



ØKOKR

Financial Intelligence Unit

Annual Report 2022

2022 was characterised by war in Europe and economic challenges and uncertainty. In these circumstances, our work to combat money laundering and financing of terrorism is, if possible, even more important and relevant than before.

National and international cooperation is an important success factor in the fight against money laundering and financing of terrorism. Cooperation between the public and private sectors in Norway has yielded good results. In addition to mutual exchange of expertise and knowledge and a greater understanding of our joint challenges, cooperation builds trust and mutual respect. International cooperation is now a central element in our work. Throughout the year, the Financial Intelligence Unit (FIU) participated in meetings of the Egmont Group of FIUs and the Financial Action Task Force (FATF), in addition to working more closely with other FIUs. This cooperation has given us greater understanding of and opportunities to combat cross-border crime. Cross-border crime is increasing, making international cooperation key in the global fight against money laundering and financing of terrorism.

Preface



Sven Arild Damslora
Head of FIU

A handwritten signature in blue ink, which appears to read "Sven Arild Damslora".

The number of submitted Suspicious Activity Reports (STRs) in 2022 once again increased from the previous year. We interpret this as a sign that the awareness and understanding of the threat that money laundering and financing of terrorism constitute to society has never been higher. In 2022, estate agents made up the group of obliged entities which, after banks, submitted the most reports. Information from multiple obliged industries provide a better and broader basis for our analyses. Information received from foreign FIUs also increased significantly in 2022. We are therefore focusing on developing new techniques for enriching, processing and analysing the data and other information we receive in order to better exploit their potential.

Throughout 2022 we saw the introduction of new payment services and utilisation of artificial intelligence. New technology is beneficial to society and has the potential to make everyday life more efficient, but can also be used for criminal purposes and challenge our work against money laundering and financing of terrorism. The war in Europe has also significantly changed the overall threat picture. Experience tells us that we are facing new threats and challenges, particularly from state actors, whose presence is seen more often in connection with money laundering and misuse of the financial and commercial systems. This affected our work and is something we must continue to monitor closely.

