Financial Intelligence Unit -
the Netherlands

Annual review FIU-the Netherlands 2024

Table of contents

Preventing and combating money laundering, predicate offences and terrorist financing. That is the mission of FIU-the Netherlands. Together with national and international public and private partners, we safeguard the integrity of the financial system.
As FIU-the Netherlands we provide excellent financial intelligence, as well as identification of trends and new phenomena. We share these findings with our partners. This is how we jointly contribute towards preventing and investigating crime.

The year *2024*

Thursday 30 May 2024 was a historic day for our whole domain. On this day, the new European anti-money laundering package was adopted. Its goal is to improve the efficacy of the European anti-money laundering approach through harmonization of regulations and monitoring at a European level.

The new European anti-money laundering package consists of two regulations and one directive. The regulations lay down the core obligations of gate keepers (Anti-Money Laundering Regulation, AMLR) and the establishment of a European Anti-Money Laundering Authority (AMLA, as outlined in the AMLA regulation). The sixth European directive (AMLD6) in this package builds upon the previous directive by promoting judicial cooperation between European national authorities. The package will be in force from July 2027.

In contrast to directives, regulations are directly in effect without transposition into national legislation. Having only worked with European directives, this is a new phenomenon for our domain. This means we will soon have to implement three laws: the new implementation act for the prevention of money laundering and terrorist financing (Implementatiewet ter voorkoming van witwassen en financieren terrorisme, Wwft), the Wwft Bonaire, St. Eustatius and Saba (Wwft BES) and the new European AMLR.

The new European package will have a considerable impact on both the private and public sector. While the details are still being finalized, the general trend is clear: we are moving towards more uniformity within Europe, increasing judicial cooperation, tougher penalties, more power for FIUs, and legislation covering an increasing number of sectors. This conveys a clear message from the European legislator: our joint public-private fight against money laundering, predicate offences and terrorist financing remains of pivotal importance.

Our efforts in 2024 underline the necessity of collaboration. In that year, we continued our analysis of the money laundering method called Cash Compensation Model (CCM) together with our partners. As our insights were growing, so did my concerns. CCM encompasses a large-scale, deep-seated

> Our focus on collaboration and risk-based work also delivered valuable results in 2024

abuse of the financial system, where various fraud methods and laundering of criminal money go hand in hand. This is a worrying development, especially, since many of these complex systems involve organised crime and terrorist financing. These problems require more than criminal and administrative law or impeding facilitators. To achieve supported systemic interventions, structural cooperation with all public and private partners is required. As FIU-the Netherlands, we consistently work towards this goal. In 2024, we increasingly focused on prevention by providing information and education. For example, by sharing FIU products about exploitation and misuse of specific benefits with reporting entities.

We also continued our commitment to risk-based work. I am therefore pleased with the publication of the National Risk Assessment Money Laundering and the National Risk Assessment Terrorist Financing in April 2024, which will provide additional guidance for FIU-the Netherlands and our reporting entities.

The combination of collaboration and risk-based work to identify criminal systems, has been centre to many of my conversations with our partners last year. This reinforces my belief that we should hold up our efforts, both as a chain and as FIU-the Netherlands. After all, our focus has continued to deliver valuable results in 2024, as you can read in this year's review.

The first chapter focuses on numbers. Here, you will discover that 2024 brought another increase of unusual transactions. However, interesting undercurrents can be found. In the second chapter, you can read about our growing ability to uncover complex networks. Consequently, we gain a better understanding of the current risks for the integrity of the financial system. Finally, in chapter three we update you on the new European anti-money laundering package, among other things.

I hope you find this review both insightful and enjoyable.

Hennie Verbeek-Kusters
Head of FIU-the Netherlands

Chapter 1

The figures

The ***figures***

In 2024, the number of suspicious transactions (STRs) decreased while the number of unusual transactions (UTs) strongly increased to almost 3.5 million. In this chapter, we interpret these figures and outline the context.

523
incoming requests
from 72 countries

Top 5:
1. Germany
2. Malta
3. Italy
4. Belgium
5. Finland

671
671 outbound requests
to 78 countries

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

118,408
suspicious transactions
of which 86% is based on the subjective indicator

3,484,373
unusual transactions
of which 49% is based on the subjective indicator

860
FIU requests [4]
Top 3:
1. Police
2. FIOD (Fiscal Information and Investigation Service)
3. KMAR (The Royal Netherlands Marechaussee)

Top 3
crime types based on number of cases
1. Money laundering
2. Fraud
3. Illegal drugs

33
Financial Intelligence Reports [3]
(FIR's)

17,527,978,979
euro
linked to suspicious transactions [1]

16,306
case files
on suspicious transactions

2,328
Article 17 requests [2]

1,871
institutions
reported at least one transaction

[1] *This is a decrease of approximately 7.75 billion euros compared to 2023. Fluctuations like this are primarily caused by suspicious transactions with an exceptionally high value. In 2022, 37 STRs had a value higher than one hundred million euros with a total value of more than twenty billion euros. 2023 counted 34 of these STRs with a total value of 14 billion euros, while in 2024 only fifteen of these transactions were reported with a total value of 9.7 billion.*

[2] *Section 17 of the Money Laundering and Terrorist Financing (Prevention) Act (Wwft) empowers FIU-the Netherlands to request data and information from reporting entities. Furthermore, it allows FIU-the Netherlands to access the Banking Information Reference Portal: https://www.justid.nl/producten-en-dienstencatalogus/digitaal-uitwisselen/routeren-informatie/verwijzingsportaal-bankgegevens-vb, which happened 4,434 times in 2024.*

[3] *A Financial Intelligence Report (FIR) is an intelligence product with a broad report on related STRs and the underlying phenomenon. FIRs provide management information for the investigation, intelligence and security services.*

[4] *With an FIU request the investigation services can request FIU-the Netherlands to perform a targeted analysis as part of an ongoing investigation.*

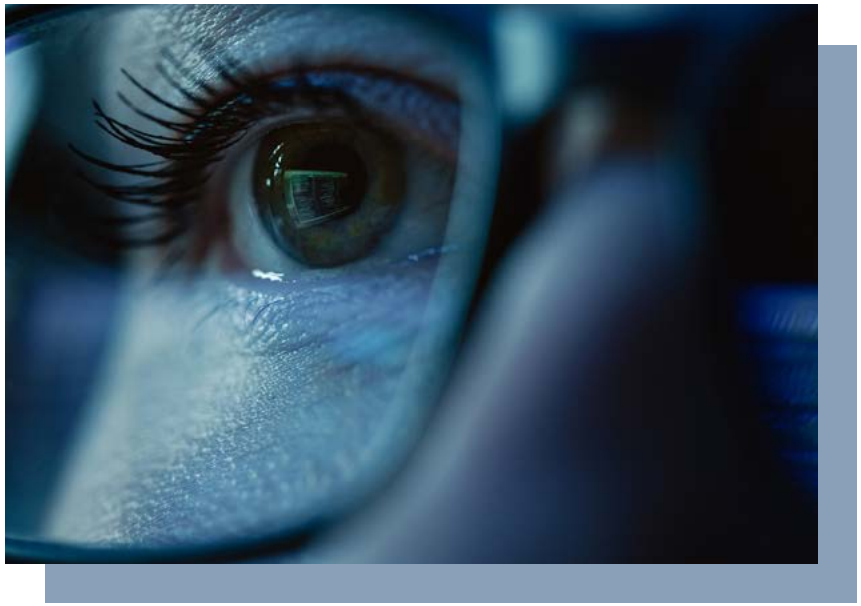
1.1 Objective versus subjective

FIU-the Netherlands received reports of unusual transactions from 30 different reporting groups based on the Money Laundering and Terrorist Financing (Prevention) Act (Wwft). The Wwft Implementation Decree 2018 contains the legal indicators that prescribe the reporting entities when a transaction is unusual. Because these indicators and their differences are important, we introduce them again in this annual review.

- **Objective indicators:** these are threshold-values that must be reported if exceeded. There are multiple objective indicators which can differ between reporting groups. For example, all credit card payments above 15,000 euros must be reported. In general, these reports contain little to no context information. Therefore, in themselves they usually give no cause to initiate or direct a further analysis. However, they provide useful additional information in ongoing investigations, like giving insight into financial positions or certain purchases.

