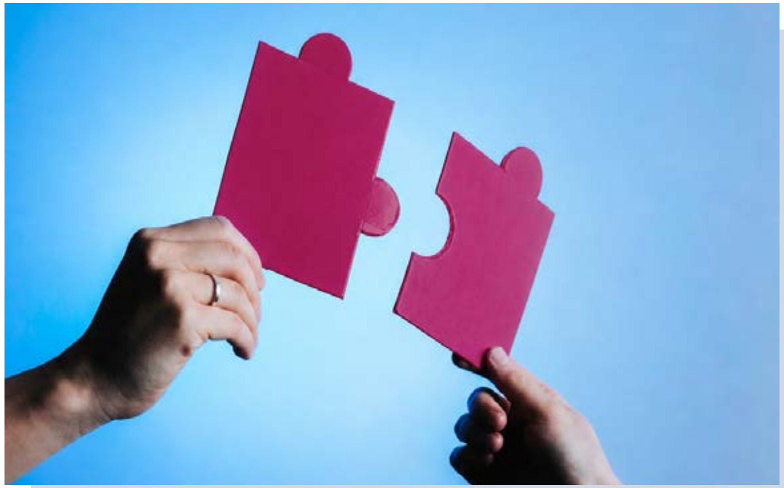
Due to the jumble of payments through these transit accounts, linking a transaction to the correct criminal organisation is an extremely complex process. In collaboration with the investigative authorities, FIU-the Netherlands analyses the modus operandi of criminal networks where transactions are carried out on request for various criminal networks. Following the results of the analysis, a phenomenon-based investigation was launched, which led to the launch of criminal investigations. Based on the modus operandi observed in the transit accounts, 26 case files were declared suspicious. These case files were provided to the investigation team for the purposes of the phenomenon-based investigation.

Investigation into money laundering schemes at main ports

In the 2023 annual review, we wrote about the successful Thalys project: a public-private partnership with ING, Zeehavenpolitie Rotterdam (Rotterdam's sea port police service), the FIOD and FIU-the Netherlands. Within this project, investigations were carried out into transactions that could indicate corruption and drug trafficking in or around the port of Rotterdam.
This project was subsequently continued in collaboration with other parties, such as the Royal Netherlands Marechaussee at Schiphol Airport, the Zeehavenpolitie in Vlissingen and various agencies associated with the North Sea Canal area. As a result of these various projects, a total of 89 case files were declared suspicious following investigations by FIU-the Netherlands and referred to the participating investigative authorities. The case files have led to the launch of various criminal investigations. In one instance, a case file led to the termination of employment of an employee working for a company operating in an area of significant interest to criminals. This followed consultation between the investigative authority and the company.

Investigation into excessive violence

Excessive violence is a recurring theme within organised crime. At the request of the Nationale Intelligence Voorziening (‘National Intelligence Service’, NIV), FIU-the Netherlands therefore took part in a ‘sprint week’ in 2025, during which excessive violence in the Netherlands and Belgium was scrutinised. FIU-the Netherlands actively investigated transactions linked to individuals prioritised by the NIV. The investigation resulted in 13 new case files, which FIU-the Netherlands provided to the NIV. Analysis of financial transactions led to the identification of relationships between individuals and clusters. New individuals have also come to light, including sellers of illegal fireworks. The NIV is responsible for transferring the FIU case files to the relevant units.



Figures on criminal money flows

245	Files
2,809	Number of suspicious transactions

2.2 Cybercrime

The scale of digital crime continues to grow. Criminals exploit the relative anonymity of cryptocurrencies for various forms of fraud, money laundering and terrorist financing. FIU-the Netherlands identified several examples of this in its analysis.

The investigations that FIU-the Netherlands conducted into cybercrime in 2025 can broadly be divided into the following: investigations relating to cryptocurrencies, cyber fraud and investigations arising from the J5 Cyber Challenge (more information on this is provided below).

Cryptocurrencies

Cryptocurrencies featured in 29 case files containing 524 transactions. The investigations focused on a wide range of criminal activities, including:

- illegal online marketplaces operating on the dark web;
- illegal crypto service providers serving customers without the required licence;
- crypto transactions for the purchase of child sexual abuse material.

The total value of the cryptocurrency investigations conducted in 2025 amounts to €22 million. Of this, a single case accounts for over half of the value of the transactions declared suspicious: €11 million. This case focuses on fraud relating to funds from a construction deposit, which the loan recipients misused by investing them in cryptocurrency.

Helpdesk fraud

In 2025, FIU-the Netherlands received several reports of helpdesk fraud,[3] including from customers of a Dutch crypto exchange, which is a platform where you can buy and trade cryptocurrency. Criminals posed as employees of the platform and contacted customers by text message or telephone, warning

[4] *Formally, all forms of helpdesk fraud are referred to as ‘bank helpdesk fraud’. As this case concerns a crypto exchange service rather than a bank, we have used the term ‘helpdesk fraud’ to avoid confusion.*

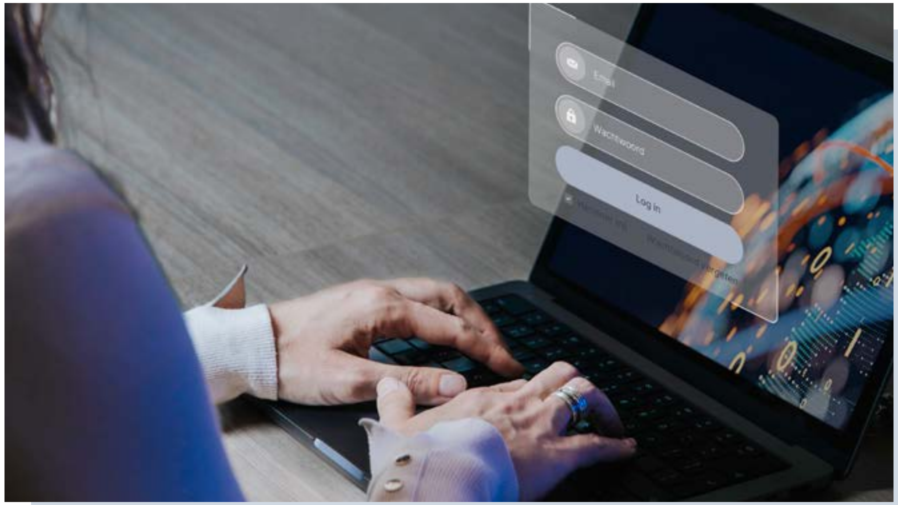
them that their wallet (a digital wallet for cryptocurrency) was at risk. Victims were told to call a number and then advised to transfer their cryptocurrency to a secure 'trust wallet', for which they first had to download an app. Once the victims had transferred their funds, the perpetrators diverted the cryptocurrency to external wallets that they themselves had access to.
Due to the low reporting rate for crypto losses, there is limited information about the number of victims and total loss. In this case, the initial estimate was approximately €500,000 in losses, but analysis conducted by FIU-the Netherlands revealed that this type of fraud was much more extensive, with the reported transactions alone representing four times that estimate. Blockchain analysis was used to identify several wallets into which large sums of fraudulent funds were channelled.

Terrorist financing with bitcoins

Another analysis led to the arrest of a man in March 2025 by the FIOD.[5] The man is suspected of financing terrorism with bitcoins. The FIOD launched its criminal investigation following a report of unusual transactions by a crypto exchange to FIU-the Netherlands. The report revealed that the suspect had sent bitcoins to wallet addresses suspected of being linked to terrorist organisations. In recent years, terrorist financing using bitcoins has become increasingly common on a global scale, as evidenced by criminal investigations in Europe and the USA. This is also confirmed by analysis conducted by our own Terrorist Financing Task Force.

Cyber fraud

These investigations focus on online crime. We encountered several forms of online fraud in our analysis, and the best known is phishing. So-called 'rug pulls' were also investigated; a specific type of investment fraud that is particularly prevalent within the cryptocurrency sector. A rug pull occurs when the creators of a crypto project build trust, for example through influencers and social media, get people to invest money (usually crypto) and then suddenly disappear with the proceeds. The creators, for instance, withdraw all of the funds in one go, rendering the crypto coin worthless.



[5] https://www.fiod.nl/aanhouding-vanwege-terrorismefinanciering-met-bitcoins/

Our investigations also uncovered 'co-scams', where fraudsters pretend to be investing alongside you (in co-investments). The fraudster acts as a partner rather than a seller. However, as soon as your investment is received, your 'partner' vanishes with the proceeds.

J5 Cyber Challenge

FIU-the Netherlands also gained valuable information during the J5 Cyber Challenge. This annual international collaboration and investigation event is organised by the Joint Chiefs of Global Tax Enforcement (J5), which is a collaboration between the FIODs and FIUs of the United Kingdom, the USA, Australia, Canada and the Netherlands. Experts from various disciplines spend a week working closely together on joint analysis of cyber-related financial crime. The 2025 edition took place in Zwolle and focused on intelligence involving cryptocurrency. The investigations are still ongoing, and we hope to be able to share the insights gathered at some point in 2026.
In addition to the operational output, the J5 week yielded further valuable results. It enhanced our international collaboration and the opportunity to share knowledge on cryptocurrency and crypto investigations provided added value for all participants.

Enhancing collaboration with the police

In 2025, FIU-the Netherlands took significant steps towards enhancing collaboration with police units. Our operational effectiveness has noticeably increased thanks to frequent coordination with the cyber intelligence teams of the regional units, the national intelligence forum and several police investigation departments. This has led to improved follow-up on FIU case files and a clearer picture of underlying patterns in financial and digital crime.

Cybercrime figures

69 files

6,661 Number of suspicious transactions

2.3 Healthcare fraud

Healthcare fraud remains a major problem. In 2025, we declared 63 case files suspicious. In total, these files related to approximately 1,000 transactions. Our analysis revealed a number of worrying trends that have been ongoing for some time and continued in 2025.

Man opgepakt wegens miljoenenfraude met Cozo-subsidie

ACCOUNTANCY, NIEUWS

De opsporingsdienst van de Arbeidsinspectie heeft een 49-jarige man opgepakt op verdenking van witwassen, valsheid in geschrifte en fraude met corona-subsidieregeling Cozo.

1 december 2025 door Accountancy Vanmorgen

In totaal zou hij ruim € 8 miljoen ten onrechte hebben losgeweekt. T
doorzoekingen gedaan in twee woningen en een bedrijfspand. De m
netwerk met anderen en faciliteerde 32 zorgondernemingen die on

NOS Nieuws • Vrijdag 4 juli 2025, 09:48

Miljoen aan cash, merktassen en sieraden: CAK-medewerkers betrokken bij zorgfraude

De Arbeidsinspectie heeft gisteren beslag gelegd op meer dan een miljoen aan contant geld en luxe goederen zoals merktassen, sieraden en horloges in een onderzoek naar fraude met zorggeld voor vreemdelingen zonder verzekering. De spullen werden gevonden bij doorzoekingen van vijf woningen, voertuigen en kluizen.

Bij de fraude zijn medewerkers van het Centraal Administratie Kantoor (CAK) betrokken, zo meldt de Arbeidsinspectie. Het CAK zegt tegen de NOS dat twee

Traditional healthcare fraud

The number of suspected cases of ‘traditional’ healthcare fraud remained high in 2025. By this, we mean claiming healthcare costs for care that was not provided, was only partially provided or was of insufficient quality. The picture emerging from our analysis is that there are parties operating solely to extract as much money as possible from the healthcare system. These are organised networks that collude in order to submit as many false claims as possible.

Dubious self-employment

‘Dubious’ self-employment is well represented in the analysis. Dubious self-employed individuals are people who set up their own businesses in the healthcare sector without any relevant experience. In some cases, they have committed criminal offences in the past. Through the Health and Youth Care Inspectorate, the Inspectorate of Education and the National Police, it is known that dubious self-employed individuals in the healthcare sector regularly use false qualifications and qualifications issued under false pretences. Many also have varied criminal records.
Our analysis shows that sole traders generate exorbitant turnover, yet hardly pay any tax. These sole traders appear to inflate fictitious costs by paying false invoices to companies in professional money-laundering networks. These invoice payments are presumably settled in cash, but for tax purposes, there is hardly any taxable profit left.

Using temporary staffing agencies

FIU-the Netherlands observes in its analysis that large, legitimate healthcare organisations make extensive use of temporary staffing agencies in the healthcare sector. Most workers supplied by these agencies are self-employed individuals, some of whom are of dubious character and exhibit various characteristics, as described above. The temporary staffing agencies included in our analysis are experiencing enormous growth in turnover, which is unusual for this sector. They have managed to tap into a source of healthcare staff that other organisations are unable to find. Given the reports of fake qualifications in the healthcare sector, this carries significant risks.