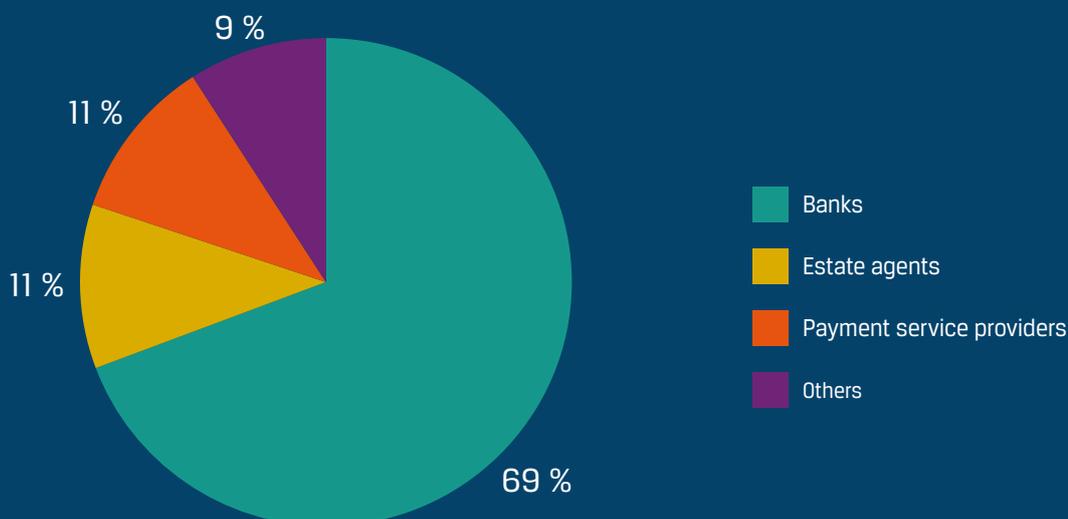
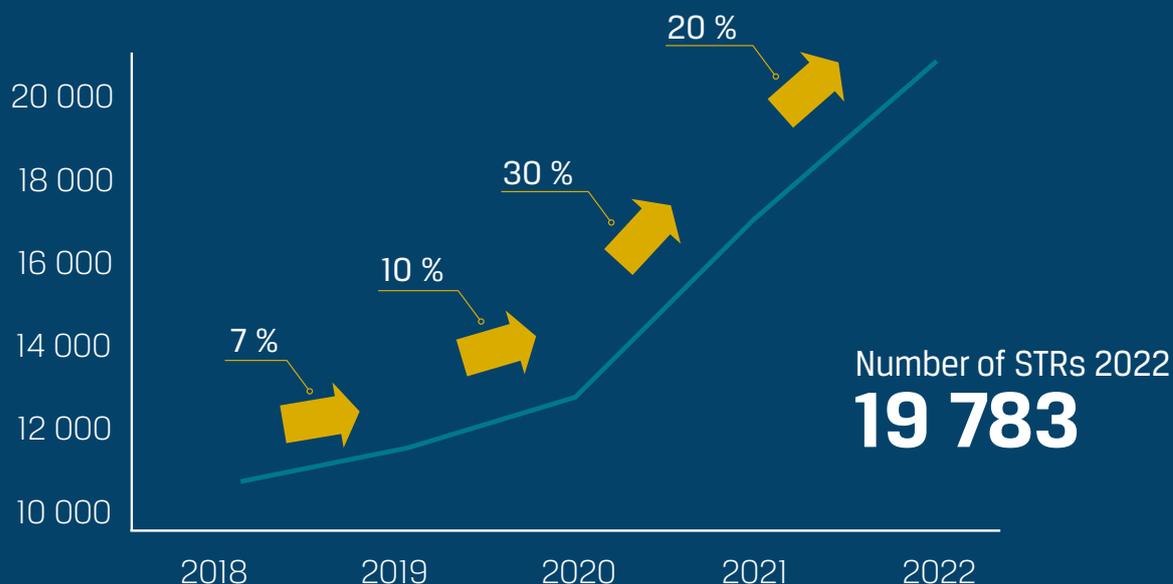
As noted above, good cooperation is important to be able to tackle these threats and challenges. In 2022, we saw a number of positive results of such cooperation. Joint projects and analyses combined with more expertise and information sharing are key to combat the challenges society faces.

I would like to take this opportunity to thank everyone who has contributed and assisted us in our work in a demanding year.

2022 Highlights

Financial Intelligence Unit – Norway

STRs 2022



National & international cooperation

Nasjonal

OPS AT
Contact forum
Supervision
Supervisory authorities

Internasjonal

FATF
EGMONT Group of FIUs
EU FIUs Platform



Contents

1. Introduction	5
1.1. The organisation of the FIU at Økokrim	5
1.2. Role and function.....	6
1.3. Priorities and activities	6
2. Processing of Suspicious transaction Reports	8
2.1. New form for reporting suspicious activity.....	8
3. Production and activities	10
3.1. Suspending transactions	11
3.2. Sanctions.....	12
3.3. International information sharing	12
3.4. Inquiries received and replied to.....	13
4. Operative and strategic analyses	15
4.1. Operational analyses	15
4.2. Strategic analyses	26
5. Knowledge sharing and guidance	28
5.1. First quarter.....	28
5.2. Second quarter	28
5.3. Third quarter.....	29
5.4. Fourth quarter	30
6. National collaboration	31
6.1. The Norwegian police	31
6.2. OPS AT	31
6.3. The Contact Forum.....	32
6.4. Supervisory authorities	32
6.5. Regulatory authorities.....	33
7. International cooperation	34
7.1. FATF.....	34
7.2. Egmont Group of FIUs	35
7.3. Participation in international meetings	35
8. STR statistics.....	36
8.1. Source data	36
8.2. Submitted STRs.....	36
8.3. Reporting industry groups.....	37
8.4. Obligated entities	38
8.5. Reporting time.....	39
8.6. Suspicion codes	40
8.7. Crime trends.....	41
8.8. Who are reported?	46