- **Subjective indicators:** in contrast to objective indicators, there is only one subjective indicator that is applicable to all reporting groups. It states that if a gatekeeper suspects money laundering, a relation to crime, or terrorist financing, the transaction must be classified as unusual. The reporting entity explicitly motivates its suspicion in the report. While the quality of these reports varies, they often give FIU-the Netherlands cause to start or give direction to an analysis.

Each reporting group reports on specific indicators in varying degrees. Last year, 98% of accountant reports were based on subjective indicators. In contrast, custodial wallet providers only used subjective indicators in 3% of the reports. This is not surprising, since each reporting group provides different services and therefore different indicators are relevant. Table 6 in the annex lists the indicators for each sector.



1.2 Increases and decreases

In 2024, FIU-the Netherlands received almost 3.5 million reports of unusual transactions. This is a big increase compared to the 2.3 million reports in 2023. The rise stems from three reporting groups. First, the Payment Service Providers (PSPs), companies that enable businesses to accept a wide range of payment methods by acting as an intermediary between the merchant and the customer's bank. The number of unusual transactions from this reporting group showed a 40% increase reaching 1.4 million reports, making them the group with the highest reporting number. Although they are only one out of 29 reporting groups, they are responsible for approximately 40% of all unusual transaction reported in 2024. The predominant cause is the increasing number of transactions that this internationally operating sector processes. These reports were based on subjective indicators in 29% of the cases.

The second reporting group responsible for the rise in reports are the cryptocurrency exchanges. The number of reported unusual transactions from this group more than doubled with a total of 578,312. Since the reporting group became subject to the law, the number of reports has increased each year. This is due to the growth of the crypto market itself, resulting in more institutions that report to us. Furthermore, increases in value play a role, therefore the threshold of objective indicators is exceeded more often. 95% of the unusual transactions from this group was based on objective indicators.
Simultaneously, we observed an increasing professionalisation of licenced operators in their role as gatekeeper. Fulfilling that complex gatekeeper role within institutions takes time, especially within a sector that had no experience with the Wwft. Our meetings with the sector are a fitting example. While in early days, we predominantly met with founders and/or directors, nowadays we confer with (departments of) specialists whose job it is to combat and prevent money laundering or terrorist financing.

The third cause for the high number of reports are the credit card companies. While the group sent 10,771 reports of unusual transactions in 2023, this increased to 421,189 reports in 2024, of which 97% was based on subjective indicators. The cause of this trend is clear: The supervisory authority, the Dutch Central Bank (De Nederlandsche Bank, DNB) instructed these institutions to report all forms of fraud, if necessary, with retroactive effect. Therefore, a large subset of the unusual transactions date from before 2024 but were only reported this year.

The contrast between these three reporting groups and the banks is considerable this year. While the number of reports from credit card providers, PSPs and cryptocurrency exchanges increased drastically, the reports of banking companies decreased significantly. In 2024, banks reported over a hundred thousand fewer unusual transactions than a year earlier. Despite the decrease, banking companies remain in the top three reporting groups with the highest number of reports in 2024.

Reporting group	Number of reports	Based on subjective indicators
Payment Service Providers (PSPs)	1,416,103	29%
Cryptocurrency exchanges	578,312	5%
Bank	534,103	99%
Non-bank – credit cards	421,189	97%

The decrease of bank reports is a distortion caused by one bank in particular. As described in previous annual reviews, one bank used to report individually instead of using compiled reports. For example, if a criminal scams the same person in hundred separate transactions of 1,000 euros, most banks would file one report for 100,000 euros. However, the bank in question would report 100 separate transactions. Both ways of reporting are allowed, but it resulted in a huge difference between banks and skewed data.

In 2024, the aforementioned bank switched to filing compiled reports, reducing its number of unusual transactions from 500,000 to 220,000 reports. It remains the most frequent reporter within its group, but instead of filing 75% of the reports, it now is responsible for approximately 40%. This means that the figures are becoming more uniform. Due to the way of reporting but also due to what is reported. Just as the credit card companies, the DNB reminded institutions in the banking sector that reporting all forms of fraud is obligatory under the Wwft. As a result, several banks started filing more reports, making the numbers more comparable.

1.3 International transactions

A substantial part of the unusual transactions we receive concern international transactions. This can be divided into two categories: international transactions with a sending or receiving party linked to the Netherlands or international transactions that make use of the Dutch financial system but have no further link with the Netherlands.

An example: imagine an Italian webshop contacting a PSP based in the Netherlands to handle its payments. If a German buys something from the webshop, the Dutch PSP facilitates the transaction. The PSP then monitors the transaction according to the Wwft and may conclude it is an unusual transaction. According to current laws and regulations, the Dutch PSP has to report the transaction to FIU-the Netherlands. Consequently, we include the transaction in our analyses, but we also share the information with the FIUs of Italy and Germany.

Within the PSP sector, more than 70% of the 1.4 million unusual transactions in 2024 had no direct link with the Netherlands. In contrast, of all unusual transactions in total only 40% had no sender or receiver linked to the Netherlands. This emphasises the international use of the Dutch financial system.

1.4 Suspicious transactions

Table 1 shows that in 2024, 118,408 suspicious transactions[5] in 16,306 case files were shared with the corresponding investigation, intelligence, and security services in the Netherlands or abroad.

The number of case files originating from own investigations slightly increased in 2024. These files are initiated based on signals, our own insights or requests from abroad. These tend to be more complex analyses, as can be seen from the number of transactions per file. Although this category accounts for only 17% of the files we produce, it contains more than half of all the suspicious transactions of the year.

In the case of FIU requests, case files are opened on request of (special) investigation departments who ask for targeted analyses as part of an ongoing investigation. The 'Match Investigation, Prosecution and Execution' (Match Opsporing, Vervolging en Executie - MOVE) case files contain suspicious transactions specifically related to subjects that are already under investigation. Despite the subjects already being in the picture of investigation services, the additional financial intelligence often provides valuable information for the investigation. For instance, it may reveal that the suspect has further assets that were unknown to the investigation services. Or financial relationships with parties that were not included in the investigation yet. In table 2, the distributions of objective and subjective reports in these workflows are listed.

Table 1: Number of STRs and case files per workflow

Workflow	Number of transactions	Share of transactions (%)	Number of case files	Share of case files (%)
Own investigation	61,410	52%	2,994	17%
- of which based on information requests from foreign FIUs	*2,869*	*2%*	*178*	*1%*
FIU request	3,618	3%	317	2%
Match Investigation, Prosecution and Execution	53,380	45%	12,995	80%
Total	**118,408**		**16,306**	

Table 2: Share of objective/subjective indicators within the STRs

	Objective	Subjective
Workflow	**Share of transactions (%)**	**Share of transactions (%)**
Own investigation	15%	85%
- of which based on information requests from foreign FIUs	9%	91%
FIU request	21%	79%
Match Investigation, Prosecution and Execution	13%	87%
Total	**14%**	**86%**

[5] *As described previously, the FIU-the Netherlands analyses all UTs to determine whether they qualify as suspicious. Since UTs have to be retained for five years according to the Wwft, an STR from 2023 does not necessarily correspond to a UT from 2023. The UT may come from an earlier year*

1.5 Caribbean Netherlands

Table 3 shows 8,596 unusual transactions from 25 reporting entities that have been reported in Caribbean Netherlands this year. This is an increase of 8%, caused by a higher reporting rate of banks, as was also the case in previous years.

Table 4 lists the case files containing analyses connected to Caribbean Netherlands and the number of STRs. The number of file cases remained more or less the same (60 vs. 61), but the number of suspicious transactions in these case files dropped drastically from 728 to 249. Responsible are a few case files from 2024 which were based on few transactions but led to complex and lengthy analyses. Therefore, the value of a file with a limited number of transactions may be as large or larger than a file with many transactions.