An ecosystem of financial and economic crime

Finally, the analysis provides information about an ecosystem of financial and economic crime, of which healthcare fraudsters form part. In such a system, everyone has their own role to play (task specialisation) and criminals and fraudsters use each other's services:

- A group of criminals focuses on recruiting straw owners.
- Professional money launderers use straw owners to set up companies in the straw owners' names.
- Healthcare fraudsters use money laundering structures to settle false invoice payments, evade tax and pay workers in cash.
- Drug criminals use money laundering structures to convert their cash (presumably derived from drug trafficking) into bank transfers, including those originating from the healthcare sector.
- Somebody specialises in producing fake qualifications. A temporary employment agency uses this service to employ a self-employed person without the correct paperwork.
- The self-employed person sees an opportunity to earn money in the healthcare sector through the agency. Money laundering schemes are then used to evade tax through false invoices.

In short, there are many examples of criminals and fraudsters who, within broader ecosystems of financial and economic crime, purchase and offer services to commit their preferred offences. Task specialisation leads to economies of scale. Unfortunately, this manifests itself in the form of larger fraud structures, greater adaptability and significantly more fraudulently obtained money for criminals.

Arrests, seizures and convictions

The analysis carried out by FIU-the Netherlands led to a number of interventions in 2025. At the end of January, for example, the Investigation Service of the Netherlands Labour Authority arrested three people for laundering at least €1 million in healthcare funds.[6] In December, a 49-year-old man was arrested on suspicion of committing fraud under the Coronabanen in de zorg (COZO) subsidy scheme, money laundering and forgery.[7] The suspect collaborated with other individuals and legal entities, and it is believed that they formed a criminal network. The man facilitated 32 healthcare companies that wrongfully applied for and received over €8 million in COZO subsidies.
In another investigation into healthcare funding fraud, the Investigation Service of the Netherlands Labour Authority seized over €1 million in cash and luxury goods, including designer bags, jewellery and watches.[8] This case, which FIU-the Netherlands contributed to by analysing unusual transactions, concerns fraud involving claims by rogue healthcare providers for medically necessary care for

[6] https://www.nlarbeidsinspectie.nl/actueel/nieuws/2025/01/29/3-aanhoudingen-voor-witwassen-van-zorggelden
[7] https://www.nlarbeidsinspectie.nl/actueel/nieuws/2025/12/02/man-aangehouden-voor-miljoenenfraude-met-coronasubsidies
[8] https://www.nlarbeidsinspectie.nl/actueel/nieuws/2025/07/04/doorzoekingen-in-zorgfraudeonderzoek-met-subsidieregelingen-voor-onverzekerden

the uninsured and care for uninsurable foreign nationals (the 'Subsidy Scheme for Medically Necessary Care for the Uninsured' (SOV) and the 'Scheme for Uninsurable Foreign Nationals' (OVV)). It is suspected that several employees at the Central Administration Office (CAK) were involved in the fraud. The CAK is an independent administrative body that performs public tasks on behalf of the Ministry of Health, Welfare and Sport. One of those tasks is paying healthcare claims to healthcare providers. FIU-the Netherlands has also sent a report to the Ministry of Justice and Security regarding misuse of the SOV and OVV subsidies. Furthermore, in June 2025, the Amsterdam District Court convicted a 45-year-old man of embezzling €414,147 and laundering €320,859 in healthcare funds. The judge sentenced him to 16 months' imprisonment, six months of which were suspended.[9] The healthcare funds originated from the healthcare company managed by the man's daughter. During the analysis of the unusual transactions, FIU-the Netherlands identified large transfers from the healthcare company to the man's private accounts. It was also noted that thousands of euros in cash were withdrawn from the man's private accounts each month and that large sums were spent on transactions through TikTok.

[9] https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2025:3781&showbutton=true&keyword=verduister&idx=1

Case study

Misuse of care funds uncovered

Three banking institutions reported several dozen unusual transactions involving two healthcare companies. In particular, the banks noticed that there were a large number of cash withdrawals. The healthcare funds were spent on luxury consumer goods and other goods unrelated to the sector.

FIU-the Netherlands analysed the reports and the following emerged:

- The liquidator had previously established that two individuals involved were guilty of personal care budget (PCB) and bankruptcy fraud.
- One of the suspects has an extensive criminal record and had previously been a suspect in a criminal investigation into fraud.
- There were irregularities in the tax payroll data of one of the individuals involved.
    - The companies had generated a remarkably high amount of profit.
    - Notably few labour costs had been reported.
    - The individuals involved drove very expensive cars, raising questions about their financial situation.

hese are merely a few of the findings. The case file was transferred to the Netherlands Labour Authority, which has since arrested several people on suspicion of laundering over €1 million in healthcare funds.

Utrechters opgepakt voor witwassen van ruim 1 miljoen aan zorggeld

29 januari 2025, 11:49 • Aangepast 6 maart 2025, 02:02 • 2 minuten leestijd

Ter illustratie.
© Politie

Utrecht - Drie Utrechters zijn aangehouden door de opsporingsdienst van de Arbeidsinspectie. Zij worden verdacht van het witwassen van meer dan 1 miljoen euro aan zorggeld. De verdachten zijn twee vrouwen van 55 en 60 en een man van 61 jaar uit de regio Utrecht.

Archieffoto. © Marco Okhuizen

Verbaasde rechercheurs vinden kilo's harddrugs bij inval in Utrechtse woning in groot onderzoek naar zorgfraude

Stomverbaasd waren ze, rechercheurs van de Nederlandse Arbeidsinspectie die vorige week een woning midden in Utrecht binnenstapten. Tijdens hun zoektocht naar waardevolle spullen, stuitten zij op tientallen kilo's harddrugs.

Healthcare fraud figures

63	Files
1,000	Number of suspicious transactions

2.4 The Caribbean Netherlands

The islands of Bonaire, St Eustatius and Saba (the BES islands) are special municipalities of the Netherlands. Together, they form the Caribbean Netherlands. FIU-the Netherlands is also the reporting centre for unusual transactions for these islands.

In 2025, 8,853 unusual transactions were reported in the Caribbean Netherlands by 20 different 'obliged service providers', as obliged entities are known in the Caribbean Netherlands. This means that the number of reports remains virtually stable compared to 2024, when the number of unusual transactions reported stood at 8,596.

Fewer case files, more suspicious transactions

Table 6 shows the numbers of suspicious transactions and case files compiled in 2025. While the number of case files fell from 61 in 2024 to 44 in 2025, the number of suspicious transactions rose from 249 in 2024 to 1,955 in 2025. The reduction in the number of case files can be partly explained by a comprehensive phenomenon-based analysis of underground banking. This analysis has resulted in more detailed case files containing a large number of suspicious transactions.

Table 6: Numbers of suspicious transactions (STRs) and case files in the Caribbean Netherlands

Reason for reporting	Number of STRs	Proportion (%)	Number of case files	Proportion (%)
Own investigation	1,698	87%	17	39%
FIU request [10]	224	11%	9	20%
Match Investigation and Prosecution [11]	33	2%	18	41%
Total	**1,955**		**44**	

[10] In the case of an FIU request, a special investigative service asks FIU-the Netherlands to carry out targeted analysis for the purposes of an ongoing criminal investigation.
[11] In the context of Match Investigation and Prosecution, FIU-the Netherlands makes files available that contain suspicious transactions related to suspects who are already under investigation.

Real estate transactions predominate

Real estate transactions feature frequently in the case files. Approximately one in three case files declared suspicious contains at least one real estate-related transaction. Our analysis shows that real estate transactions reported to FIU-the Netherlands are often linked to other forms of crime, such as labour exploitation, fraud, corruption, human trafficking, drug smuggling and underground banking. This connection may help to indicate the origin of the funds and subversive activities.
We shared the information gained from our analysis during a seminar on the risks of real estate investments. The seminar was organised by the supervisory authorities in the BES islands (the Dutch Central Bank, the Dutch Authority for the Financial Markets, Bureau Toezicht Wwft ('Wwft Supervision Bureau') and Toezichtautoriteit Wwft BES-Advocatuur ('BES Wwft Supervision Authority for the Legal Profession'). We highlighted the recurring indicators found in transactions declared suspicious. We also used case studies to emphasise the importance of timely, accurate reporting for a comprehensive understanding of money laundering schemes and targeted follow-up actions.

Phenomenon-based analysis

One phenomenon that received particular attention in 2025 was underground banking. This involves various forms of payment transactions outside of the regulated financial infrastructure that are used to move criminal funds. Reports of unusual cash withdrawals and deposits, as well as reports of non-cash transactions and transactions by legal entities, provide important information about the modus operandi. Based on strategic analysis, FIU-the Netherlands investigates both the physical movement of criminal cash and the misuse of the regular payment system. The aim is to identify structures and detect subversive patterns and means by which underground banking is facilitated.

Figures for the Caribbean Netherlands

44	Files
1,955	Number of suspicious transactions

2.5 Corruption

In 2025, FIU-the Netherlands detected various forms of public official corruption and private party corruption in its analysis. Potential breaches of the European public procurement directives stood out prominently in our analysis.

Corruption is a collective term that does not appear as such in the Dutch Penal Code, but acts associated with it do appear. These acts include bribery, forgery, leaking and falsifying information and accepting gifts such as bribes and kickbacks.

The importance of corruption investigations

As there are always one or more aggrieved parties, it is important to investigate corruption. Corruption leads to unfair competition, greater inequality between the rich and poor and higher prices for consumers. It also undermines trust in the government at both national and local levels. Reports of corruption therefore need to be analysed in order to safeguard the integrity of both the public and private sectors.

Types of analysis

Within the theme of corruption, FIU-the Netherlands distinguishes between different types of analysis:

- **Private party corruption:** This concerns investigations in the Netherlands and abroad involving a bribery element, mostly in the private sector. FIU-the Netherlands forwards case files on private party corruption to the FIOD's Anti-Corruption Centre (ACC). The same applies to case files on foreign public official corruption.
- **Public official corruption:** These investigations involve a Dutch public official. FIU-the Netherlands refers these cases to two parties:
  - **The Rijksrecherche:** These are investigations into civil servants (police officers, local government officials and employees of government ministries) where a criminal element is involved. It may concern bribery, forgery or another criminal offence.
  - **Royal Netherlands Marechaussee (KMar):** These investigations concern

individuals working for the Ministry of Defence. As with WODC cases, there may be a criminal element here, which need not relate exclusively to corruption-related offences.

Bribery

In 2025, our analysis revealed several forms of public official and private party corruption. An example is the arrest of two men by the FIOD in a criminal investigation into domestic corruption. The suspects, a man and a former employee, were accused of private party bribery. The investigation was launched following a report of an unusual transaction to FIU-the Netherlands. The suspect is alleged to have bribed his former employee to secure a multimillion-euro contract. The other man received a commission of hundreds of thousands of euros for this, possibly without his employer's knowledge. Cryptocurrency, two cars and various bank accounts were seized. [12]

Bribes

The corruption cluster also completed analysis regarding suspected cases of corrupt employees at various government departments. Illustrative of such cases is a matter in which two companies were suspected of public official corruption and forgery. For years, bribes were paid through the suspect companies to secure construction contracts for public projects abroad. The payments, presumably intended for a high-ranking foreign official, were transferred to foreign bank accounts held by an intermediary. To conceal the payments, false documents such as agreements and invoices were drawn up. The projects were financed by a Dutch bank and insured by the Dutch government. The criminal investigation began following a report of an unusual transaction to FIU-the Netherlands. [13]

European public procurement legislation

A topic that emerged prominently from our analysis is potential breaches of the European public procurement directives. Failure to comply with public procurement legislation is risky and leaves government organisations vulnerable to abuse and corruption.
In its analysis, FIU-the Netherlands regularly identifies transactions that indicate potential breaches of these European public procurement directives; in particular, a failure to put contracts out to tender where this is required.
The reports show that, for several years now, a number of local and provincial authorities have been alerted by a reporting body to shortcomings in their compliance with public procurement rules. Nevertheless, in a significant proportion of the cases known to us, little to no improvement has been observed in practice.
An example of a breach of European public procurement legislation concerns the investigation conducted by the WODC and the FIOD into corruption and fraud concerning tenders by the Municipality of Rotterdam, to which FIU-the Netherlands contributed.[14] There is an ongoing investigation into this matter, which is being led by the Dutch Public Prosecution Service (OM).