1. Introduction

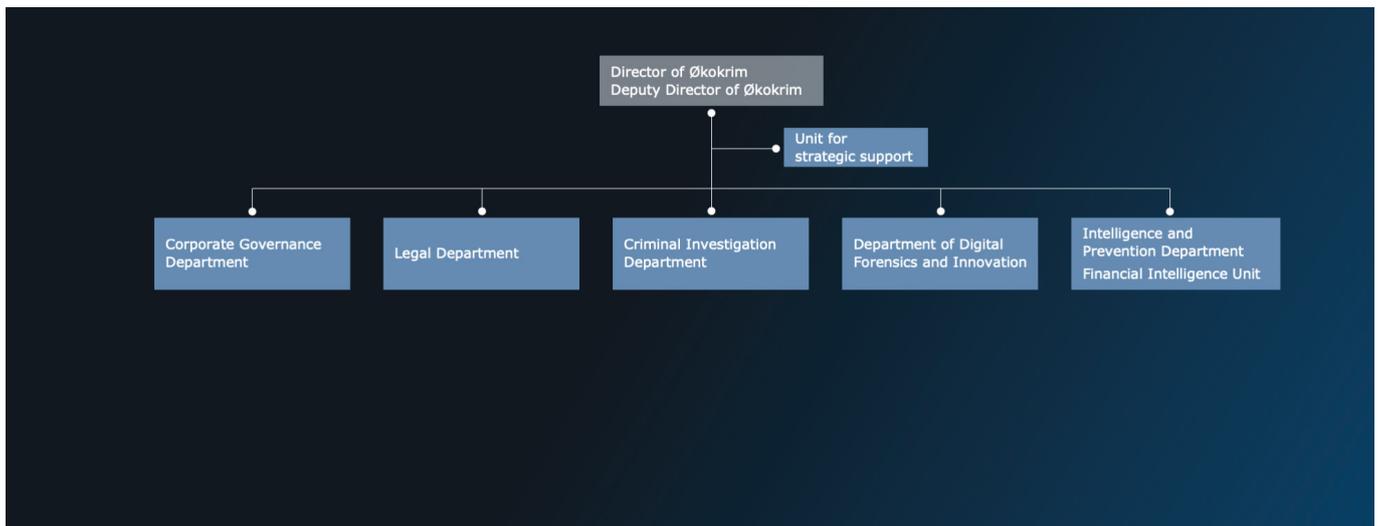


Figure 1: Økokrim organisational chart

1.1. The organisation of the FIU at Økokrim

International recommendations, guidelines and legislation require the signatory countries to establish and maintain Financial Intelligence Unit (FIUs). The national FIUs are part of the countries' efforts to prevent money laundering and financing of terrorism in accordance with article 32 of the EU's fourth money laundering directive, and work both nationally and internationally. In Norway, the FIU is organised under the Norwegian National Authority for investigation and Prosecution of Economic and Environmental Crime (Økokrim). The FIU, together with the intelligence and prevention units, make up the Intelligence and Prevention Department at Økokrim (see figure 1).

The FIU had 20 employees at the end of 2022, of which roughly two-thirds worked with investigative and operational analysis, and the rest with following up the obliged entities and cooperation with foreign FIUs. The employees are primarily recruited from the police, tax authorities, customs service, finance and computer industries, including two with law degrees.

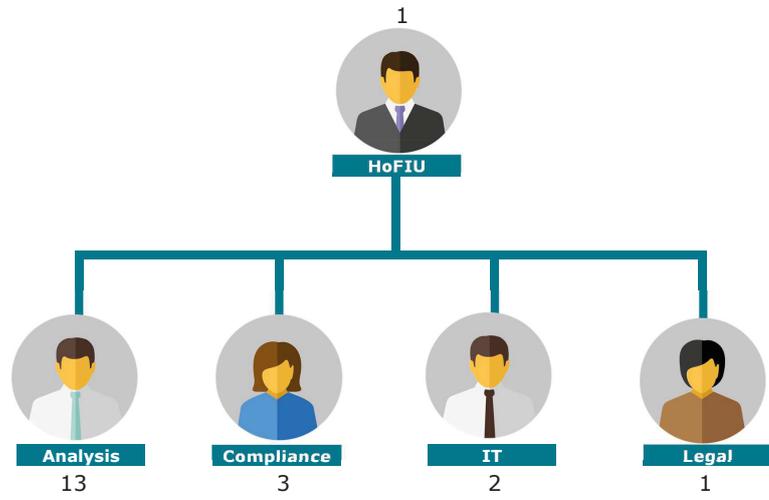


Figure 2: FIU organisational chart

1.2. Role and function

Nationally, the FIU's primary function is to receive suspicious transaction reports (STRs) from entities obliged by the Anti-Money Laundering Act to submit them. The information in these reports is processed, enriched and analysed before the results are distributed to the police, supervisory and regulatory authorities, and foreign cooperating law enforcement organisations.