Table 3: Number of reporters and transactions per reporting group in the Caribbean Netherlands

Reporting group	Number of reporters	Number of transactions
Bank	5	8,364
Tax advisor	1	12
Customs	1	71
Trader in items of great value and building materials	3	39
Life insurer	1	1
Civil-law notary	3	10
Gambling casino	2	99
Total	**16**	**8,596**

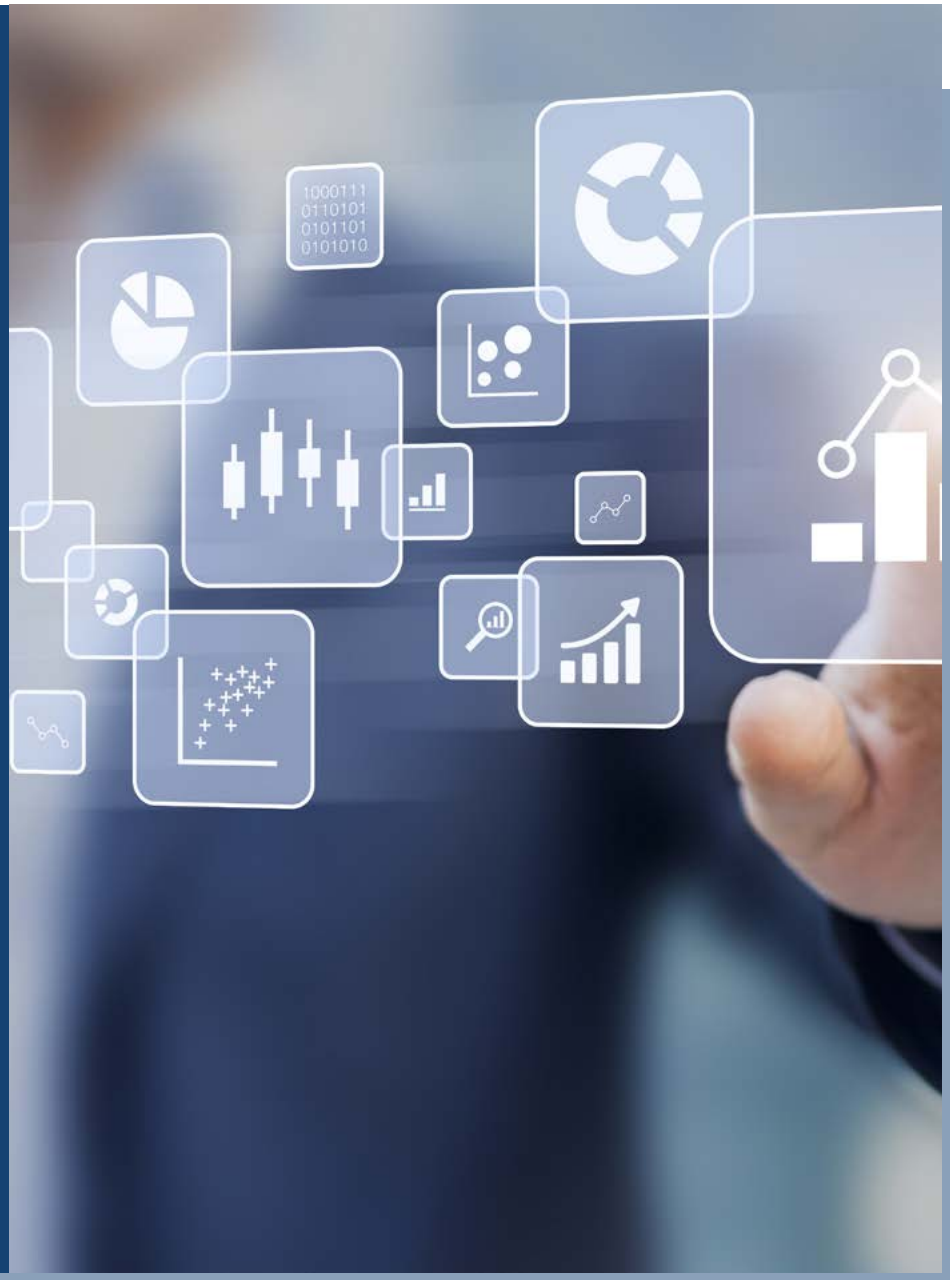
Table 4: Number of STRs and case files in the Caribbean Netherlands

Workflow	Number of transactions	Share of transactions (%)	Number of case files	Share of case files (%)
Own investigation	111	45%	12	20%
FIU request	25	10%	6	10%
Match Investigation, Prosecution and Execution	113	45%	43	70%
Total	**249**		**61**	

Chapter 2

The insights

In this section, we discuss some of the insights that emerged from our analyses. The first section focuses on money laundering and offences that precede it. The second section focuses on terrorist financing.



2.1 Misuse of legal entities

In 2023, we described the deployment of straw owners[6] to set up companies or take over companies via share transactions. Also in 2024, we frequently encountered the phenomenon in our analyses. A worrying development, since there are strong indications that setting up (shell) companies occurs in an organised fashion with the help of professional service providers. Criminal – or in some cases naïve - professional service providers are using their knowledge and expertise to aid criminals in navigating the financial system. From setting up and registering a (shell) company with straw owners, to preparing visits to the notary or Chamber of Commerce's trade register and supervising the process. Or helping to jointly open a business account or certifying real estate contracts.

The misuse of legal entities is not limited to few cases. It is a multifaceted development that seems to be spreading rapidly. From abusing legal entities for money laundering to using legal entities to facilitate criminal processes. For instance, justifying the sourcing of certain raw materials. Europol already mentioned these signals in their Serious Organised Crime Threat Assessment in 2021. According to their report, 80% of criminal networks use 'legal' business structures.[7]

Our analyses show that this is a systemic vulnerability in our financial system. Our previous annual review described a phenomenon called Cash Compensation Model.[8] A money laundering method using subcontracts to exchange criminal cash for non-cash money with sometimes legal origins. In 2024, we built upon our understanding of this method and the first convictions ensued.[9] With each new analyses it became more evident how organised, extended and systemic the misuse of legal entities is. For obfuscating transactions intended for money laundering or terrorist financing, for purchasing resources for criminal purposes, or for committing fiscal, shopping and healthcare fraud.

A recurring observation in our analyses is how fast and easy legal entities are created to open bank accounts or send fake invoices, for example. Or to establish an obscuring set of enterprises, making it extremely difficult to follow financial flows. In 2025, we plan to look further into the subject and assess with our partners in what ways we can intervene. Because, although our understanding is steadily growing, the phenomenon turns out to be hard to tackle by criminal justice alone. Since these networks are deeply rooted in our society, a more extensive strategy is needed.

[6] *Straw owners are people who, on paper, are the owners of bank accounts, companies etc. to keep the real owners out of sight.*

[7] *https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021*

[8] *https://www.fiu-nederland.nl/knowledge_base/cash-compensatie-model/*

[9] *https://www.ad.nl/binnenland/broer-en-zus-leefden-in-luxe-met-spookbedrijf-miljoenen-verdwenen-in-school-villa-en-dure-autos~aeaf2477/*

2.2 Third-party payments

In third-party payments, a supplier delivers goods or services to a customer, while another party makes the payment. There are valid reasons for using this type of arrangement. For example, a customer based in a country without a well-functioning banking system who still wants to pay for goods. However, it has become clear that this type of payment involves considerable risks, because the actual customer and/or the origin of the funds are not transparent. Already in April 2023, investigative journalists from Argos and Platform Investico published an article about the risks of third-party payments.[10] Analyses also showed that malicious parties use this method to launder money on a large scale, circumvent sanctions and, in some cases, finance terrorism. In addition, strong links with underground banking were found.[11] Sometimes the paying and supplying legal entities are fully aware of the risks or deliberately exploit them. However, we also have indications that this is not always the case, which makes it an even greater risk.

Given the nature and scale of these risks, we organised a knowledge session with accountants on third-party payments in 2024. This session highlighted characteristics that may indicate third-party payments, such as transactions that are unusual for the sector and round amounts.[12]

In the Fintell Alliance, FIU-the Netherlands and the participating banks frequently analyse criminal networks. These networks are often involved in large-scale VAT and healthcare fraud, money laundering of criminal cash via, among other things, the Cash Compensation Model, and other criminal activities.