[12] https://www.fiod.nl/twee-aanhoudingen-in-onderzoek-naar-binnenlandse-corruptie/
[13] https://www.fiod.nl/doorzoekingen-in-internationaal-corruptie-onderzoek/
[14] https://www.om.nl/actueel/nieuws/2025/02/18/rijksrecherche-en-fiod-doen-doorzoekingen-in-corruptieonderzoek

Forms of corruption

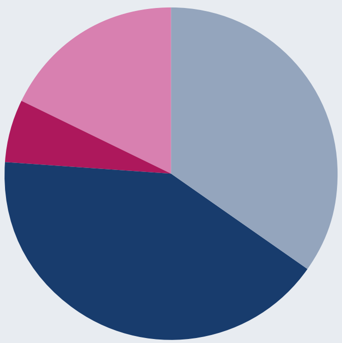
Corruption comes in all shapes and sizes. There are common forms of corruption, such as bribing public officials with the aim of gaining influence, a licence or a contract. In addition to these classic forms, corruption also occurs in the form of so-called ‘kickback schemes’, the bribed party receives a secret payment that is partly channelled back to the briber. These schemes are particularly prevalent within the private sector. Although such practices are sometimes presented as entrepreneurship, they generally result in one or more parties being disadvantaged.

Corruption figures

174 Files

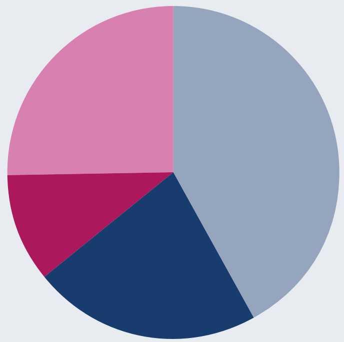
726 Number of suspicious transactions

Files



- 47: Anti-Corruption Centre (ACC)
- 56: Rijksrecherche
- 8: Royal Netherlands Marechaussee
- 24: Other

Total transactions reported



- 305: Anti-Corruption Centre (ACC)
- 162: Rijksrecherche
- 77: Royal Netherlands Marechaussee
- 182: Other

Interview

I feel so proud when I see a case that I've worked on featured in the news.

Linda* works as a financial investigator specialising in corruption. In this interview, she talks about her work: "You really notice societal issues being reflected in the work, and you can make a difference."

Is corruption really a big issue in the Netherlands?
"We're still in the top ten least corrupt countries globally, but unfortunately, the Netherlands has slipped down the anti-corruption index in recent years. Thankfully, bribing the police and other officials isn't seen as a 'normal' thing to do here, as it is in some countries. But we're not slipping down the anti-corruption index for no reason. Corruption does exist in the Netherlands, though it tends to happen more under the radar. However, it can involve large sums of money and have serious consequences, so it's important to combat corruption here as well."

What actually is corruption?

"There are two types of corruption: public official corruption and private party corruption. Public official corruption occurs when an employee at a government organisation does, or fails to do, something in order to gain a personal advantage. Private party corruption concerns fraud, bribery and other forms of abuse of power in the private sector."

Can you give an example of private party corruption?

"Take Robert and Michiel, for example: old friends who know each other from football. Robert works for a company that is selling a plot of land. Armed with that inside information, Robert and Michiel set up a small company to buy that plot of land. Since Robert is responsible for sales at his company, he has quite a bit of say in the matter and is able to exert pressure. He ensures that the plot of land is sold for a very low price to the small company he has set up with Michiel, but of course his employer is unaware of this. A short while later, Michiel and Robert then sell the plot of land on for a much higher price, making a tidy profit in the process. This is unfair to both the second buyer and Robert's employer. This form of corruption is also common when awarding major contracts."

Is corruption a criminal offence?

"Corruption is a collective term and does not appear as such in the Dutch Penal Code. Bribery, on the other hand, does appear in the Penal Code and is often accompanied by various criminal offences. These offences could include forgery, leaking and falsifying information and documentation and accepting gifts in various forms, such as bribes, kickbacks (which are rewards for awarding a contract or deal) and facilitation payments.”

You receive a report of suspected corruption. What happens next?

“That depends on the exact wording of the report. Usually, I first of all check our own database. Do we have any other reports about the person or legal entity? The logical next step and a way to obtain more context is to ask an ‘Article 17 question’. This allows us to ask reporting bodies for data and information. In other words: more details. For example, any invoices or a bank statement they have so that we can track money flows. Another useful source for the analysis is tax data, as it allows me to check whether an income or assets are justifiable and correspond with the tax information. If, for example, there is a counterparty based abroad, or if I notice money going abroad, I can request a bank statement through the FIU in that country to find out what’s going on. We can also request police data, which naturally provides very valuable information for our analysis. Links to other individuals, for example, can also be very useful.”

Why is it important that corruption is reported?

“Imagine that a police officer leaks information to criminals, or a customs officer presses a button to allow a container of drugs to pass through without being inspected. These things harm society, erode trust in the government and also helps the criminals. That’s far from desirable. Private party corruption leads to unfair competition between businesses and disadvantages people. Someone always ends up suffering, for example through environmental and health standards not being met, lower-quality products, higher prices. It sometimes even facilitates organised crime. Corruption isn’t easy to spot on the street, but we can work with the gatekeepers to recognise certain things within money flows. That’s why these reports are so important.”

Who reports corruption?

“Reports of suspected corruption can come from many different gatekeepers, but there are two reporting groups that stand out. Accountants mainly report private party corruption, while banks report more on public official corruption.”

When do you feel proud?

“When I notice that my work is having an impact, through whatever form of intervention. And I do feel a bit proud when I see my own case featured in the news. That’s how I felt when the news broke that two cardiologists from a hospital in Zwolle were suspected of corruption.[15] They were alleged to have received millions from a supplier of medical devices, in exchange for which this brand was given preferential treatment. There’s also the case of the former director of a Van der Valk hotel, who defrauded COA funds intended for housing asylum seekers.[16] That’s the great thing about our work: you really see societal issues reflected in it and you can help address them. Financial investigation might not sound sexy and it may seem boring, but it’s anything but. The motive behind almost all forms of crime is to make money. And we can expose it. How brilliant is that?!”

**Linda is a pseudonym.*

[15] https://www.hartpatienten.nl/twee-cardiologen-isala-zwolle-verdacht-van-corruptie/

[16] https://www.bd.nl/binnenland/fiod-valt-binnen-bij-van-der-valk-om-opvang-asielzoekers~ac5070a6/?referrer=https%3A%2F%2Fwww.google.com%2F

2.6 Exploitation

Human trafficking, labour exploitation and child abuse are issues that always demand our attention. The financial characteristics vary depending on the form of exploitation, and the money flows involved are becoming increasingly complex.

Human trafficking

Within the issue of human trafficking, FIU-the Netherlands focuses on sexual exploitation and labour exploitation, and particularly cross-border human trafficking involving foreign victims and perpetrators. In addition, in 2025 there was an increasing focus on the issues of child pornography and transnational sexual violence against children.

The financial characteristics vary depending on the form of exploitation, but victims are often forced to hand over all or a large portion of their income, or receive no money at all for their services. The money flows involved are becoming increasingly complex.

Whereas we used to observe bank transfers between suspects within a network, we now observe that there are often more ‘layers’ involved. Examples include transactions to or through a PSP, the use of straw owners, and multiple payments through foreign accounts.

In addition, there were already indications in previous years of a convergence between Eastern European and Latin American networks involved in sexual exploitation, and this became even more apparent in 2025. For example, we observe that some exploiters and facilitators receive payments from both Eastern European and Latin American networks.

Report on online child abuse

The money flows associated with the online sexual abuse and exploitation of children do not remain within national borders. Although these forms of child abuse are difficult to trace, financial intelligence ensures that certain patterns can be identified. Transactions can also serve as additional information and evidence in ongoing investigations, and transactions can be used to identify victims, perpetrators and facilitators. For this reason, reports on this matter are extremely important. Transactions do not merely relate to the abuse as the predicate offence; they also relate to the revenue model and laundering of proceeds from this serious form of organised crime. To raise awareness of this among reporting bodies, we contributed to an international report published by the Financial Action Task Force in 2025. The report outlines recognisable indicators for reporting bodies, such as PSPs, and specifically addresses sexual abuse by live stream and the sexual extortion of children ('sextortion').

Purchasing child pornography with cryptocurrency

Over the past year, the number of reports concerning the purchase of child pornography using cryptocurrency has risen significantly. This is reflected in our weekly analysis: compared to 2024, FIU-the Netherlands is receiving significantly more transactions related to this issue. The reason for this is that the issue has been given higher priority by blockchain analysis tool providers, which themselves also carry out analysis on the blockchain. In collaboration with the Internet Watch Foundation, they flag up crypto addresses linked to child sexual abuse material. These addresses are then given a CSAM (child sexual abuse material) label. Although crypto is often seen by these individuals as an anonymous payment method, the transactions can effectively be traced using blockchain analysis tools. The relevant crypto service providers receive a notification from these blockchain analysis tool providers that their customer has sent cryptocurrency to a crypto address labelled as CSAM. In turn, the crypto service providers report this to FIU-the Netherlands. We shared the insights from our analysis with the Team Combating Child Pornography and Child Sex Tourism (TBKK), which reinforces the fight against child abuse.
To make better use of reports related to this issue within our analysis, technical solutions have been implemented to increase the efficiency of the work process. This created more scope for substantive analysis and enabled us to share more information with the investigation teams.

Transnational sexual violence against children

When individuals abuse children abroad, we refer to this as transnational sexual violence. This also includes the abuse of children abroad by webcam. Thanks to the high priority that various partners in the chain attach to this phenomenon, close collaboration has developed with both investigative services and reporting bodies. This collaboration is characterised by regular coordination and intensive contact. In the fight against transnational sexual violence against children, exchanging operational data with foreign FIUs constitutes an essential source of information. This data is hugely important for interpreting and analysing financial transactions and gaining information about cross-border money flows.

[17] *https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html*

Labour exploitation and the CCM

In recent years, FIU-the Netherlands has drawn obliged entities' attention to both labour exploitation and the Cash Compensation Model (CCM).[18] As a result, there has been a noticeable increase in the number of reports containing indications of these phenomena. Given that labour exploitation and the CCM are most prevalent in labour-intensive sectors, we also received reports in which both offences were present simultaneously.

Seizures, arrests and convictions

The case files referred by FIU-the Netherlands ultimately resulted in several convictions. For instance, the Amsterdam District Court sentenced a man to two years' imprisonment for operating an escort service in the illegal prostitution sector. The women who were victims of human trafficking came from Morocco, Spain, Costa Rica and Cuba.[19] In other cases, €120,000 and €25,398.60 in overpaid social security benefits were recovered, and the payments have also stopped.

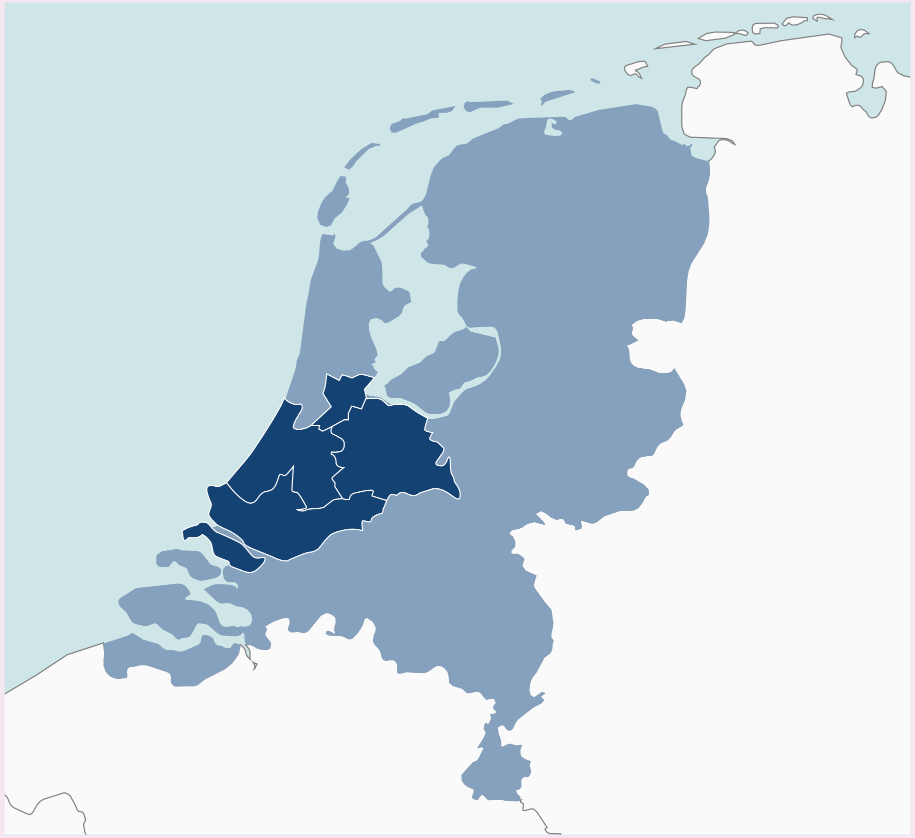
Exploitation figures

189	Files
2,889	Number of suspicious transactions

[18] https://www.fiu-nederland.nl/knowledge_base/cash-compensatie-model/
[19] https://www.at5.nl/artikelen/233675/twee-jaar-cel-voor-man-die-illegale-buitenlandse-sekswerkers-faciliteerde

2.7 Geographical collaboration

Targeted analysis that is aligned with local practice and enables focused, effective interventions. To this end, FIU-the Netherlands regularly works with public partners in the Amsterdam, Rotterdam, Central Netherlands and The Hague regions.