A key task for the FIU is also the preparation of operational and strategic intelligence products and reports for use by the police and other authorities in their efforts to combat money laundering and financing of terrorism.

1.3. Priorities and activities

International framework

In addition to providing the FIU's legal basis, the international recommendations and directives also include specific requirements relating to functions, tasks, roles etc. that an FIU must fulfil. These are tasks that the FIUs perform, and on which they are constantly measured.

National legislation – the Anti-Money Laundering Act and the Police Databases Act:

The FIU is data controller for the money-laundering database Ask and tasked with ensuring that current privacy and confidentiality legislation is complied with in the processing of information entered in the database. This also entails a responsibility for deletion of data, processing requests for access etc.

It is a fundamental principle that the FIU's activities, operations and intelligence production be prioritised based on the risk posed by money laundering and financing of terrorism.

"The information in the STRs is processed, enriched and analysed before the results are distributed to the police, supervisory and regulatory authorities, and foreign cooperating law enforcement organisations."



Figure 3: Prioritisations – EFE



National directives:

The Government and other authorities (e.g. the National Police Commissioner and Director of Public Prosecutions) issue national directives and define national priorities which must be taken into account in the preparation of strategic and tactical analyses and intelligence products. One example in this regard is the Government's prioritisation of tax fraud and exploitation of workers.

National risk:

Risk and threat assessments prepared by the national security services and other national threat and risk assessments also inform our prioritisation of analyses and allocation of resources to various tasks and requests.

Priorities – Norwegian FIU:

In addition to the elements described above, we have a particular focus on cases where there is a potential for confiscating proceeds of crime, and we prioritise cases and areas where our information is unique and in particular demand, and where we see that it can make a significant difference as regards prevention of crime and solving cases.

2. Processing of Suspicious transaction Reports



Suspicious transaction reports (STRs) are, as mentioned above, reports about suspicious circumstances submitted by obliged entities under the Anti-Money Laundering Act. The reports can concern both private individuals and companies. The information in the STRs is automatically processed, enriched and checked against a number of external sources and police databases. Various automatic and manual processes are used to decide which STRs – enriched with additional information – should be used in various projects and analyses. Our current data system automatically transfers information from the reports to the police intelligence database based on given parameters and rules.

2.1. New form for reporting suspicious activity

The development of a new and improved form for reporting suspicious activity has been an important and prioritised task for the FIU in 2022. The Schrems II judgment has represented an uncertain and unclarified factor in this connection¹. During the course of 2022, it became clear that the Schrems II judgment and the use of cloud services in the USA in the Altinn 3.0 digital government dialogue service, were going to become a bigger challenge than expected. A risk assessment was therefore carried out of whether or not Altinn 3.0 could be applicable for the reporting form and for our purposes. The assessment was carried out in cooperation with the Norwegian Police IT Unit with particular focus on the contents of the reports. The assessment concluded that the use of cloud services in the USA would entail both risks and challenges related to the transfer of personal data to countries outside the EU/EEA, but most importantly a not significant and unacceptable risk of disclosure of information under US intelligence legislation. In view of the particularly sensitive nature of the information (suspicion of money laundering, financing of terrorism and the proliferation of weapons of mass destruction), the consequences of such disclosure could be very serious for private individuals, businesses, the Norwegian police and Norwegian interests. The assessments and recommendations were duly noted and it was decided not to develop a reporting form based on the Altinn 3.0 platform. We are now looking into alternative solutions in cooperation with the Norwegian Police IT Unit. Until the reporting has migrated to a new solution, this will not affect the existing Altinn reporting solution.