In one of these analyses, we identified a network suspected of large-scale money laundering and fraud. Criminals used a structure of dozens of legal entities with straw owners for these purposes. Various professional money launderers managed the accounts of these legal entities, which received money from more than 150 companies. These companies are active in labour-intensive sectors such as transport, healthcare, construction and infrastructure. FIU-the Netherlands suspects the involvement of cash compensation, whereby millions of euros in cash are laundered every year. Here, criminal cash is sold by professional money launderers to many companies, who in exchange pay a false invoice to the money launderer. There are indications that the received cash is used to pay staff under the table, in full or in part, which provides a tax advantage.

None of the money transferred to the accounts managed by the money launderers was used to pay staff. The money was mainly used to purchase (luxury) vehicles. Often, constructions were involved that appeared to involve tax fraud. Also, large amounts of gold were purchased. FIU-the Netherlands registered many purchases abroad of goods that appeared to be unrelated to the business operations and sectors in the Netherlands. This may indicate third-party payments.

[10] https://www.platform-investico.nl/onderzoeken/meer-dan-honderd-nederlandse-bedrijven-verstrikt-in-witwaszaak

[11] https://www.om.nl/actueel/nieuws/2024/07/24/groothandel-in-parfums-en-cosmetica-schikt-met-om-voor-199.000-euro-vanwege-witwassen

[12] https://www.fiu-nederland.nl/knowledge_base/derdenbetalingen/

This analysis also illustrates how adaptive professional money launderers are. If a VAT number is withdrawn, the corresponding legal entity is quickly and easily replaced by a new one. If the bank closes an account, a new one is available within a short period of time. Significantly, this and other analyses have shown that (large-scale) tax frauds are often involved in these types of networks.

This analysis has been handed over to an investigative service. Additionally, we use our insights for preventive measures at barriers like banks. This way, we try to frustrate the criminal system and thus keep the financial system clean.

2.3 Real estate

Real estate is mentioned in various studies and reports as one of the major money laundering risks in the Netherlands. For example, in the National Risk Assessment Money Laundering[13], the Financial Action Task Force report about the Netherlands[14], the National Risk Assessment Money Laundering and Terorrist Financing BES[15] and the Supranational Risk Assessment, which looks at the situation across Europe.[16]

2.3.1 Real estate and money laundering

Tactical analyses by FIU-the Netherlands confirm the picture painted by these risk assessments, both from the perspective of money laundering and facilitating crime. To illustrate: in one of the cases involving real estate, we gained insight into the real estate portfolio of a criminal who was attempting to launder money through the purchase of properties. Cash deposits of illegally earned money were ultimately used to purchase real estate through a concealment process involving legal entities. As a result, the criminal received legal income from rental payments. We uncovered this method thanks to reports from several gatekeepers, such as notaries, payment service providers and banks. This is a strong example of the power of individual reports from different gatekeepers and the inextricable link between them.

2.3.2 Real estate and foreign legal entities

In the above case, an international legal entity also played a role. This phenomenon frequently recurs in both our analyses and court rulings. To such an extent that in the spring of 2024, FIU-the Netherlands and the Anti Money Laundering Centre (AMLC) established new money laundering typologies on the subject of ‘foreign legal entities and money laundering’. These typologies can be found on the website of FIU-the Netherlands.

2.3.3 Real estate and the criminal process

Other analyses show that real estate is also used to facilitate the criminal process. The purchased properties are for example used to house a cannabis plantation or to facilitate illegal gambling. Or the properties serve as a place for illegal prostitution, where sexual exploitation occurs. Previously, the report 'criminal buildings' by the WODC (Dutch Research and Data Centre) in 2019 already indicated that this is a serious problem.[17] The report states that at the time, approximately fifty thousand properties in the Netherlands were being used for subversive criminal activities. The WODC estimates that approximately 80% of these properties are residential. This means that at the time, no fewer than forty thousand homes in the Netherlands were removed from the legal system and were not available to home seekers.

[13] https://repository.wodc.nl/handle/20.500.12832/3352
[14] https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-netherlands-2022.html
[15] https://repository.wodc.nl/handle/20.500.12832/3087
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:554:FIN
[17] https://repository.wodc.nl/handle/20.500.12832/3027

2.4 Fraud

In 2024, fraud was once again one of the most common types of crime identified in our analyses. This involves both horizontal and vertical fraud. In horizontal fraud, private individuals and/or legal entities victimise each other. In vertical fraud, the government is the victim.

2.4.1 Vertical fraud

An example of vertical fraud is benefit fraud. This involves applying for benefits to which one is not, or only partially, entitled. If the fraud occurs in an organised context, the amounts can run into millions of euros per case.[18] Our analyses show that this type of organised fraud is common, with multiple types of benefits being claimed illegally. It appears to be a criminal business model and therefore poses a significant risk to the integrity of the financial system.

2.4.2 Healthcare fraud

Healthcare fraud is unfortunately a recurring issue that seems to be growing. In 2024, our analyses showed increasing complexity and links to serious crime. One example is the organised misuse of two specific healthcare schemes involving large numbers of legal entities. In December 2024, FIU-the Netherlands sent an FIU Alert to several reporting groups warning them about the risks of these schemes.

We also found links between healthcare fraud and the Cash Compensation Model. An analysis focusing on fraudulent employment agencies in the healthcare sector revealed that large amounts of care funds ended up with foreign legal entities linked to money laundering. Some care was provided, but there were strong indications that care workers were paid in cash under the table. This obviously has many consequences. Because no payroll taxes are paid, legal companies are at an immediate cost disadvantage compared to their

criminal competitors. There are also indications that not all training programmes are up to standard, which may have consequences for the quality of the provided care. Healthcare is not only a victim of fraud in this network, but it is also being abused to launder criminal money and transfer it abroad.

2.4.3 Fiscal fraud

The analysis described above shows how paying staff under the table within the Cash Compensation Model leads to unfair competition and tax fraud, for instance non-payment of income tax. In 2024, FIU-the Netherlands noticed legal entities offering their 'cash compensation services' to hundreds of 'legitimate' companies in the legal world. It therefore appears to be happening on a large scale.

Unfortunately, this form of tax fraud is not the only one. In 2024, analyses also regularly revealed large-scale VAT (carousel) fraud in the Netherlands and other European member states. This was specifically addressed in the project 'cross-border VAT fraud' of the Financial Expertise Centre, in which FIU-the Netherlands participates.

Given the high number and scale of these tax fraud structures, FIU-the Netherlands is concerned about the undermining aspect. A legitimate company that does meet its tax obligations cannot compete with an entrepreneur who wrongfully claims back VAT, pays staff under the table and privately spends untaxed profits.

2.4.4 Horizontal fraud

Unfortunately, in 2024, we again identified many cases of fraud between citizens, for example investment fraud and dating fraud. These forms of fraud have an enormous impact on the victims, and we are trying to gain more insight into these phenomena. In 2024, the DNB (Dutch Central Bank) explicitly informed several institutions that fraud is a predicate offence for money laundering and is therefore subject to the reporting obligation under the Wwft. As described in the first chapter, not all institutions were already handling fraud accordingly. DNB's instruction therefore led to an increase in the number of fraud reports. This is one of the reasons why FIU-the Netherlands sent an FIU Instruction to banks specifically, in December 2024. The instruction described a uniform method for reporting certain types of fraud, to enhance the efficiency of our analyses.

Another example of horizontal fraud is mortgage fraud. One type we encountered last year is fraud involving income data. In these cases, individuals have mortgages that are much higher than their income would allow, because they declare higher salaries to the mortgage lenders. What strikes us, is that often cash is deposited into the account of a legal entity. This money then directly or indirectly ends up in the account of the private individual, who uses it to pay the mortgage. In this sense, the mortgage lender does not suffer any direct damage. Nevertheless, it is a highly undermining form of fraud. Fraud that enables the use of criminal money to buy homes in the competitive housing market and build up seemingly legal assets in real estate.

[18] *https://www.ad.nl/dordrecht/man-zou-illegaal-miljoenen-euros-kinderopvangtoeslag-binnen-hengelen-voor-bulgaren-ik-wilde-hen-helpen~a631f629/*

2.5 Corruption

Corruption is a collective term that does not appear in the Dutch Penal Code, bribery does, however. Bribery often involves multiple acts. These include:

- forgery
- leaking and/or falsifying information or documentation
- accepting gifts such as bribes, kickbacks or facilitation payments

In 2024, our analyses revealed several forms of official and non-official corruption, involving both active and passive bribery. Active bribery relates to the party offering the bribe, while passive bribery relates to the party receiving the bribe. The initiative for bribery does not necessarily always lie with the active party, for passive parties may also initiate it.