In 2025, as in previous years, FIU-the Netherlands continued to invest heavily in regional collaboration with police units[20] through Regional Information and Expertise Centres (RIECs). These centres are collaborations between the National Police, the OM, local authorities, the Dutch Tax and Customs Administration and the FIOD, and focus on information exchange, analysis and integrated interventions against subversive crime. The RIEC makes a specific budget available for hiring additional capacity for the unit in question. This capacity takes the form of an analyst seconded from the National Police to FIU-the Netherlands. The analyst examines the FIU transaction database[21] through a 'regional lens' and considers the unit's needs and priorities. They select unusual transactions that align with local priorities and tailor analysis accordingly. Implementation remains the full responsibility of the FIU, resulting in customised financial intelligence (intervention recommendations) for the National Police and other investigative partners. This approach results in a better understanding of criminal patterns and concrete leads for investigations and interventions, ranging from criminal investigations to alternative measures. Regions may cover a wider area or a specific city, with the additional capacity enhancing FIU-the Netherlands' effectiveness and delivering local results.

In 2025, FIU-the Netherlands shared 259 case files with its public partners. These files contained 3,267 suspicious transactions in total. The focus of the analysis varies by region; for example, the Rotterdam region focused on issues such as underground banking, while the Hague region concentrated on issues such as healthcare fraud.

[20] This concerns the Rotterdam-Rijnmond, Amsterdam-Amstelland, The Hague and Central Netherlands units.
[21] The database of suspicious transactions can only be accessed by FIU staff. When an RIEC decides to second an employee to the FIU, that employee will work entirely under the authority of the Head of the FIU.

Conviction for money laundering

Geographical collaboration led to numerous positive results in 2025. For instance, the court sentenced a man in the first instance to five months' imprisonment for money laundering after he purchased a luxury sports car using tens of thousands of euros in cash. The car dealership reported this to FIU-the Netherlands. The analysis revealed what appeared to be unexplained wealth, and FIU-the Netherlands subsequently declared the transaction suspicious and transferred the case file to the Financial Intelligence Team within the relevant police unit. The criminal investigation then uncovered several cash deposits amounting to over €100,000 in total. The suspect's legal income was completely out of proportion to this amount, giving rise to suspicion of money laundering.

Investigation into criminal conspiracy

In the Rotterdam region, following an FIU tip-off, the Dienst Regionale Recherche ('Regional Investigation Service', DRR)[23] launched an investigation into a large criminal organisation that was suspected of being involved in drug trafficking. Furthermore, based on FIU tip-offs in Rotterdam, several investigations have been launched into individuals suspected of being involved in criminal activity such as money laundering and drug-related offences.
Furthermore, the case files declared suspicious by FIU-the Netherlands have contributed to the accelerated establishment of suspicion among various investigation departments within the Amsterdam unit. An example of a successful outcome was the seizure of various luxury goods and a large amount of cash following a money laundering investigation.

Seizures during operation days

In addition to regional collaboration with police units through the RIECs, FIU-the Netherlands also works directly with the Zeeland-West-Brabant police unit. Within this collaboration, FIU-the Netherlands' intelligence is jointly translated into initial information for the investigation service. The investigation service thus receives FIU case files that directly lead to new criminal investigations and align with current priorities and available capacity. Every case file declared suspicious within the collaboration is followed up by the investigation service, as this ensures the effectiveness of FIU-the Netherlands' operations. The collaboration also enables information exchange at phenomenon level. As a result, a number of operations took place in 2025 as part of various investigations. On those days, millions of euros' worth of cryptocurrency, narcotics, a firearm, a Rolex watch, cars and real estate were seized. The assets seized were worth over €4 million in total.

Figures on geographical collaboration

394	Files
4,090	Number of suspicious transactions

[22] https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBNHO:2025:1130&showbutton=true&keyword=maserati,witwassen&idx=3
[23] The Regional Investigation Service conducts large-scale investigations into criminal activities such as subversion, criminal networks, fraud, sexual offences and environmental crime.

2.8 Sanctions evasion

In 2025, the European Union imposed new sanctions on Russia due to the war with Ukraine. A number of sanctions were also imposed on Iran. As a result, FIU-the Netherlands' analysis of unusual transactions that might indicate sanctions evasion continued unabated.

FIU-the Netherlands' analysis resulted in 234 case files and 2,494 suspicious transactions with a sanctions element. The analysis related to transactions involving individuals, companies and financial institutions on sanctions lists, as well as goods subject to export restrictions, for example.

Dual-use goods and luxury goods

The sanctioned goods identified in our analysis included dual-use goods. These are goods that can be used for both civilian and military purposes. Examples include computer chips, certain chemical substances and engine blocks. However, the sanctions evasion cluster also identified instances of sanctions evasion through the purchase of luxury goods.

Foreign payment cards and VPN connections

The analysis of unusual transactions indicating sanctions evasion through luxury goods has provided important information about the modus operandi surrounding this phenomenon. It is notable, for instance, that luxury goods are often purchased using debit cards originating from third countries. The purchaser's actual location is frequently concealed using a VPN connection. The analysis also shows that the goods are sold via countries that have not imposed sanctions on Russia.

Recurring methods

In the sanctions evasion case files, we observe a number of recurring methods:

- **U-turn constructions**
  In this scenario, sanctioned goods are exported through one or more third countries. In most cases, these are 'circumvention countries': countries that have not imposed sanctions on Russia, for example. On paper, it appears as though the goods will end up in the third country, while in reality, they are later exported to a country subject to sanctions.

- **Third-party payments** [24]
  A third-party payment involves a supplier delivering goods or services to a customer while another party makes the payment. These payments are legal in themselves, but are sometimes used for criminal purposes. As such, third-party payments frequently feature in sanctions evasion analysis. Front companies routinely process transactions on behalf of sanctioned entities, for example. In addition, dual-use goods are purchased through third-party payments and subsequently exported through roundabout routes to a country subject to sanctions.

- **Layering**
  In the context of sanctions evasion, layering involves deliberately splitting up money flows or financial transactions and devising complex structures to conceal the fact that sanctions are being evaded. The origin and destination of the funds and parties involved can be concealed by using multiple 'layers' of, for example, intermediaries, shell companies, legal entities and international transactions.

The methods of evading sanctions as described in the 2023 and 2024 annual reviews remain relevant. One example is a system where companies appear to play an informal role as financial intermediaries. In 2025, further investigations were carried out into this system.

Collaborations

As in previous years, in 2025 FIU-the Netherlands collaborated on the issue of sanctions evasion internationally, on both an operational and strategic level. At national level, the FIOD was the main partner, and FIU-the Netherlands collaborated with partners within the Samenwerkingsplatform Sancties ('Sanctions Cooperation Platform', SPS).

Figures on sanctions

234 Files

2,494 Number of suspicious transactions

[24] https://www.fiu-nederland.nl/knowledge_base/derdenbetalingen-risico-voor-witwassen-terrorismefinanciering-en-sanctieontwijking

2.9 *Terrorist financing*

In 2025, transactions related to terrorist financing also remained a key focus of our attention. We investigated modus operandi, observed how transport companies were being exploited and identified key figures operating as underground bankers and using cryptocurrency for the benefit of terrorist organisations.

In 2025, 272 case files containing suspected cases of terrorist financing were shared with investigative authorities and intelligence services. Quantitatively, there was a continued trend in case files relating to jihadism as well as in case files relating to the far right with a money laundering, terrorist financing or violence element.
In addition, there was an increase in the number of case files linked to violence from anti-institutional circles.
Examples of the payment methods that emerged in these investigations include the use of non-profit organisations,[25] 'trade-based' terrorist financing, third-party payments,[26] the movement of cash and payments in virtual currencies.

Virtual currencies and underground bankers

Focusing on the latter, our investigations show that terrorist financiers are not switching entirely to new methods, but are integrating virtual currencies into financing methods that have been in use for some time. We observed the following things happening:

1. The transfer of funds that were collected under false pretences to a crypto exchange; a platform where you can buy and trade cryptocurrency.
2. The use of crypto exchanges by individuals for whom there are strong indications that they are involved in underground banking.
3. The transfer of virtual currencies to wallets that appear to be under the control of terrorist organisations.

[25] https://www.fiu-nederland.nl/knowledge_base/derdenbetalingen-risico-voor-witwassen-terrorismefinanciering-en-sanctieontwijking
[26] https://www.fiu-nederland.nl/knowledge_base/terrorismefinanciering-via-non-profit-organisaties

In 2025, there was also a focus on the funding of Hezbollah and Hamas. Analysis of Hamas' financing resulted in indications that Hamas uses cryptocurrency. Our own analysis identified several key figures acting as underground bankers, collecting funds and subsequently converting them into cryptocurrency. There are also indications that various terrorist groups use the same key figures and their services. Although these services are partly provided outside of the scope of the Wwft, this does not mean that regulated financial service providers are not utilised. Financial intelligence on these matters can therefore be provided to investigative partners and intelligence services.

Jihadism

Jihadist terrorism is cited by the National Coordinator for Security and Counterterrorism (NCTV) as the greatest terrorist threat. In the past, FIU-the Netherlands received many reports relating to jihadist activities and jihadists operating in Syria. The link with the Netherlands in these reports was twofold; on the one hand, due to the involvement of Dutch natural and legal persons in transactions to and from the region, and on the other hand, due to the involvement of obliged entities active in the Netherlands.
International developments and the activities of globally operating terrorist groups have a direct impact on the fight against terrorist financing and FIU-the Netherlands' activities in this area.
The fall of the Assad regime in Syria in December 2024 and the establishment of a transitional government have meant that Syria is no longer the global stronghold of jihadist terrorism.
Reports relating to jihadist individuals and groups in Syria had been declining for some time, and by 2025, were virtually non-existent.
However, this does not mean that jihadism has disappeared. In recent years, the

activities of internationally operating jihadists have shifted to Central Asia and various parts of the African continent. Jihadist activity has increased particularly in the southern Sahel region and East Africa, where both Islamic State (IS) and Al-Qaeda (AQ) are active through multiple affiliated groups and splinter factions. This shift is still reflected to a limited extent in terrorist financing reports. The only exception to this are transactions linked to Al-Shabaab, an AQ affiliate in Somalia that has been active for almost 20 years and has featured in financial transactions and reports for just as long.
Due to the increase in jihadist activities in Africa and the fact that jihadist terrorism is consistently cited by the NCTV as the greatest terrorist threat, FIU-the Netherlands organised a knowledge session in early September for reporting bodies and partners in the chain, in order to draw greater attention to terrorist financing in Africa. Experts from Europol, FIU Nigeria and an internationally renowned academic in the field of terrorism and terrorist financing discussed recent developments in this area. Developments in Africa also featured high on the agenda in various international collaborations, including the Egmont Group and the FATF. Throughout 2025, FIU staff participated in various working groups focusing on this theme.

Transport companies misused

Our analysis from the previous annual review, which showed that 'cash compensation structures' and transport companies were being used to finance terrorist groups, was reinforced this year. We also observed examples of high-risk goods such as weapons and drone parts being purchased through CCM networks.

Social media use

In 2025, a number of cases also examined the risks of terrorist financing through social media. Social media platforms were found to be used for spreading radical ideology and collecting donations. A major risk identified in this analysis is the fact that the final destination of funds sent to social media platforms is unknown.