¹ <https://www.digdir.no/handlingsplanen/hva-er-schrems-ii-dommen/2581>.

Obligated entities
cf. AMLA s. 4

Auditors
Lawyers

Banks
Estate agents

PSP*
Accountants

Insurance companies
Payment service providers

Duty to conduct examinations cf. MLA s. 25



Suspicious transaction that may be linked to money laundering or financing of terrorism

Duty to report cf. MLA s. 26

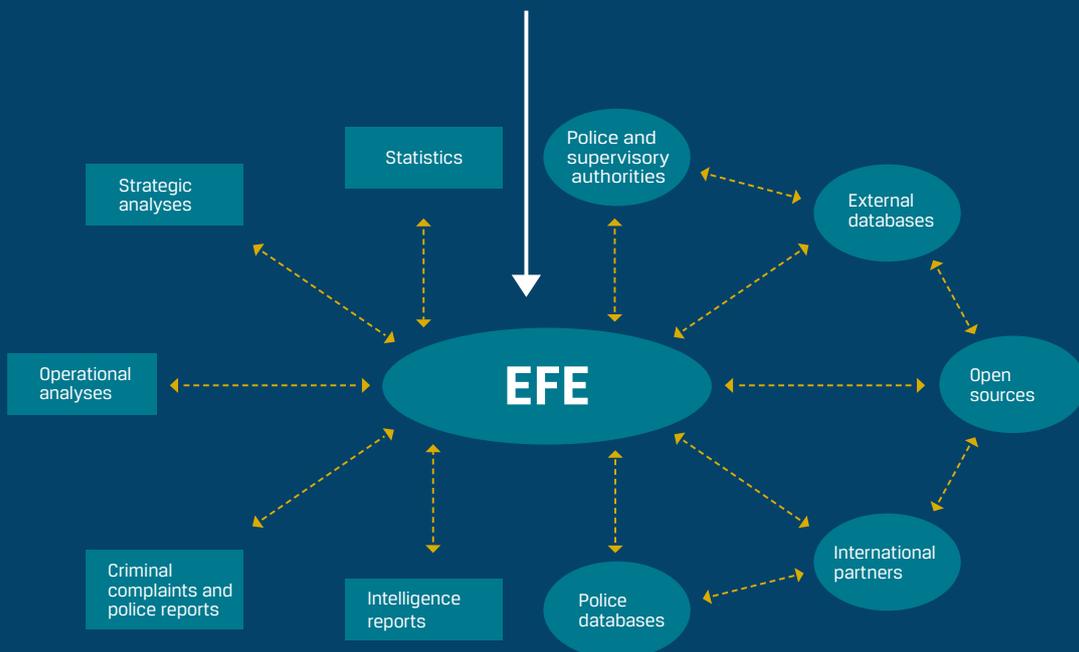


Note: STRs are not criminal complaints

Information input from STRs



Processing of internal and external information

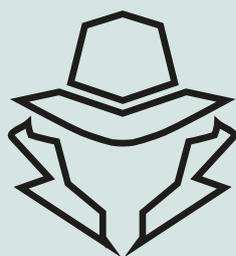


*Cryptocurrency exchanges

3. Production and activities

Previously known to the police

**Known:
8426**



**Unknown:
8270**

The statistics show that just over half of all persons were unknown to the police before being reported to Økokrim in 2022. As a result of the anti-money laundering regime, Økokrim obtains information about individuals whom the regular police are unaware of.

One of the FIU's key tasks is to process and enrich the information received through the STRs. The information is assessed and primarily distributed to the police for use in criminal investigations and confiscation. The information is also shared with other specialist agencies, supervisory and regulatory authorities, and other FIUs. The products provided and their formats depend on the recipient and the recipient's intended use of the information.

Table 1 presents an overview of products shared with the police, regulatory authorities and foreign FIUs in 2022. Products may include intelligence reports, replies to requests and information sharing. A product may include data and information from multiple STRs and internal and external sources.

Intelligence products and criminal cases communicated to	2022
The police	989
Regulatory and auditing authorities	107
Foreign FIUs	84
TOTAL	1181

Table 1: Products shared in 2022.