Our analyses revealed indications of active bribery by Dutch multinationals in various sectors abroad. One example is a Dutch company that purchased scarce goods from a European supplier. The Dutch company paid substantial invoices to a third party without it being clear what services would be provided in return. Our analyses showed that the beneficiary of the unknown third party had a family relationship with a high-ranking person within the supplier. Therefore, these may have been indirect payments of bribes. Information from another FIU played an important role in this analysis. Files like these are transferred to the Anti-Corruption Centre of the FIOD (Fiscal Information and Investigation Service).

We also completed analyses based on indications of corrupt employees at various government agencies. For example, one analysis revealed a government employee who possibly abused his position by accepting monetary gifts from a private party in exchange for awarding contracts. We transfer files relating to official corruption to the National Criminal Investigation Department.

2.6 Exploitation

There are various forms of exploitation. Below, we highlight a few forms that emerged from our analyses.

2.6.1 Labour exploitation

Labour exploitation refers to serious abuses in working conditions or in the relationship between employer and employee. In 2024, we shared an FIU knowledge update on this subject with reporting entities. With these knowledge updates, we highlight trends and phenomena that emerge from our analyses or from operational partnerships. They provide reporting entities with background information on a particular phenomenon to support them in their gatekeeping role.

2.6.2 Sexual exploitation

In the case of sexual exploitation, sex workers experience unfair and/or unsafe conditions. Sometimes, this is accompanied by deception, physical violence, human trafficking, fraud, threats and/or other crimes to force someone to perform sexual acts. The perpetrator's aim is to gain financial benefit for themselves. This form of exploitation therefore leaves financial traces that may be recognisable for financial institutions.

To raise awareness about this subject and spread knowledge, an FIU alert was shared with reporting entities. The alert contained specific red flags indicating sexual exploitation. The information enables reporting entities to be more alert during the monitoring of transactions. Additionally, we organised knowledge sessions on this subject with various reporting entities.

In 2024, promising results in combating sexual exploitation were also achieved through a so-called Field Lab. In this project, a specific, complex security problem is tackled through integrated, strategic and effective cooperation. For the Field Lab, FIU-the Netherlands collaborated with the municipality of Amsterdam, the Royal Netherlands Marechaussee, the Amsterdam police and the Dutch Public Prosecution Service.

We focused on tackling so-called facilitators. These facilitators exploit vulnerable, unlicensed foreign sex workers by forcing them to hand over very high percentages of their earnings. They also charge absurdly high amounts for advertising, travel, accommodation and/or mediation costs. The facilitators operate in a grey area between human trafficking, human smuggling and violations of local regulations. In addition, they almost never pay taxes, often receive unjustified benefits and use houses for sex work which are therefore removed from the housing market. This is a subversive problem with far-reaching consequences for the victims.

By gathering the knowledge and expertise of all partners in the Field Lab, several facilitators were prosecuted through criminal, administrative and fiscal routes in 2024. As a result, individuals were prosecuted for human smuggling and human trafficking, benefits were reclaimed, rental contracts were terminated, fines were imposed and the municipality of Amsterdam imposed penalties on several individuals.[19]

2.6.3 Child pornography

Child pornography is a form of exploitation, as well. Child pornography is not exclusively a lust-driven crime. For some perpetrators, it is a lucrative business model, making financial intelligence extremely valuable for detecting and combating child pornography. Therefore, FIU-the Netherlands actively investigated the subject in 2024. Our files contributed, among other things, to selection of and giving verbal warnings to 150 persons in the Netherlands as part of early intervention.[20] In addition, we participate in a project of the Financial Action Task Force (FATF) aimed at sextortion[21] and live streaming to increase our shared knowledge and expertise on the subject.

[19] https://www.parool.nl/nederland/man-aangehouden-op-schiphol-op-verdenking-van-mensenhandel-en-seksuele-uitbuiting~bded4848/

[20] https://www.politie.nl/nieuws/2024/november/20/politie-deelt-150-waarschuwingen-uit-tijdens-landelijke-actieweek-bezit-kinderporno.html

[21] *Sextortion is a form of extortion in which the perpetrator uses explicit material (such as nude photos of the victim) to blackmail someone.*

2.7 Sanctions evasion

Sanctions evasion involves transactions that can be linked to entities on the terrorism sanction or EU sanction list. On this topic, FIU-the Netherlands cooperates internationally at multiple levels. At the knowledge level, this resulted in an FIU knowledge update on the illegal purchase of dual-use goods.[22] We also joined forces at the operational level, leading to the inclusion of new entities on a sanctions list, for example.

In 2024, FIU-the Netherlands received various reports about possible evasion of sanctions. In total, there were 226 files and 6,437 suspicious transactions with a sanction component. These files concerned, for instance, transactions in which the beneficiary or beneficiaries were on a sanctions list or contraband. Some of our analyses focused on donations to military fundraisers and on the suspected export of sanctioned goods using a detour. In these analyses, we regularly noticed unusual flows of money and/or goods through neighbours of the sanctioned country.

Another method we encountered involved third-party payments (see also section 2.1.2). In our 2023 annual report, we discussed one case that accounted for a quarter of the suspicious transactions that year. The case provided insight into companies that appear to have taken on an (informal) role as financial intermediary. This system enables large-scale sanctions evasion and money laundering, among other things. In 2024, we also performed analyses on the subject, concerning very large sums. Furthermore, FIU-the Netherlands identified a second, similar system in 2024. In this network, sanctioned entities used front companies to handle their transactions.

2.8 Geographical cooperation

In 2024, FIU-the Netherlands invested heavily in regional partnerships with public partners. Regional cooperation results in targeted, locally valuable analyses and thus in efficient interventions. Cooperating regions may cover a larger area or a specific city. For example, in 2024, 428 files were shared with local public partners in the region Rotterdam. This led to excellent results. Among other things, a drug lab was identified in a densely populated area, where also firearms, cash and luxury goods were seized. In the region of Amsterdam 111 files were shared. These files contributed, among other things, to an investigation into a large-scale mortgage fraud network. This network is believed to be responsible for the criminal purchase of hundreds of homes in the capital.[23]

[22] *https://www.fiu-nederland.nl/knowledge_base/fiu-kennis-update-illegale-aankoop-van-dual-use-goederen/*

[23] *https://fd.nl/samenleving/1522875/crimineel-netwerk-kocht-honderden-woningen-via-listige-hypotheekfraude*

2.9 Terrorist financing

The terrorism threat remained high in 2024, with the National Coordinator for Counterterrorism and Security (NCTV) maintaining threat level 4.[24] This means, there is a real chance of an attack in the Netherlands. The threat comes from multiple angles, including a substantial threat from jihadism and a risk that individuals from the right-wing terrorist movement will resort to violence. Also, violent anti-institutional extremists pose a potential threat. In 2024, FIU-the Netherlands carried out analyses across the entire spectrum.

Within the Counter Terrorist Financing Project, the Egmont group[25] focused specifically on so-called lone actors.[26] The findings from this project were incorporated into FIU-the Netherlands' work processes to identify preparatory acts ahead of time. This includes the financing or purchase of the necessary means for an attack. One of the main recommendations, for example, was to gain a better understanding of the purchase of firearms. In 2024, thirteen files were compiled involving a combination of firearm-related cases and terrorist financing. A striking feature was the high percentage of individuals who belonged to or were in contact with extreme right-wing groups.

In March 2024, the National Risk Assessment Terrorism Financing (NRA-TF) 2023 was published, identifying the twelve greatest terrorism financing risks for the Netherlands at the time.[27] According to the NRA-TF, the greatest risk lies with 'unlicensed payment service providers and hawala banking', also known as underground banking. Although these services are, by definition, partially outside the scope of the Wwft, regulated financial service providers are used, as well. It is therefore possible to provide our investigative partners with financial intelligence on these subjects. For instance, information about complex international money laundering schemes[28] or transactions linked to drug crime.[29]

In 2024, seventeen files containing indications of underground banking and terrorist financing were shared with investigative authorities. Several analyses showed that 'cash compensation structures' and underground banking were being used to supply terrorist groups with weapons and/or money. Additionally, there are indications that (transport) companies are being used for terrorist financing purposes. Cash collected in this way can be used to pay staff under the table. The money earned from services that are provided, is used to make third-party payments for companies in the Middle East. There, hawala bank payments can be made to locally active terrorist groups.