Terrorist financing figures

272 Files

2,505 Number of suspicious transactions

2.10 Fintell Alliance

Within the Fintell Alliance, analysts from Rabobank, ABN AMRO, ING Bank, Knab, de Volksbank/ASN Bank, Triodos Bank and FIU-the Netherlands work together in a single location. They focus on identifying, analysing, investigating and addressing vulnerabilities in the financial system that arise from or are linked to criminal offences. This collaboration takes place within the context of the participating parties' Wwft obligations and powers.

The topics that dominated Fintell Alliance investigations are: criminal networks and facilitators, underground banking, criminal third-party payments and VAT fraud. The Fintell Alliance also focuses on terrorist financing. The focus of these investigations was on identifying modus operandi and enhancing knowledge. One major analysis concerned Dutch wholesalers importing goods from the Middle East. The case exposed individuals with links to terrorist organisations, as well as to underground banking and narcotics (see the interview at the end of this chapter). In several networks analysed by the Fintell Alliance in 2025, we observed that terrorist financing and other forms of crime appeared to go hand in hand.

Signs of misuse of legal entities

FIU-the Netherlands already drew attention to the misuse of legal entities back in 2023 and 2024, and it is something we encountered again on a large scale in the Fintell Alliance's network analysis in 2025. Large numbers of companies appear to be set up solely by facilitators to commit various forms of crime, such as VAT fraud and money laundering through CCM schemes. FIU-the Netherlands issued a risk alert on this matter to the Ministries of Justice and Security and Finance in order to further highlight the urgency of this problem.

Civil-law notaries play a crucial role in the incorporation of legal entities and the transfer of shares. When analysing the networks of malicious legal entities, particular attention was therefore paid to reports from civil-law notaries. In 2025, FIU-the Netherlands analysed several reports from civil-law notaries and other reporting groups concerning the incorporation of private limited companies and share transactions. The findings of this analysis prompted the Royal Dutch Association of Civil-law Notaries (KNB), alongside the Financial Supervision Office and FIU-the Netherlands, to publish an article on recognising fraudulent incorporations and share transactions.[27] Patterns emerged, such as the use of straw owners, short-lived companies in a variety of sectors and businesses with implausible registered addresses. FIU-the Netherlands also observed that shell companies were regularly set up through online platforms, with intermediaries acting as an additional link between the actual client and the civil-law notary. It is worth noting that attempts at fraudulent incorporation often do not stop at a rejected transaction: case files that are rejected by one civil-law notary are regularly found to be carried out elsewhere. This practice of so-called 'notary shopping' also came to light in a joint project involving the OM, the Financial Supervision Office, the National Police and various banks.[28]

Fintell Alliance figures

373	Files
3,231	Number of suspicious transactions

[27] *This article is only available to civil-law notaries on NotarisNet, an internal online platform for the notarial profession.*
[28] *https://www.bureauft.nl/nieuws/pilot-rotterdam-uitdagingen-notaris-bij-poortwachtersrol/*

Interview

We've moved from incident to insight

As part of the Fintell Alliance (FA), FIU-the Netherlands works on joint financial analysis along six major banks active in the Netherlands. Coordinator Benny explains what this public-private collaboration achieved in 2025.

"Together we see more. That's exactly the idea behind the Fintell Alliance," says Benny. Since 2019, he has coordinated this collaboration, which comprises 14 FIU employees and 40 bank analysts who have been specially vetted for this purpose. He continues, "The added value of public-private partnership is evident in all of the analysis. Together, we expose criminal networks based on money flows and identify modus operandi much more efficiently. Everyone's knowledge base grows, and banks use this information for prevention and detection. FIU-the Netherlands can also use the information gained from the Fintell Alliance to inform other reporting groups and supply chain partners and to counter vulnerabilities within the financial system."

Acceleration through queries

If you ask him what he is most proud of in terms of what was achieved within the FA in 2025, he highlights this: the acceleration. "Together, we're succeeding in gaining valuable information about criminal systems. We use that information to provide our investigative partners with excellent opportunities for intervention, and we also explore alternative interventions and barriers. A very important development that began in 2025 is that we're now moving from 'incident to insight' more quickly. Where large-scale issues were suspected, countless cases used to be analysed, which was very time consuming. Nowadays, we build smart search queries based on red flags and modus operandi, which we run against banking data and FIU data. In doing this, we accelerate the process of finding out whether the problem is limited to the case at hand, or whether it's much larger. This method is still in the trial-and-error phase, but it does have enormous potential."

Criminal third-party payments

An example of this thematic approach to modus operandi is criminal third-party payments (see box). Benny explains: “In 2025, we carried out extensive analysis of third-party payments, also in collaboration with the French FIU. The analysis looked for patterns and red flags, which subsequently helped us identify more cases that met the same criteria. All of this helps us gain an understanding of the nature and scale of this kind of money laundering method.”

It appears that Dutch businesses frequently accept third-party payments. Regarding the scale, Benny says: “In one analysis of third-party payments to Dutch companies, we flagged up 2,000 transactions as suspicious, with a value totalling €300 million. In the analysis, we came across quite a few businesses where a significant proportion of their turnover consisted of third-party payments. This poses a major risk, as these businesses sometimes unwittingly become part of a money laundering scheme.”

For example, the analysts identified a Dutch company that received money from several hundred third-party payers from many different European countries. Incidentally, the Netherlands is not merely a recipient of third-party funds; there are also numerous Dutch companies that make payments to parties in other EU countries without any goods or services being provided in return.

Interconnected systems

In its analysis of various phenomena, the FA observes that these phenomena often do not stand alone but form part of a larger criminal system. For several years now, the FA has been investigating the Cash Compensation Model, and third-party payments feature very frequently in these investigations. Benny says, “It’s great that we’re now starting to see the connections. Now that we’ve got the CCM within our scope, we also understand how third-party payments work and how criminals use them to launder money.”

Another phenomenon linked to this is VAT fraud. There are entire networks of third-party payers for which VAT fraud appears to form an integral part of their revenue model. Benny: “CCM, third-party payments, underground banking and VAT fraud are all interlinked. By properly understanding how these criminal systems work, we can also put better barriers in place to combat this.”

Investigative interventions

Financial intelligence leads to investigative interventions and prevention products. “Because we want to prevent our financial system from being abused at the outset, prevention is just as important,” says Benny. For that reason, work began in 2025 on developing a barrier model. “We look at the steps someone has to take in order to make a third-party payment, so that we can then throw up barriers at various points in the process to prevent this criminal payment method. The barriers can be placed within various organisations, such as within the professional accountants’ association. They can ensure that accountants impose certain requirements on their clients when drawing up commercial contracts. Agreements can be made in this contract regarding transparent payments. If clients (often the recipients of third-party payments) do not comply with these agreements, it becomes more difficult to obtain the accountant’s approval.

At each stage, we also examine which facilitators and opportunities enable the phenomenon and which indicators may point to criminal third-party payments. We are continuing our analysis in this area in 2026 in order to gain an even more comprehensive understanding of the issue.”

Abuses

Another topic that came up in 2025 was money laundering within the taxi industry, where small businesses are registered as sole traders but still receive over €1 million euros in revenue for journeys made. This is too much turnover for a single driver, and no salary payments are made to other drivers. Instead, there is evidence of criminal payments, and here too, there are third-party payments, involving the purchase of machinery for African entrepreneurs or their export to Africa. All in all, Benny says that these are clear red flags signalling criminal involvement.

The FA's output pays off for everyone involved; the collaboration has certainly proven that. Benny: "In investigations, it leads to effective criminal and alternative interventions. Banks use the information to improve their own processes, and together we enhance our knowledge base. But it all starts with the analysis carried out by our analysts."

What is a third-party payment?

A third-party payment is a payment in which a party with no direct involvement in a transaction or agreement makes the payment on behalf of one of the parties involved. Instead of the purchaser paying the seller directly, the money comes from this third party.

There may be legitimate reasons why the paying party is not the same as the customer, but third-party payments can also be used for money laundering, terrorist financing and circumventing economic sanctions. When the funds are of criminal origin, this is referred to as a criminal third-party payment.

Types of cases

Around half of the analysis carried out by the FA is based on input from FIU-the Netherlands or one of the participating banks. The other half are cases referred by the investigation services. An example is the analysis carried out within the Terrorism Financing Task Force (TFTF). In addition, there is the Serious Crime Task Force (SCTF), which is a collaboration between the FA, the FIOD, the OM and the National Police.

The SCTF focuses on effectively combatting criminal facilitators within serious and organised crime. Based on intelligence from the investigation service, FIU-the Netherlands and the banks identify the facilitators' money flows and networks. The investigation team then immediately sets to work on the leads obtained. There is an emphasis here on opportunities for intervention by the investigation team, as well as the learning effect. This analysis also results in new information about criminal systems, and in this way, weaknesses in the financial system are exposed and alternative interventions and barriers are explored.

naar alternatieve interventies en barrières.

2.11 Fraud

Fraud is a widespread, persistent phenomenon that undermines the integrity of the financial system and affects society in various ways. Unlike the thematic clusters, this topic is not a separate theme within FIU-the Netherlands' working method, but plays a role in virtually all of our analysis.

Fraud takes various forms and occurs across a wide range of sectors. It often forms the underlying motive or context of unusual financial transactions. This chapter devotes separate attention to fraud, not as a standalone theme, but as a common denominator running through the work of FIU-the Netherlands. In 2025, FIU-the Netherlands flagged up 17,000 transactions as suspicious where a link to fraud emerged from the transaction or analysis. Behind these transactions, there are thousands of victims, misused services and criminals who use the financial infrastructure to secure their proceeds.
Fraud is not a standalone offence; it is always part of other criminal activities. We observe schemes in which:

- healthcare fraud is combined with money laundering;
- third-party payments are combined with VAT fraud;
- underground banking and online scams are used to channel money flows towards organised crime.

For FIU-the Netherlands, this means that we do not just look at individual transactions, but primarily at the patterns: which modus operandi recur, which sectors are affected which what types of legal entities and intermediaries play a role?
The following sections examine the key trends from 2025, the sectors and target groups affected and the money laundering methods associated with fraud. We also demonstrate how collaboration with obliged entities and supply chain partners helps us act more swiftly, moving from incident to insight and from insight to intervention.

Investment fraud: an urgent problem

In 2025, FIU-the Netherlands made a substantive contribution to the AFM report entitled 'From pyramid to iceberg: the hidden scale of investment fraud in the Netherlands', in the form of a strategic sub-analysis based on suspicious transactions involving an element of fraud.[29] Our analysis showed how the proceeds of investment fraud are channelled through the financial system, for example through foreign accounts, crypto transactions and accounts held in the names of straw owners. In this way, the FIU data complements the picture provided by supervisory and victim figures and offers information about the organised, more professional layers of investment fraud that are otherwise difficult to trace.

The AFM investigation confirms that the recorded losses represent only the tip of the iceberg: while the National Police and supervisory authorities observe around €75 million per year in reported losses, the AFM estimates the actual losses at approximately €750 million per year. The FIU reports support this picture of a much larger, largely invisible iceberg beneath the surface. The reports show that investment fraud is not a marginal phenomenon, but an urgent and growing problem that is undermining confidence in financial markets. By analysing transactions relating to investment fraud, FIU-the Netherlands can help partners in the chain to take targeted action against both the providers and the underlying money flows.

Mortgage fraud: links to criminal networks

Fraud is not limited to investment products; the housing market is also affected. While investment fraud siphons off consumers' savings, mortgage fraud undermines both the financial sector and access to affordable, fair housing in the Netherlands.

Our analysis shows that mortgage fraud is often organised in nature and intertwined with other criminal activities. Properties are financed using forged documents and then used for criminal purposes, such as housing cannabis farms, using homes as brothels or housing migrant workers in exploitative situations. This not only causes nuisance and insecurity for local residents; seemingly legitimate real estate purchases arise which, in reality, form part of serious criminal activity. This means that mortgage fraud should not be regarded as an isolated offence, but as part of broader money laundering and subversion structures.

A recurring element in our analysis is so-called 'facilitators'. These are intermediaries who oversee mortgage applications, ensure that false documents are included in applications and work towards securing mortgage approval. These facilitators are often invisible in the formal documents and their names do not appear in the files, even though they play a crucial role in enabling fraud. The analysis also revealed that there was still room for improvement in this area regarding how unusual transactions are reported: a better system of recording who plays which role and reporting transactions and signals in such a way that key figures are identified more quickly.