The FIU routinely enters enriched information obtained from STRs in the police's intelligence system. Table 2 shows the number of private individuals and organisations for which the FIU entered information in the intelligence system in 2022.

Information about private individuals and organisations entered into the intelligence system	2022
Private individuals	4606
Organisations	201

Table 2: The number of private individuals and organisations for which the FIU entered information in the intelligence system².

² In all, the FIU had entered information about 40,902 private individuals and 1925 organisations in the intelligence system per 01.01.2023. Private individuals and organisations are routinely deleted from the intelligence system due to statutory requirements.

The purpose of suspending transactions is to give the FIU time to contact the police for their assessment of whether or not to start an investigation and whether the funds should be seized as part of criminal proceedings.

3.1. Suspending transactions

Under the Anti-Money Laundering Act section 27, the FIU can, in special cases, suspend transactions. The majority of these actions come as a result of the FIU receiving information from obliged entities indicating that a transaction should be suspended. The obliged entity does not request that a transaction be suspended, it merely informs the FIU that there are special circumstances which could justify suspending the transaction under the Anti-Money Laundering Act section 27. When the FIU suspends a transaction, the decision is executed by the obliged entity. The wording of the provision makes it clear that the authority to suspend transactions should be practised as an exception, not as a general rule.

The purpose of suspending transactions

The purpose of suspending transactions is to give the FIU time to contact the police for their assessment of whether or not to start an investigation or whether the funds should be seized as part of criminal proceedings³. This is particularly important in order to seize funds for later confiscation. Suspending a transaction may also provide an opportunity to prevent a criminal act.

In 2022, the FIU received 100 reports from obliged entities of cases where suspending transactions should be considered. 35 of them were suspended.

Suspending transactions	2020	2021	2022
Number of requests to suspend transactions:	62	62	100
Number of suspended transactions:	28	16	35
Total amounts suspended	NOK24,536,763	NOK30,915,031	NOK38,901,231

Table 3: Number of transactions 2020–2022.

Suspending transactions is an intrusive measure, and the FIU makes a thorough assessment before deciding to suspend a transaction. An important element in the assessment is to find out if the police want to seize the funds as part of a criminal investigation. Transactions can also be suspended pending a letter of request from from a foreign country. In some cases the conclusion may be that suspending a transaction would be disproportionate, that the conditions have not been met, or that the

³ When the FIU suspends a transaction, the decision does not constitute seizure under the Criminal Procedure Act



obliged entity should make inquiries with the customer to obtain sufficient information on which to base a decision.

Our experience is that the obliged entities increasingly apply the legal authority they have under the Anti-Money Laundering Act sections 4-13 and 4-14 to suspend transactions, and that the FIU in many cases therefore does not have to make a decision to suspend transactions under section 27 of the act.

3.2. Sanctions

Russia's full-scale invasion of Ukraine in February 2022 has fundamentally changed the security situation in Europe. As a result of Norway's changed economic and diplomatic relations with Russia, the demands on the obliged entities have become even stricter, as they since the invasion have had to relate to and comply with new rounds of (restrictive) sanctions becoming Norwegian law.

The money laundering and sanctions regulations are separate regulations with different reporting processes. Nevertheless, the obliged entities have an independent duty to consider whether any identified infringements and measures implemented under the sanctions regulations also trigger an inquiry and reporting duty under the Anti-Money Laundering Act sections 25 and 26.

The FIU's experience from 2022 is that many obliged entities have been mindful of their responsibilities and have laid down considerable effort to identify and report suspicious activity that can be tied to the stricter sanctions against Russia. Many of the reported violations are complex and may include both circumvention of sanctions and money laundering. Apart from contributing to preventing and combating money laundering, the information received from the obliged entities also helps us form a better picture of how the war in Ukraine affects crime in Norway and makes the Norwegian police better placed to catch new trends and MOs for how to circumvent sanctions.

3.3. International information sharing

During the last three years, the FIU has increased its information sharing with foreign FIUs, and the total amount of information received increased significantly in 2022, particularly information received from FIUs in the EU and EEA, see figure 4. The FIU receives information from other FIUs mostly in the shape of XBR⁴ reports, which are about specific cross-border transactions, and XBD⁵ reports, which disseminate relevant informa-

4 XBR = cross border report

5 XBD = cross border dissemination

XBDs are STRs received by a foreign FIU but which also may be of interest to other FIUs, among them Norway.