Another risk identified in the NRA-TF concerns 'funds obtained through other forms of crime'. In 2024, analyses revealed links between organised crime and individuals, or legal entities associated with terrorist organisations. In line with the findings of an EU project on terrorist financing, we also detected developments pointing towards Crime Enabled Terrorism Financing (CETF).[30] This doesn't concern a transactional relationship between organised crime and a terrorist organisation, but rather crime which finances terrorism. Internationally, the fight against the financing of Hamas within Counter Terrorism Financing Taskforce Israël (CTFTI)[31] has also continued. This led to several files being shared with relevant investigative partners both nationally and internationally.

Table 5 shows the number of files produced in 2024 based on analyses of terrorist financing risks. Such analyses have three possible outcomes, which result in files containing suspicious transactions. The analysis may show there is no indication of terrorism or terrorist financing, but there are indications of another crime. Second, it may be a combination of both or third, an analysis may indicate terrorism (financing) on its own. Table 5 shows the number of files with indications of terrorism (financing), including combinations with other crimes, amounted to 247 in 2024. This is an increase of 35% compared to 2023. Files with a possible jihadist background are still strongly represented. Some of these files concern older/less recent unusual transactions that were subsequently declared suspicious by recently launched criminal investigations in the Netherlands or abroad. Additionally, recent transactions were used to support investigations into current and concrete terrorist threats in the Netherlands and abroad.

The insights into terrorist financing derived from our analyses are used in various ways. We share them with specialist investigation teams in the Netherlands and abroad. In addition, FIU-the Netherlands contributes financial intelligence to international partnerships for knowledge development, resulting in more insight worldwide. Finally, we use our insights to provide advice at the policy level.

Table 5: Case files initiated on suspicion of terrorism/terrorist financing in 2024

	Number of files	Share of files (%)	Number of transactions	Share of transactions (%)
T/TF[1]	173	56%	695	27%
T/TF+other[2]	74	24%	1,122	44%
Other[3]	62	20%	737	29%
Total	**309**		**2,554**	

[1] These are files with an indication of terrorism (financing) where FIU-the Netherlands analysed and confirmed a possible link.
[2] These are files with an indication of terrorism (financing) where FIU-the Netherlands found another possible link with a different offence.
[3] These are files with an indication of terrorism (financing) where FIU-the Netherlands only found a possible link with a different offence.

[24] https://www.nctv.nl/onderwerpen/dtn/documenten/publicaties/2024/12/17/infographic-dreigingsbeeld-terrorisme-nederland-december-2024
[25] https://egmontgroup.org/about/organization-and-structure/
[26] https://egmontgroup.org/wp-content/uploads/2021/09/20190712-IEWG-Lone-Actors-and-Small-Cells-Public-Sumary.pdf
[27] https://repository.wodc.nl/bitstream/handle/20.500.12832/3353/Infographic-NRA-terrorismefinanciering.pdf
[28] https://www.om.nl/actueel/nieuws/2024/11/19/om-eist-celstraffen-van-4-en-7-jaar-tegen-broers-voor-witwassen-miljoenen-euros-via-ondergronds-bankieren
[29] https://www.fiod.nl/man-verdacht-van-illegaal-bankieren-en-overtreding-opiumwet/
[30] https://rusieurope.eu/ova_doc/missing-connections-crime-enabled-terrorism-financing-in-europe/
[31] https://www.fiu-nederland.nl/wp-content/uploads/2023/11/CTFTI-Public-Statement.pdf

Chapter 3

Relevant developments and projects in 2024

FIU-the Netherlands collaborates with national and international public and private partners. Our common goal is to combat and prevent money laundering, offences preceding it and terrorist financing to safeguard the integrity of the financial system. In 2024, important developments took place in this field.

3.1 International collaboration

FIU-the Netherlands actively contributed to the Egmont Group during the year. This partnership that consists of 177 FIUs, organised its thirtieth annual plenary meeting in Paris in June 2024. This event brought together four hundred FIU delegates and partner organisations. The aim: to strengthen global cooperation in the prevention and combating of money laundering and terrorist financing. During this plenary meeting, FIU Surinam formally joined the Egmont Group, partly with the help of FIU-the Netherlands. Furthermore, the head of FIU-the Netherlands received a special token of appreciation for her exceptional and long-standing commitment to the Egmont Group.

Furthermore, we collaborated on an operational level, especially within Europe. For example, together with the Italian and Spanish FIU, we analysed unusual transactions related to a payment service provider (PSP) with companies in various European countries. This strongly indicated that the PSP is part of a network involved in laundering money obtained through tax fraud and misuse of public funds. Between 2021 and 2024, approximately one hundred million euros were moved through this network. It appears that this PSP abused various licences in different countries, resulting in fragmented supervision. This allowed the party to take advantage of the missing overview by a single supervisory authority. The supervisory authorities have been informed of this case.

3.2 National collaboration

Also on the national level, FIU-the Netherlands actively sought cooperation with both public and private partners.

3.2.1 Project chain reinforcement

In 2024, we continued our efforts within the chain reinforcement project. In this project, we collaborate with the police, the Public Prosecution Service (OM) and the Fiscal Information and Investigation Service (FIOD) to improve and optimise the use, quality, insight into and knowledge of suspicious transactions. Attention is also being paid to the feedback loop. In this context, we are exploring how we can further strengthen the feedback from public partners on the use of suspicious transactions to provide even better information to reporting entities.

The project focuses primarily on improving internal and mutual work processes. In 2024, it was ensured that the investigative services have a recipient in place for each suspicious transaction file, allowing for better assessment of the investigative interest and relevance of each file. The resulting feedback strengthens the connection between investigative services and FIU-the Netherlands. This also helped to bring ‘Match Investigation, Prosecution and Execution’ more in line with the investigative interest.

Additionally, in 2024, FIU-the Netherlands continued improving its website and worked on more targeted information/feedback for reporting entities. For example, through FIU articles, like FIU alerts, on LinkedIn and in the form of case studies on the website.

3.2.2 Further developments of the Fintell Alliance

FIU-the Netherlands has been effectively collaborating with its affiliated partners within the Fintell Alliance for more than five years. Analysts from Dutch Banks (Rabobank, ABN AMRO, ING, Knab, Volksbank, Triodos) and FIU-the Netherlands work together at a single location to identify, analyse, investigate and address vulnerabilities in the financial system arising from or in connection with criminal offences. This work is carried out based on the Wwft obligations and powers of the participating parties.

Within FIU-the Netherlands, we share insights into how criminal networks are structured and how they operate financially. With these insights, we want to enable the investigative services to take targeted actions. Additionally, we inform banks and other chain partners about the relevant risks, so they can take the appropriate preventive measures. This way, our insights can contribute to a system-oriented approach in which we frustrate the criminal system and make the financial system more resilient.

3.3 The European legislative package

In June 2024, the final texts of the European anti-money laundering package were published. These include:

- the European Anti-Money Laundering Regulation (AMLR) for prevention of the use of the financial system for money laundering or terrorist financing,
- the Anti-Money Laundering Directive 6 (AMLD6), an amended anti-money laundering directive and
- the Anti-Money Laundering Authority Regulation (AMLAR) for establishing an Anti-Money Laundering Authority (AMLA).

In addition to its role as anti-money laundering supervisor, the AMLA is also responsible for coordinating and supporting cooperation between the FIUs of the EU Member States. The AMLA will be established in Frankfurt.