Based on these findings, proposals have been made to enable institutions to report these cases more effectively, for example by developing new guidance for reporting bodies on how to identify and report attempted mortgage fraud; something that currently happens very rarely.

The analysis on this theme has been passed on to the investigation services so that targeted investigations can be conducted into the networks involved.

In addition, a project on mortgage fraud was carried out within the Financial Expertise Centre (FEC). This was a collaboration involving DNB, the AFM, the Dutch Tax and Customs Administration, the OM, the National Police and FIU-the Netherlands that has led to various recommendations. There is now a focus on greater collaboration between stakeholders in the chain.

[29] https://www.afm.nl/nl-nl/sector/actueel/2025/dec/pb-beleggingsfraude

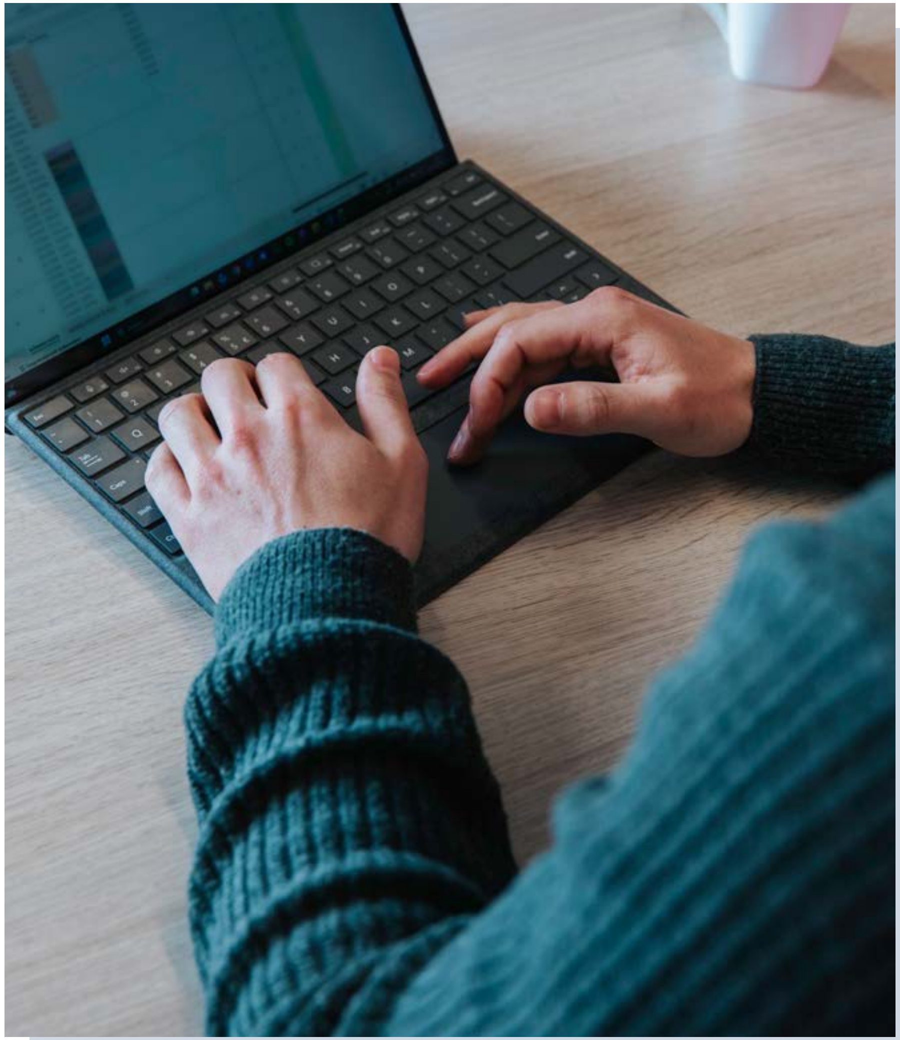
Real estate fraud: a major money laundering risk

An issue closely linked to mortgage fraud is real estate fraud. In our 2024 annual review, we noted that real estate is one of the greatest money laundering risks in the Netherlands. This is also evident from the National Risk Assessment on money laundering and the FATF report on the Netherlands. Tactical analysis conducted by FIU-the Netherlands corroborates the picture emerging from these risk assessments. The issue is particularly relevant to society, as criminals are withholding housing from the market, exacerbating shortages and causing unfair competition within the housing market. In 2025, FIU-the Netherlands conducted an extensive strategic review on the issue of real estate crime. The review provided a broad overview of modus operandi, offering a greater insight into how criminals exploit loopholes in the legislation and deliberately mislead financial institutions.

- **Insight 1:** Malicious speculation and exploitation
  Based on our analysis, a distinction can be made between the ways in which real estate can be misused: malicious speculation and exploitation. Malicious speculation revolves around real estate as a money-laundering vehicle, such as in a fraudulent ABC transaction involving artificial price inflation by multiple parties. As FIU-the Netherlands highlighted back in 2024, malicious exploitation uses real estate for criminal activities such as cannabis farms, drug labs, housing illegal immigrants and criminal gatherings. These forms often overlap, which makes it difficult to distinguish between them. Illegal and legal activities can go hand in hand, creating some semblance of legitimacy.

- **Insight 2:** Financing and purchase
  Our analysis reveals various methods of real estate financing that may involve malicious speculation:
  - unusual loan structures, such as financing by high net worth individuals, buy-to-let and crowdfunding;
  - organised mortgage fraud, where intermediaries and facilitators facilitate large-scale fraud;
  - fictitious arrangements involving cash for purchase, conversion or renovation, often of unknown or illegal origin. In such cases, offshore structures and other opaque foreign financing arrangements, such as foreign bank accounts, are sometimes used to conceal the origins of funds;
  - split ownership rights, where ownership rights are split or master clauses are used to keep the actual owner or user of the real estate out of the picture. Specific legal entities may be used for this purpose, such as partnerships, trust management companies, limited partnerships and foreign entities.

Another striking feature is the link to mortgage fraud, as described above. The analysis shows that it is often committed in an organised manner, with intermediaries and parties assisting with financing applications playing a key role. These professional facilitators actively assist in committing large-scale mortgage fraud.



VAT fraud: unfair competition

Another form of fraud that we encounter systematically in our analysis of money laundering and terrorist financing is VAT fraud. By VAT fraud, we mean the deliberate submission of incorrect VAT returns in domestic business-to-business transactions relating to goods and services. Our 2025 analysis shows that this is a widespread problem. VAT fraud results in significant tax losses, laundering criminal cash and unfair competition for bona fide businesses.
The VAT reporting requirements for domestic commercial transactions are minimal. A tax return does not clearly indicate which supplier is being paid, thereby creating the right to deduct input tax. Current policy measures make it virtually impossible for the Dutch Tax and Customs Administration to identify and take enforcement action against this type of fraud in a timely manner. In fact, it is only through a combination of analysing unusual transactions and tax data that these instances of fraud come to light. That is why, in 2025, FIU-the Netherlands asked the partners in the chain to pay greater attention to large-scale VAT fraud. We also shared our concerns about this widespread form of fraud with the relevant government ministries.

In many cases, in addition to VAT fraud and money laundering, there is also evidence of fraud involving corporation tax, income tax and payroll taxes. Moreover, this modus operandi is frequently encountered within CCM structures where criminal cash is converted into bank transfers through false invoices.

Payment fraud

Payment fraud, which can take the form of bank helpdesk fraud, dating fraud or investment fraud, for example, is a problem for all banks. However, FIU-the Netherlands noted that all of the various reporting banks had different reporting methods. At the end of 2024, all reporting bodies within the banking reporting group received instructions on reporting payment fraud. The instructions focused on the standardised reporting of common types of fraud in payment transactions and, in particular, the laundering of those fraudulently obtained funds. Harmonising the data on these types of fraud is important as it enables better, faster analysis.
During 2025, FIU-the Netherlands found that consistently reporting scams and bank fraud was more complicated than anticipated. Providing feedback to institutions on the data quality of fraud reports required more resources than expected. As a result, the focus in 2025 was more on feedback than on analysis, and the latter is now on the agenda for 2026. The analysis and guidance are being extended to other reporting groups.

In 2025, we developed a dashboard for reports from banks concerning payment fraud that were already being submitted to us correctly. The most common form of payment fraud reported was dating fraud, followed by investment fraud and scams through sales sites such as Marktplaats and fake websites. Looking at the value of the unusual transactions, investment fraud is clearly in first place, with an UTR value of €118 million. Bank helpdesk scams come in second place, with an UTR value of over €28.6 million.

Other forms of fraud

Other forms of fraud that featured in our 2025 analysis include dividend fraud. Related to this, we are investigating the misuse of legal entities, turbo liquidations and bankruptcy fraud. Legal entities are being dissolved, leaving creditors with unpaid bills. In other cases, proceeds are being realised while minimising tax liability.
Although the focus of our 2024 analysis was on fraud involving the Temporary Employment Bridging Measure for Sustained Employment (NOW), we continued to handle and close case files in 2025. The aim of applying for NOW subsidies during the coronavirus pandemic was to enable businesses to continue paying staff costs despite falls in turnover. Their use was to be checked retrospectively. FIU-the Netherlands found that some business owners saw opportunities to use the funds for improper purposes; it was effectively a cheap loan for their own business. There were also business owners who, strictly speaking, were not entitled to the funds and used them for improper purposes. Examples include granting loans to third parties, purchasing real estate and buying expensive goods. Following our findings, the Netherlands Labour Authority is currently overseeing several ongoing criminal investigations. We also focused on the misuse of other subsidies such as fraud involving the highly skilled migrant scheme.

Chapter 3:

Relevant developments and projects

FIU-the Netherlands works closely with public and private partners at both national and international level. The aim is always to safeguarding the integrity of the financial system. This chapter sets out the relevant developments and projects.

3.1 International collaboration

In 2025, FIU-the Netherlands made an active contribution to the Egmont Group, which is a collaboration of 181 FIUs across the globe. At policy level, the Netherlands, alongside Canada, played a leading role in the development of the new Support and Compliance Process within the Egmont Group. This procedure represents a significant step forward in safeguarding the quality and integrity of the international FIU network. The procedure provides a structured framework to guide and support FIUs as much as possible that do not yet meet the membership requirements, so that they can eventually become members. At the same time, the procedure allows for appropriate measures to be taken against FIUs within the Egmont Group in serious cases, for example where there is a risk of detriment.

Furthermore, the Egmont Group recognised the importance of FIU independence as a prerequisite for an effective national anti-money laundering and counter-terrorist financing regime. FIU-the Netherlands made a significant contribution to the approved proposal, in which the conditions for independence have been elevated to a formal standard for all members. This reflects our joint commitment to safeguarding the integrity and effectiveness of the global FIU network.

A key joint achievement of the Policy and Procedures Working Group (PPWG), chaired by FIU-the Netherlands, and the Information Exchange Working Group (IEWG), in which FIU-the Netherlands serves as vice chair, is the revision of the Principles for Information Exchange. These principles constitute the international standards for information exchange between FIUs. The revision marks an important step towards even closer and more effective collaboration within the global FIU network.

During the preparation of the new European package, staff from FIU-the Netherlands also participated in various international working groups, for example in the ‘Contents and Formats of STRs and TRs’ (Suspicious Transaction Reports and Transaction Reports) working group. The focus here is on the technical implementation of Article 69 of the Anti-Money Laundering Regulation (AMLR) concerning the reporting obligation. The working group focuses on the standardised specification of the content and format of suspicious transaction reports within Europe.

3.2 National collaboration

In 2025, FIU-the Netherlands continued to focus on strategic collaboration within the chain. We maintain intensive, structured contact with public and private partners including supervisory authorities, obliged entities and investigative partners. Through collaborations such as the Financial Expertise Centre (FEC), the Infobox on Criminal and Unexplained Assets (iCOV) and the Strategic Programme on Criminal Money Flows, we pool signals and insights, identify risks and phenomena and provide input for policy development. These collaborations enhance our collective intelligence position and contribute to a coherent, sector-wide approach to money laundering and terrorist financing. On an operational level, we work in close collaboration with national and regional investigative partners on priority areas such as serious organised crime, high tech crime, fraud and corruption. An initiative has also been launched to bring together financial intelligence and criminal intelligence more effectively.

Fintell Alliance

Within the Fintell Alliance, analysts from Rabobank, ABN AMRO, ING, Knab, ASN Bank, Triodos Bank and FIU-the Netherlands work together at a single location. They share expertise and focus on identifying, analysing, investigating and addressing vulnerabilities in the financial system that arise from or are linked to criminal offences. The operational collaboration takes place under the participating parties' Wwft obligations and powers.