XBRs are cases in which the obliged entity submits an STR to its national FIU, but the service was performed in a foreign country. The FIU to which the STR is submitted must without delay forward the STR to the country where the service was performed.

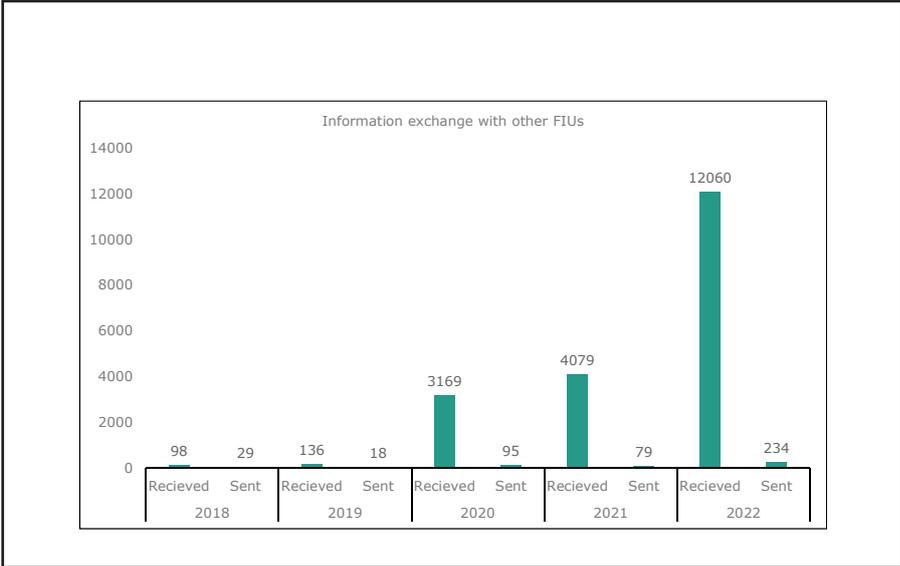


Figure 4: Number of inquiries sent to and received from foreign FIUs.

tion to multiple countries, see fact box.^{6,7} In 2022, the FIU received 10,456 XBD and 1471 XBR reports.

The increase in the number of XBD and XBR reports received is mostly due to automatically generated reports from FIUs in the EU and EEA. The EU Commission coordinates the cooperation between the EU FIUs through the "EU FIU Platform". The EEA FIUs, including Norway, participate in this cooperation.

Due to the EU Commission's efforts to strengthen European cooperation and information exchange, it is probable that the amount of information received from other FIUs will continue to increase. As a result, it will be possible to uncover more cases of money laundering and financing of terrorism, something which is also important in combating cross-border crime.

3.4. Inquiries received and replied to

The FIU has extensive contact with other national and international law enforcement organisations. In 2022, the FIU received 686 inquiries and replied to 653. An inquiry implies that the sender requests information that the FIU is expected to provide. The inquiries come mostly from

6 The sharing of information between the EU and EEA FIUs is an EU directive requirement, and the Commission monitors how the FIUs comply with this obligation. The EEA FIUs are not covered by this obligation. They are, however, monitored in the same way as EU FIUs.

7 The other information the FIU receives, is information and analyses which might be relevant to other countries, including non-EU and EEA countries. This information differs from XBD and XBR reports in that the information has been enriched beyond the STR itself.

police and regulatory authorities, who request information about private individuals and organisations entered in the money laundering database. The remaining inquiries come from other FIUs.

The 33 pending inquiries mostly concern requests from the Norwegian police where information gathering was still ongoing. These inquiries will be replied to in 2023. In cases where the Norwegian FIU requests information from other FIUs, the foreign FIUs must reply before the information can be forwarded to the Norwegian police.