The AMLAR and AMLR apply to all Member States as of 10 July 2027. The AMLD6 will be implemented in national legislation before that date. Consultation on this amendment will take place in 2025. Although the exact impact is still being investigated, it is already clear that it will be significant. For example, the new package will affect the reporting system, give more powers to the FIUs and provide more opportunities for international information exchange with other FIUs of the Member States. Joint analyses by European FIUs are an important feature of the new package, in which the AMLA will have an initiating and coordinating role. To this end, a lot of preparations had to be made in 2024. For example, on 4 October 2024, the head of FIU-the Netherlands contributed to the FFIS Amsterdam Workshop on AMLR Article 75 ‘Charting the new path for AML collaboration in the Netherlands’

3.4 Technological developments

In 2024, FIU-the Netherlands took steps in further developing the provision of information.

3.4.1 Software development

In 2024, we continued our work with the UN on the development of GoFintel. This is a new system that supports complex analyses. Naturally, we also continued to develop our core system GoAML. In the second half of 2024, this system was migrated to a new infrastructure, which contributed to improved security. In 2025, GoAML will be updated, a major project for which we already prepared in 2024.

3.4.2 New report forms and data quality

We also continued to develop customised report forms. In 2024, these became available to traders, accountants, notaries and estate agents in Caribbean Netherlands. These forms give reporting entities more guidance on how to report unusual transactions, which is an important step towards more uniform data quality.

Data quality is high on our agenda. During the year, we set up a structural process for dealing with data quality issues. Data quality is our priority, both internally and externally. Internally, for example, we improved the work process just mentioned. Externally, we are improving data quality with the aforementioned customised report forms and instructions. We will continue our efforts in 2025.

3.5 Organisation development

In 2024, FIU-the Netherlands further aligned staffing levels with the workforce plan (128.5 FTE) based on previously allocated resources. On 31 December 2024, operational staffing levels amounted to 109 FTE, excluding external hires. Thanks to the new ‘digital analysis’ job group, our research and analysis capacity is at full strength, making us equipped even better to explore our data, both tactically and strategically. On the technological side, we invested in application and data management to give substance to our data-driven organisation.

This growth requires continuous attention and appropriate guidance, with focus on our employees, their development and our shared culture. We also worked on professionalising our (business) structures and processes. The newest part of the organisation, the management office, has been further developed and set up. This department was created to further strengthen the foundation of FIU-the Netherlands. In addition to providing broad policy advice and performing operational tasks, the management office has taken steps to organise a continuous process of strengthening information security.

Afterword

At the time of writing, the geopolitical situation worldwide is extremely turbulent. Conflicts, sanctions and shifting power relations are having a direct impact on financial markets and crime patterns. In the Netherlands, there are concerns about subversive crime, its deep roots in our society and the violent incidents that result from it. Simultaneously, the regulatory framework in Europe is rapidly moving towards a new standard. With the arrival of the new European anti-money laundering package, the scale of the changes facing the sector is becoming increasingly clear. The impact of these changes will be widely felt in the coming years, both for reporting entities and for supervisory authorities and investigative services. And, of course, for us.

Outlook: new regulation and impact

The introduction of the AMLR and AMLD6 will further strengthen the fight against financial crime. The establishment of AMLA will lead to a stronger, harmonised approach to money laundering and terrorist financing within the EU. This will not only lead to stricter requirements for reporting institutions, but also to more intensive cooperation between FIUs, national supervisory authorities and law enforcement agencies.

Experience has taught us that criminal networks adapt quickly to changing legislation and supervision. Money laundering practices and fraudulent schemes are becoming more international and complex. The use of shell companies and the abuse of legal entities is likely to keep increasing, as is the use of innovative financial products such as crypto-assets and decentralised financial networks. We also see that labour-intensive sectors remain vulnerable to phenomena such as cash compensation and tax evasion. This is one of the reasons why prevention and proactive cooperation will increasingly come into focus. With the AMLR, there will be more emphasis on risk-based supervision and the sharing of insights between public and private parties. This requires further professionalisation of the cooperation between FIUs and reporting entities. To achieve this, advanced data analysis and artificial intelligence (AI) will play an increasingly important role.

Collaboration remains crucial

The challenges are growing, but so are our possibilities for combatting crime effectively. With smart technology, better international cooperation and a strong chain of public and private partners, our abilities to combat money laundering, underlying crime and terrorist financing keep growing. The transition to a stronger European anti-money laundering framework offers opportunities to work more effectively and efficiently. At the same time, we recognise that transitioning to this new framework will demand a lot from all parties involved.

These developments emphasise the importance of continuous investments in cooperation, innovation and knowledge exchange. Only by joining forces, we can effectively disrupt criminal structures and safeguard the integrity of the financial system.

Together we see more.

Annex I

Key figures

Table 6: Number of UTs per reporting group

Reporting group	2022	2023	2024	Of which subjective
Remote gambling providers	29,180	28,775	30,553	73%
Custodial wallet providers	32,594	27,087	116,788	3%
Accountant	2,233	3,195	3,388	98%
Lawyer	15	22	24	92%
Bank	553,327	672,085	534,103	99%
Tax Administration	1	0	0	n/a
Tax advisor	433	356	338	89%
Investment institution	245	139	125	99%
Investment firm	86	70	168	96%
Life insurance broker	0	0	0	n/a
Mediator of purchase/sale*	n/a	n/a	116	79%
Payment service agent	0	2	0	n/a
Payment service provider	249,504	150,075	163,363	53%
Payment service provider- PSP	751,742	1,010,385	1,416,103	29%
Domicile provider	6	31	112	96%
Customs	4,070	4,193	4,935	7%
Electronic money institution	18,790	6,158	7,034	95%
Foreign Intelligence	94,154	183,491	191,099	100%
Trader - Antiques**	3	3	n/a	n/a
Trader - Gemstones**	1,352	838	n/a	n/a
Trader - Other goods**	678	559	n/a	n/a
Trader - Art objects**	173	207	n/a	n/a
Trader - Vessels**	20	32	n/a	n/a
Trader- Vehicles**	3,230	3,316	n/a	n/a

Reporting group	2022	2023	2024	Of which subjective
Institutes for Collective Investment in Securities	7	2	1	100%
Legal service provider	1	6	6	50%
Purchaser/seller of goods*	n/a	n/a	4,437	34%
Purchaser/seller of art*	n/a	n/a	25	24%
Life insurer	42	15	20	95%
Real estate agent	218	354	155	87%
Non-bank - Credit cards	9,985	10,771	421,189	97%
Non-bank - Interbank markets	19	22	0	n/a
Non-bank - Leasing	321	26	87	98%
Non-bank - Issue of loans	406	438	422	98%
Civil-law notary	1,213	1,051	998	96%
Government - Other	2	0	0	n/a
Pawnshop	139	197	292	30%
Gambling casino	9,284	9,781	9,143	13%
Valuer	1	2	6	100%
Supervisory authority	40	29	19	100%
Trust office	89	71	39	92%
Lessor of safety deposit boxes	41	76	92	100%
Virtual currency exchange service	131,702	219,566	578,312	5%
Exchange institution	830	741	881	57%
Total	**1,896,176**	**2,334,167**	**3,484,373**	**49%**

*As of 2024, the reporting groups around goods have been divided into mediators, purchasers/sellers of goods and purchasers/sellers of art. This was done to bring them into line with the Wwft.

**This reporting group was used in annual reviews prior to 2024 and has been moved to the appropriate reporting group mediators, purchasers/sellers of goods and purchasers/sellers of art as of 2024.

Table 7: Number of institutions who reported at least one UT, per reporting group

Reporting group	2022	2023	2024
Remote gambling providers	18	21	24
Custodial wallet providers	5	7	6
Accountant	397	423	450
Lawyer	12	11	17
Bank	55	55	54
Tax advisor	77	98	115
Tax Administration	1	0	0
Investment institution	12	15	17
Investment firm	12	12	8
Mediator of purchase/sale*	n/a	n/a	4
Life insurance broker	0	2	0
Payment service provider	16	13	11
Payment service provider - PSP	31	35	35
Domicile provider	3	6	11
Customs	1	1	1
Electronic money institution	8	11	13
Foreign Intelligence	36	47	48
Trader - Antiques**	2	1	n/a
Trader - Gemstones**	36	41	n/a
Trader - Other goods**	87	84	n/a
Trader - Art objects**	10	6	n/a
Trader - Vessels**	12	13	n/a
Trader - Vehicles**	630	555	n/a
Institutes for Collective Investment in Securities	2	1	1
Legal service provider	1	5	4
Purchaser/seller of goods*	n/a	n/a	605
Purchaser/seller of art*	n/a	n/a	8
Life insurer	4	4	4
Real estate agent	99	73	74
Non-bank - Credit cards	3	3	3
Non-bank - Interbank markets	1	1	0
Non-bank - Leasing	5	6	4
Non-bank - Issue of loans	16	20	24
Civil-law notary	331	320	271
Government - Other	1	0	0
Pawnshop	3	4	4
Gambling casino	1	1	1
Valuer	1	2	3
Supervisory authority	3	4	2
Trust office	28	19	16
Lessor of safety deposit boxes	1	2	1
Virtual currency exchange service	24	30	30
Exchange institution	2	3	2
Total	**1,987**	**1,955**	**1,871**

*As of 2024, the reporting groups around goods have been divided into mediators, purchasers/sellers of goods and purchasers/sellers of art. This was done to bring them into line with the Wwft.