Over the past year, this has resulted in the insights described regarding criminal third-party payments, terrorist financing through wholesalers and domestic VAT fraud (see Section 2.10). Within the collaboration, we are constantly seeking to improve our working methods. For example, in 2025, we began working more thematically and we paid extra attention to developing knowledge products. In addition, steps are being taken to move from 'incident to insight' wherever possible; this specific analysis examines whether modus operandi occur more frequently within the financial system. This allows for a better assessment of whether an incident is isolated or part of a larger, systemic problem.

Enhancing the chain of suspicious transactions

In collaboration with the National Police, the OM and the FIOD, FIU-the Netherlands is working to improve the quality and use of transactions declared suspicious within the chain. We are also increasing the understanding of and knowledge about these transactions among partners in the chain. This collaboration was established following investigations conducted by the Netherlands Court of Audit and the Financial Action Task Force (FATF) and primarily focuses on optimising internal and mutual work processes. In 2025, we established that it was necessary to continue this collaboration as the chain and its processes require ongoing attention, particularly in view of the upcoming changes arising from the European AML package.
In 2025, FIU-the Netherlands improved the method of transferring case files containing suspicious transactions (STR case files) to investigative partners. Investigative teams now receive an automatic notification when an STR case file is linked to an ongoing criminal investigation. This enables investigative teams to immediately assess the investigative relevance of related STR case files. Furthermore, through the established workflow, we are gaining an increasingly clear picture of how STR case files are used by investigative services. These insights align with the future obligations under the AML package to share statistics on the follow-up action taken by investigative services on case files that have been declared suspicious.

3.3 *Legislation and regulations*

European Anti-Money Laundering package: preparing for implementation

In 2025, the European Anti-Money Laundering Authority (AMLA) became operational in Frankfurt and began drafting the guidelines and technical standards arising from the regulations (AMLAR and AMLR). This is happening in working groups in which AMLA collaborates with representatives of national supervisory authorities and FIUs. FIU-the Netherlands also participates in various working groups. Furthermore, from 2026 onwards, FIU-the Netherlands will permanently second a staff member to the AMLA.
In the Netherlands, consultation has taken place on the bill implementing the sixth anti-money laundering directive (AMLD6, (EU) 2024/61640): the Implementation Act on the Prevention of Money Laundering and Terrorist Financing (Iwt). This sets out FIU-the Netherlands' principles, new powers and obligations. The key new powers are the monitoring power, the notification power and the suspension power.[30] In addition, the AMLR Regulation, which will come into force at the same time, leads to an amendment of the reporting obligation. The AMLR also offers more opportunities for information exchange and collaboration on analysis.

In preparation for the upcoming changes and at the request of the Ministry of Justice and Security, FIU-the Netherlands has drawn up an implementation assessment. This assessment identifies the impact of the entire AML package on the organisation, people, resources and technology. We concluded that although the AML package is feasible, it will place significant demands on our organisation and the performance of our duties. An internal implementation programme has been launched in order to realise this. In collaboration and coordination with the sector, we are ensuring that FIU-the Netherlands will operate in accordance with EU legislation from 10 July 2027 onwards and will make the most of the opportunities and changes presented by the AML package.

Data Processing by Partnerships Act (WGS)

The Data Processing by Partnerships Act (WGS) came into force at the beginning of 2025. This Act creates a new legal basis for FIU-the Netherlands' participation in the Financial Expertise Centre (FEC) and the Infobox on Criminal and Unexplained Assets (iCOV).

Act on Strengthening the Criminal Law Approach to Subversive Crime II

The Act on Strengthening the Criminal Law Approach to Subversive Crime II has also been adopted. This Act will give FIU-the Netherlands the power to suspend transactions from mid-2026 onwards, in anticipation of the similar power that will arise from the European anti-money laundering package as of 10 July 2027. We are currently making preparations internally and in collaboration with the relevant parties to ensure that this new power can be exercised carefully and effectively in the future.

Sanctions regimes

In 2025, four new EU sanctions packages against Russia came into force. In addition, restrictive measures against Iran were reintroduced in the form of amended EU regulations. Obliged entities such as banks play a key role in the implementation of such measures. For instance, in accordance with sanctions regulations, they have to check whether their customers appear on sanctions lists. Furthermore, under the Wwft, they report unusual transactions to the FIU, for example where there are suspected links to sanctions evasion. The FIU investigates these reports and assesses whether the reports involve suspicious

[30] *Under the Wwft (Article 17a), this power will come into effect as early as July 2026.*

transactions. More information on this is provided in Chapter 2.8. Given the clear overlap between sanctions and the Wwft, the FIU closely monitors any rapid developments. This enables it to establish the impact on the number and nature of reports of unusual transactions and the investigations into them.

International Sanctions Measures Act (Wis)

At national level, work is currently underway to modernise the Sanctions Act 1977, which will eventually result in the International Sanctions Measures Act (Wis). This Act will bring about various changes in the sanctions domain that will have an impact on reporting groups such as civil-law notaries and accountants as well as on our own organisation. For this reason, in 2025, at the request of the Ministry of Justice and Security, we conducted an analysis based on the draft bill of the impact of the Wis on FIU-the Netherlands.

3.4 Technological developments

In 2025, we invested heavily in technological innovation, with the aim of enhancing our operational capabilities. Our main focus was on continuing the digital transition: optimising the provision of information, ensuring a future-proof infrastructure, improving data quality and achieving greater uniformity within European data exchange.

New reporting forms and data quality

Better data quality starts with receiving high-quality reports. Customised reporting forms for each reporting group help to achieve this. This is a development that FIU-the Netherlands was working on for some time, and in 2025, these forms became available to lawyers and legal service providers in the Netherlands and the Caribbean Netherlands. The forms are more user friendly and ensure better data quality in incoming reports.
In 2025, FIU-the Netherlands completed an internal data quality project in goAML, which is the software platform that we use for receiving, analysing and managing reports. The key results were improved data monitoring (verification and enrichment), the addition of secondary sources and the streamlining of the extensive list of transaction types, increasing clarity for reporting bodies. Risks of data issues relating to financial institutions’ accounts have been mitigated through separate labelling and checks on accounts with two or more account holders; safeguards that are now consistently embedded in the system. We also developed a data management app, which serves as a single, central point where such risks are identified and handled in a semi-automated manner. The data quality project not only covered incoming reports; it also covered analysis input and registration by financial investigators.

IUGM chair

At the end of 2025, FIU-the Netherlands was elected chair of goAML's International User Group. This group now comprises 75 FIUs across the globe that use goAML. Representing the interests of all of these countries is both an honour and a significant responsibility. As chair, FIU-the Netherlands intends to focus on establishing regional groups comprising like-minded FIUs from specific geographical regions. For Europe, this will be of great benefit in terms of collaborating with other FIUs from the European Union in preparation for the AML package, which will be technically demanding. This will enable us to harmonise across Europe and maintain a direct line of communication with the UNODC's goAML team in order to implement the necessary technical measures.

3.5 Organisational development

In 2025, FIU-the Netherlands brought the organisation further into line with the staffing level (128.5 FTE) based on previously allocated resources. On 31 December 2025, the operational headcount stood at 114 FTE, excluding 10 FTE of external staff. Growth is particularly evident within the operational support unit, which was set up to enhance operational management tasks.
In considering the organisation's development, we have expressly looked ahead to the new AML legislation and regulations, which will have a significant impact on FIU-the Netherlands from 2026 onwards. With this in mind, we have focused on establishing a solid, future-proof organisational foundation. In addition to increasing the number of FTEs, attention has been paid to further professionalisation processes, management and working methods. Efforts were also made to improve transparency, enhance measurability and deploy capacity and resources more effectively. At the same time, we invested in improving the quality of our analysis and investigations. This enhances the organisation's agility and operational capacity and helps ensure that FIU-the Netherlands can continue to perform its tasks sustainably and to a high standard, even in the face of increasing complexity and changing requirements.
In 2025, the Acting Chief Information Security Officer (CISO) of FIU-the Netherlands further established risk management within the organisation. Awareness sessions on information security were organised, advice was provided on various information security issues, and based on that, appropriate security measures were implemented.

Development of the compliance function

Since the end of 2025, FIU-the Netherlands has had a Compliance Officer. We have begun assessing the current internal processes and associated risks, and we have started carrying out internal audits, which is being further expanded in 2026. The Compliance Officer also advises on the application of the European AI Act within FIU-the Netherlands and is contributing to the implementation of the new European AML package.

Talent development

Finally, FIU-the Netherlands invests systematically in talent development through the talent programme. This offers students valuable practical experience and knowledge development within the FIU, with the aim of attracting new talent. In this context, three dissertations were successfully completed in 2025.

Afterword

As you come to the end of this annual review, here at FIU-the Netherlands we find ourselves preparing for the new European anti-money laundering framework. The introduction of the European package will radically change the way that we collaborate as a sector. It requires us to further prepare our organisation, adapt processes and continue refining our analysis so that we can operate effectively within the new system from day one.

One conviction is central to this transition: we cannot combat money laundering, predicate crime and terrorist financing on our own. It is emphatically a joint task. Obliged entities, supervisory authorities, investigative, intelligence and security services, policymakers and international partners; each makes its own indispensable contribution. Our strength lies in bringing together all of these sources of information and expertise.

This is already happening within the public-private partnership of the Fintell Alliance.
Pooling our intelligence enables us to see the bigger picture. Criminal third-party payments, VAT fraud and the misuse of legal entities are not isolated phenomena but nodes in broader criminal structures. We observe the organised nature of networks, facilitating service providers and various forms of fraud recurring in virtually all of our analysis. This underlines just how intertwined these criminal activities are with the mainstream economy, as well as the significant difference we can make by identifying and sharing signals in good time.

The outcome benefits everyone involved. In investigations, it leads to effective interventions, both criminal and alternative. Reporting bodies use the information gained to improve their own processes, and together, we enhance our knowledge base.

This means that our slogan, ‘Together we see more’, is not just an empty phrase. It is the very essence of how we understand our work. We have access to unique financial intelligence, while our partners possess operational capabilities, supervisory tools and policy leeway. It is only when we connect these worlds that we gain the comprehensive picture needed to effectively disrupt criminal structures. This applies within the Netherlands, and equally so in the European and international collaboration of which FIU-the Netherlands is a part.
As the new Head of FIU-the Netherlands, I see it as my mission to deepen and broaden that collaboration.
This means continuing to invest in trust and knowledge sharing, and also in innovation: better data analysis, smart use of technology and clear feedback to our partners.

I would like to thank all of our partners, both public and private, for their efforts in 2025. Together, your reports, analysis, investigations, supervision and policy decisions form the backbone of our financial system’s integrity.
The challenges will not diminish over the coming years. However, when I reflect on what we have achieved together, I’m confident that we can continue to fulfil our role effectively within the new European framework.
Together we see more, and together we go further.

Lisette Heerze
Acting Head, FIU-the Netherlands

Appendix 1

The figures

Table 7: Number of UTs per reporting group in 2025

Reporting group	2023	2024	2025	Of which subjective
Remote gambling provider	28,775	30,553	9,828	57%
Custodial wallet provider[1]	27,087	116,788	93,814	9%
Accountant	3,195	3,388	3,810	98%
Lawyer	22	24	43	98%
Bank	672,085	534,103	630,461	89%
Tax advisor	0	0	0	N/A
Dutch Tax & Customs Administration	356	338	279	92%
Investment institution	139	125	67	100%
Investment firm	70	168	512	92%
Mediator of purchase/sale[2]	0	0	0	N/A
Life insurance broker	N/A	116	118	95%
Payment service provider	2	0	0	N/A
Payment service provider - PSP	150,075	163,363	210,275	56%
Cryptoasset service provider[1]	1,010,385	1,416,103	1,386,790	11%
Domicile provider	N/A	N/A	8,332	100%
Customs	31	112	126	99%
Electronic money institution	4,193	4,935	5,586	6%
Foreign intelligence	6,158	7,034	22,496	97%
Legal services provider	183,491	191,099	146,545	100%
Trader - Antiques[3]	3	N/A	N/A	N/A
Trader - Gemstones[3]	838	N/A	N/A	N/A
Trader - Other goods[3]	559	N/A	N/A	N/A
Trader - Art objects[3]	207	N/A	N/A	N/A
Trader - Vessels[3]	32	N/A	N/A	N/A

Table continued on the next page.

Table 7: Number of UTs per reporting group in 2025

Reporting group	2023	2024	2025	Of which subjective
Trader - Vehicles[3]	3,316	N/A	N/A	N/A
Institutes for Collective Investment in Securities	2	1	3	100%
Legal service provider	6	6	11	55%
Purchaser/seller of goods[2]	N/A	4,437	3,728	39%
Purchaser/seller of art[2]	N/A	25	6	0%
Life insurer	15	20	29	100%
Real estate agent	354	155	115	93%
Non-bank - Business consultancy	0	0	4	100%
Non-bank - Credit cards	10,771	421,189	191,008	93%
Non-bank - Interbank markets	22	0	0	N/A
Non-bank - Leasing	26	87	389	99%
Non-bank - Issue of loans	438	422	601	69%
Civil-law notary	1,051	998	1,052	97%
Government - Other	0	0	0	N/A
Pawnshop	197	292	443	12%
Gambling casino	9,781	9,143	10,057	20%
Valuer	2	6	2	100%
Supervisory authority	29	19	27	100%
Trust office	71	39	281	99%
Lessor of safety deposit boxes	76	92	72	100%
Virtual currency exchange service[1]	219,566	578,312	327,826	7%
Exchange institution	741	881	636	49%
Total	**2,334,167**	**3,484,373**	**3,055,362**	**40%**

[1] Due to new regulations under MiCAR, providers of exchange services and digital wallets were required to apply for a CASP licence in order to continue operating as cryptoasset service providers in the Netherlands. A transition scheme was in place in 2025, meaning that some parties were still reporting as custodial wallet or exchange service providers at the start of the year and as CASP licence holders later in the year.
[2] Since 2024, the reporting groups relating to goods have been divided into mediators, purchasers/sellers of goods and purchasers/sellers of art. This change was made in order to ensure compliance with the Wwft.
[3] This reporting group was used in annual reviews prior to 2024. Since 2024, it has been moved to the appropriate reporting group of mediators, purchasers/sellers of goods and purchasers/sellers of art.

Table 8: Number of institutions that reported at least one UT, per reporting group

Reporting group	2023	2024	2025
Remote gambling provider	21	24	27
Custodial wallet provider^1	7	6	8
Accountant	423	450	510
Lawyer	11	17	12
Bank	55	54	52
Tax advisor	98	115	112
Dutch Tax & Customs Administration	15	17	15
Investment institution	12	8	18
Investment firm	N/A	4	6
Mediator of purchase/sale[2]	2	0	0
Life insurance broker	13	11	9
Payment service provider	35	35	36
Payment service provider - PSP	N/A	N/A	8
Cryptoasset service provider[1]	6	11	11
Domicile provider	1	1	1
Customs	11	13	14
Electronic money institution	47	48	52
Foreign intelligence	1	N/A	N/A
Legal service provider	41	N/A	N/A
Trader - Antiques[3]	84	N/A	N/A
Trader - Gemstones[3]	6	N/A	N/A
Trader - Other goods[3]	13	N/A	N/A

Reporting group	2023	2024	2025
Trader - Art objects[3]	555	N/A	N/A
Trader - Vessels[3]	1	1	1
Trader - Vehicles[3]	5	4	8
Purchaser/seller of goods[2]	N/A	605	484
Purchaser/seller of art[2]	N/A	8	2
Life insurer	4	4	4
Real estate agent	73	74	45
Non-bank - Credit cards	0	0	1
Non-bank - Interbank markets	3	3	3
Non-bank - Leasing	1	0	0
Non-bank - Issue of loans	6	4	7
Civil-law notary	20	24	24
Government - Other	320	271	251
Pawnshop	4	4	4
Gambling casino	1	1	1
Valuer	2	3	2
Supervisory authority	4	2	3
Trust office	19	16	16
Lessor of safety deposit boxes	2	1	1
Virtual currency exchange service[1]	30	30	28
Exchange institution	3	2	3
Total	**1.955**	**1.871**	**1.779**

[1] Due to new regulations under MiCAR, providers of exchange services and digital wallets were required to apply for a CASP licence in order to continue operating as cryptoasset service providers in the Netherlands. A transition scheme was in place in 2025, meaning that some parties were still reporting as custodial wallet or exchange service providers at the start of the year and as CASP licence holders later in the year.
[2] Since 2024, the reporting groups relating to goods have been divided into mediators, purchasers/sellers of goods and purchasers/sellers of art. This change was made in order to ensure compliance with the Wwft.
[3] This reporting group was used in annual reviews prior to 2024. Since 2024, it has been moved to the appropriate reporting group of mediators, purchasers/sellers of goods and purchasers/sellers of art.

Table 9: Number of STRs per reporting group

Reporting group	2023	2024	2025
Remote gambling provider	3,560	3,641	1,137
Custodial wallet provider[1]	2,798	3,735	919
Accountant	967	671	558
Lawyer	13	12	33
Bank	122,744	65,391	58,013
Tax advisor	144	118	45
Dutch Tax & Customs Administration	0	1	0
Investment institution	19	27	38
Investment firm	2	2	78
Mediator of purchase/sale[2]	N/A	6	9
Life insurance broker	0	1	0
Payment service provider	17,385	10,733	8,958
Payment service provider - PSP	18,166	15,817	8,744
Cryptoasset service provider[1]	N/A	N/A	90
Domicile provider	7	9	28
Customs	584	277	208
Electronic money institution	109	259	544
Foreign intelligence	351	457	1,345
Legal services provider	0	4	3
Trader - Antiques[3]	0	N/A	N/A
Trader - Gemstones[3]	83	N/A	N/A
Trader - Other goods[3]	40	N/A	N/A

Reporting group	2023	2024	2025
Trader - Art objects[3]	21	N/A	N/A
Trader - Vessels[3]	3	N/A	N/A
Trader - Vehicles[3]	275	N/A	N/A
Purchaser/seller of goods[2]	N/A	364	233
Purchaser/seller of art[2]	N/A	19	0
Life insurer	12	9	11
Real estate agent	29	12	13
Non-bank - Credit cards	1,027	1,659	1,252
Non-bank - Interbank markets	3	0	0
Non-bank - Leasing	14	24	35
Non-bank - Issue of loans	153	211	137
Civil-law notary	374	324	308
Government - Other	1	0	0
Pawnshop	35	40	36
Gambling casino	774	837	415
Valuer	1	4	0
Supervisory authority	32	15	20
Trust office	19	17	193
Lessor of safety deposit boxes	56	65	52
Virtual currency exchange service[1]	10,713	13,568	8,549
Exchange institution	64	79	39
Total	**180,578**	**118,408**	**92,043**

[1] Due to new regulations under MiCAR, providers of exchange services and digital wallets were required to apply for a CASP licence in order to continue operating as cryptoasset service providers in the Netherlands. A transition scheme was in place in 2025, meaning that some parties were still reporting as custodial wallet or exchange service providers at the start of the year and as CASP licence holders later in the year.
[2] Since 2024, the reporting groups relating to goods have been divided into mediators, purchasers/sellers of goods and purchasers/sellers of art. This change was made in order to ensure compliance with the Wwft.
[3] This reporting group was used in annual reviews prior to 2024. Since 2024, it has been moved to the appropriate reporting group of mediators, purchasers/sellers of goods and purchasers/sellers of art.

Table 10: Number of STRs per transaction type

Type of transaction	Number	Share (%)
Non-cash transaction	56,574	61%
Other	16,728	18%
Money transfer	10,823	12%
Cash transaction	7,918	9%
Total	**92,043**	

Table 11: Number and share of executed STRs in 2025*

Amount	Number of transactions	Share of transactions	Amount in €	Share of amount (%)
< €10,000	57,439	66%	78,630,721	1%
€10,000 tot €100,000	23,371	27%	803,441,409	8%
€100,000 tot €1,000,000	5,783	7%	1,620,011,538	16%
€1,000,000 tot €10,000,000	911	1%	2,453,568,347	25%
€10,000,000 tot €100,000,000	108	0%	2,867,233,376	29%
> €100,000,000	11	0%	2,053,984,202	21%
Total	**87,623**		**€ 9,876,869,593**	

** This only relates to executed transactions. Intended transactions have not been factored in.*

Table 12: FIU requests per investigation service

Politie	
Police Unit - Oost-Nederland	78
National Police Unit	70
Police Unit - Rotterdam	65
Police Unit - Amsterdam	54
Police Unit - Midden-Nederland	50
Police Unit - Noord-Nederland	49
Police Unit - Oost-Brabant	47
Police Unit - Den Haag	38
Police Unit - Zeeland West-Brabant	34
Police Unit - Noord-Holland	26
Police Unit - Limburg	21
Total	**532**

Other investigation services	
Fiscal Intelligence and Investigation Service (FIOD)	203
The Royal Netherlands Marechaussee	98
Netherlands Labour Authority	31
Human Environment and Transport Inspectorate	29
The Rijksrecherche	13
Caribbean Netherlands Police Force	10
Netherlands Food and Consumer Product Safety Authority	8
District Public Prosecutor's Office	7
National Office for Serious Fraud, Environmental Crime and Asset Confiscation	7
Health and Youth Care Inspectorate	2
Social Investigation Department	2
National Public Prosecutor's Office	2
Criminal Investigation Cooperation Team	1
Total	**413**

Appendix 2
The Organisation

Tasks and objectives

The statutory task of FIU-the Netherlands is laid down in Article 13 of the Wwft. This concerns the receipt, registration, processing and analysis of unusual transaction data to determine whether this data may be relevant for the prevention and detection of money laundering, underlying offences and terrorist financing. If this is the case, the unusual transactions are declared suspicious and subsequently forwarded to the various special investigation services and intelligence and security services. In addition, FIU-the Netherlands focuses on related tasks, as required by Article 13 of the Wwft. These tasks include providing information to public and private partners and conducting research into developments in money laundering and terrorist financing. In 2025, FIU-the Netherlands had a budget of €17.6 million and a staffing capacity of 128.5 FTEs for this range of tasks. For the 2021-2025 period, the following six strategic objectives were formulated within the scope of our tasks:

- **Information and research.** FIU-the Netherlands will continue to focus on enhancing and broadening its information task. Over the coming period, we will pay specific attention to improving the feedback loop in order to increase the quality of reports. In addition to operational and tactical analysis, we will continue to focus on strategic analysis and proactively share trends and phenomena that are not visible to network partners.

- **Collaboration.** Collaborating with our partners is essential for our work in preventing and combatting money laundering, underlying offences and terrorist financing. We focus on forms of collaboration that enhance our core task in the Netherlands and abroad by taking a leading role and experimenting with new forms of collaboration.

- **Digitalisation.** FIU-the Netherlands embraces and utilises technology for the purposes of smart and effective processing of unusual transactions and continuous development of our analysis. By focusing on data quality and digitisation, we create more capacity for high-quality research and further improve the value of our output. Moreover, automating our processes increases job satisfaction among our employees.

- **Prioritising.** We make conscious decisions about what we do and do not do. In view of the increasing number of unusual transactions, we apply a risk-based approach to our contribution within various collaborations and the available capacity.

- **Putting the FIU on the map.** There is still insufficient awareness of the importance and potential of financial intelligence and the unique role of FIU-the Netherlands. For this reason, we are committed to raising awareness of the value and potential of the Wwft and financial intelligence among stakeholders.

- **Growth and development.** FIU-the Netherlands is growing in every respect, and this places heavy demands on our organisation. That is why we focus specifically on current and future employees' development, harmonising existing processes and developing new working methods.

Working method

As set out in Article 16 of the Wwft, FIU-the Netherlands has been designated as the entity to which unusual transactions have to be reported. Article 1a of the Wwft lists the various reporting groups to which this reporting obligation applies. The unusual transactions that are reported are subsequently analysed in order to establish whether there are sufficient grounds to declare them suspicious. Transactions declared suspicious by the Head of FIU-the Netherlands are shared with the various special investigation, intelligence and security services.

Positioning

Formally, FIU-the Netherlands is part of the legal entity The State of the Netherlands. In terms of management, it is housed within the Dutch National Police as an operationally independent entity. Through delegation of authority, the Head of FIU-the Netherlands has the necessary powers regarding personnel and resources, thereby guaranteeing the organisation's independence and operational autonomy. The policy line runs directly from the Dutch Minister of Justice and Security to the Head of FIU-the Netherlands. The management line runs via the Chief of the Dutch National Police to the Head of FIU-the Netherlands.

Colophon

Publisher: FIU-the Netherlands
PO Box 10638
2501 HP The Hague

Editors: FIU-the Netherlands

www.fiu-nederland.nl/en/