**This reporting group was used in annual reviews prior to 2024 and has been moved to the appropriate reporting group mediators, purchasers/sellers of goods and purchasers/sellers of art as of 2024.

Table 8: Number of STRs per reporting group

Reporting group	2022	2023	2024
Remote gambling providers	1,993	3,560	3,641
Custodial wallet providers	2,631	2,798	3,735
Accountant	461	967	671
Lawyer	4	13	12
Bank	51,939	122,744	65,391
Tax advisor	60	144	118
Tax Administration	1	0	1
Investment institution	18	19	27
Investment firm	6	2	2
Mediator of purchase/sale*	n/a	n/a	6
Life insurance broker	0	0	1
Payment service provider	19,759	17,385	10,733
Payment service provider - PSP	5,000	18,166	15,817
Domicile provider	2	7	9
Customs	218	584	277
Electronic money institution	19	109	259
Foreign Intelligence	625	351	457
Legal services provider	0	0	4
Trader - Antiques**	0	0	n/a
Trader - Gemstones**	125	83	n/a
Trader - Other goods**	163	40	n/a
Trader - Art objects**	35	21	n/a
Trader - Vessels**	5	3	n/a
Trader - Vehicles**	302	275	n/a
Purchaser/seller of goods*	n/a	n/a	364
Purchaser/seller of art*	n/a	n/a	19
Life insurer	19	12	9
Real estate agent	26	29	12
Non-bank - Credit cards	811	1,027	1,659
Non-bank - Interbank markets	3	3	0
Non-bank - Leasing	14	14	24
Non-bank - Issue of loans	141	153	211
Civil-law notary	387	374	324
Government - Other	0	1	0
Pawnshop	27	35	40
Gambling casino	846	774	837
Valuer	0	1	4
Supervisory authority	29	32	15
Trust office	50	19	17
Lessor of safety deposit boxes	25	56	65
Virtual currency exchange service	6,059	10,713	13,568
Exchange institution	90	64	79
Total	**91,893**	**180,578**	**118,408**

*As of 2024, the reporting groups around goods have been divided into mediators, purchasers/sellers of goods and purchasers/sellers of art. This was done to bring them into line with the Wwft.

**This reporting group was used in annual reviews prior to 2024 and has been moved to the appropriate reporting group mediators, purchasers/sellers of goods and purchasers/sellers of art as of 2024.

Table 9: Number of registered forms of crime in case files*

Form of crime	Number of case files	Number of transactions
Threat	5	77
Corruption	87	769
Cybercrime	21	1,102
Illegal drugs	327	3,546
Fraud	922	22,313
Violence	16	167
Child pornography	27	102
Human trafficking	91	1,715
Human smuggling	12	230
Environment	9	32
Murder/manslaughter	7	12
Underground banking	80	833
Radicalisation	4	59
Sanctions legislation	226	6,437
Terrorism	119	501
Terrorist financing	167	1,684
Arms trade	32	263
Economic Offences Act	16	104
Weapons and Ammunition Act	33	56
Wildlife crime	1	2
Money laundering	2,288	41,276
Other	66	1,321
Total**	**3,362**	**65,423**

*FIU-the Netherlands assigns at least one crime form to a case file, if possible. A case file/transaction may relate to several crime forms.

** This total is the number of unique case files with one crime form. Because a case file can contain several crime forms, the sum of the registered crimes in this table is higher than the number of unique case files.

Table 10: Number of STRs per transaction type

Type of transaction	Number	Share (%)
Non-cash transaction	62,399	53%
Other	31,522	27%
Money transfer	14,055	12%
Cash transaction	10,432	9%
Total	**118,408**	

Table 11: Number and share of executed STRs in 2024*

Amount	Number of transactions	Share of transactions (%)	Amount in €	Share of amount (%)
< € 10,000	79,878	69%	€ 91,090,618	1%
€ 10,000 to € 100,000	29,072	25%	€ 925,337,796	5%
€ 100,000 to € 1,000,000	5,558	5%	€ 1,605,048,774	9%
€ 1,000,000 to € 10,000,000	886	1%	€ 2,350,357,081	13%
€ 10,000,000 to € 100,000,000	114	<1%	€ 2,774,669,706	16%
> € 100,000,000	15	<1%	€ 9,781,475,004	56%
Total	**115,523**		**€ 17,527,978,979**	

*Intended transactions have not been taken into account.

Table 12: FIU requests per investigation service

Police	
Police Unit - Noord-Nederland	67
Police Unit - Zeeland West-Brabant	65
Police Unit - Oost-Nederland	61
National Police Unit	47
Police Unit - Midden-Nederland	47
Police Unit - Amsterdam	44
Police Unit - Den Haag	41
Police Unit - Rotterdam	39
Police Unit - Oost-Brabant	29
Police Unit - Noord-Holland	22
Police Unit - Limburg	12
Total	**474**

Other investigation services	
Fiscal Intelligence and Investigation Service (FIOD)	189
The Royal Netherlands Marechaussee	106
Netherlands Labour Authority	30
District Public Prosecutor's Office	20
National Criminal Investigation Department	15
Caribbean Netherlands Police Force	10
National Office for Serious Fraud, Environmental Crime and Asset Confiscation	6
Netherlands Food and Consumer Product Safety Authority	3
Human Environment and Transport Inspectorate	3
Social Investigation Department	2
Health and Youth Care Inspectorate	1
National Public Prosecutor's Office	1
Total	**386**

Annex II

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. This includes providing information to public and private partners and conducting research into developments in money laundering and terrorist financing. In 2024, FIU-the Netherlands had a budget of 17.6 million euros and a staffing capacity of 128.5 FTEs for this range of tasks. For the period 2021-2025 the following six strategic objectives were formulated within the scope of our tasks:

- **Information and research.** FIU-the Netherlands will continue to focus on strengthening and broadening its information task. In the coming period, we will pay specific attention to improving the feedback loop 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.
- **Cooperation.** The cooperation with our partners is essential for our work in preventing and combatting money laundering, underlying offences and terrorist financing. We focus on forms of cooperation that strengthen our core task at home and abroad by taking a leading role and experimenting with new forms of cooperation.
- **Digitisation.** FIU-the Netherlands embraces and utilises technology for intelligent and effective processing of unusual transactions and for continuous development of our analyses. By focusing on data quality and digitisation, we create more capacity for high-quality research and further improve the value of our output. Additionally, automation of our processes increases the job satisfaction among our employees.
- **Prioritising.** We make conscious choices about what we do and don't do. In view of the increasing number of unusual transactions, we apply a risk-based approach to our contribution within various partnerships and the available capacity.
- **Putting FIU on the map.** The importance and possibilities of financial intelligence and the unique role of FIU-the Netherlands are still not sufficiently known. We are therefore 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, which places heavy demands on our organisation. We are therefore specifically focusing on the development of current and future employees, harmonising existing processes and developing new ways of working.

Working method

Based on the Wwft, FIU-the Netherlands has been designated as the entity to which unusual transactions must be reported as described in Article 16 of the Wwft. Article 1a of the Wwft lists the various reporting groups to which this reporting obligation applies. The reported unusual transactions are then analysed to determine 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 independence and operational autonomy of the organisation. 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.

Colofon

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

Editors: FIU-Netherlands

www.fiu-nederland.nl/en