Inquiries received	2022
The police	570
Foreign FIU	72
Regulatory authority	44

Table 4: Inquiries received in 2022

In 2022, the FIU forwarded 221 requests for information to 67 foreign FIUs. We have received replies to 200 of these requests and expect replies to the remaining 21. The FIU received 72 information requests from foreign FIUs, mainly through the EU encrypted FIU communication channel EU FIU.net. 60 of the requests have been replied to while nine will not be replied to due to deficiencies in the request⁸, and three will be replied to in 2023. Also, one request was received late in 2021 and replied to in 2022.

Information requests sent to and received from foreign FIUs	2018	2019	2020	2021	2022
Inquiries received	88	91	61	68	72
Replies sent	97	84	63	70	61
Inquiries sent	60	87	70	194	221
Replies received	62	96	60	182	218

Table 5: Information requests sent to and received from foreign FIUs

The number of requests the FIU forwards to other FIUs has increased 268% since 2018. The increase is due to better cooperation with the police districts and promotion of the opportunities for obtaining information through international police cooperation.

⁸ Usually, this concerns missing background information despite the FIU having sent reminders.



4. Operative and strategic analyses

Under FATF recommendation 29, FIUs are required to prepare analyses based on the information received. The FIU has access to the majority of the police's sources and systems, but it also has a singular source of information in the STRs. Based on the information held about private individuals and organisations the FIU is required to prepare the following types of analyses:

- Operational analyses
- Strategic analyses

In operational analyses the information is used to identify specific targets (persons, assets, criminal networks, associations etc.). The purpose is to trace specific activities or transactions and to identify connections between these and proceeds of criminal acts or financing of terrorism.

In strategic analyses the information, including information provided by other public authorities, is used to identify trends and patterns in money laundering and financing of terrorism. These analyses are used by the FIU and other state agencies to identify threats and vulnerabilities related to money laundering and financing of terrorism.

4.1. Operational analyses

This chapter gives an account of the analyses prepared by the FIU in 2022. The information received from the obliged entities is essential and has contributed to uncover suspicious activity in many types of crime and made the police aware of persons and organisations previously unknown to them. There are examples of analyses where information in a single STR combined with other sources provided vital information, while other examples are analyses where information in STRs from multiple obliged entities was combined to uncover serious crime by providing information about networks and MOs. An important task is to enrich and distribute information through relevant reports and channels to national and international partners, e.g. law enforcement and supervisory and regulatory agencies. Prioritisation and preparation based on risk assessment must be seen in connection with chapter 1.1.2.



MO

Proceeds of crime are used to purchase different types of assets and valuables to obscure their origins. Transfers abroad and purchase of various assets and valuables are among the MOs used.

Increased reporting from estate agents has provided better overview of the opportunities for money laundering through real estate and the risks this presents. The proceeds are concealed through purchase of real estate where the identity of the beneficial owner is kept hidden, e.g. through the use of nominees, blank title deeds and creation of a fictitious security interest in the property.

4.1.1. Money laundering**Laundering of proceeds of investment fraud**

In a case of investment fraud involving proceeds of at least NOK 40 million, the defendants were sentenced by the district court to imprisonment, loss of rights, compensation and asset confiscation. Økokrim has been working to track down and seize or freeze assets to cover the confiscation and compensation claims. The FIU has helped trace transactions in order to confiscate proceeds. Information collated from STRs and surrender orders issued to a number of obliged banks and estate agents provided the investigation with new information.

Also, a transaction was stopped following an alert from an obliged bank. The bank was also very helpful in following up and providing additional information, something which led to the police being able to restrain assets for confiscation. Information provided by the FIU provided grounds for searches and seizing of assets.

Professional money launderers and organised criminal networks

Several obliged entities have submitted STRs which have made it possible to find financial traces left by a presumed professional money launderer. The FIU suspects this person of laundering at least NOK 40 million of proceeds of crimes committed by several criminal networks. The proceeds are invested in real estate through "nominees", blank title deeds and purchase of shares in real estate companies registered to other persons in addition to money-lending. Evasion of taxes and excise duties on sales of assets and illegal money-lending was also uncovered.

Information provided by the obliged entities has been important in this case to reveal the complex structure and transactions in what appears what appears to be a very a very well-organised crime involving different MOs to divide up and mix illegal and legal funds. Different obliged entities have given the FIU opportunity to follow financial traces not known to other sources and databases.

Sale and export of construction machines where the origin of the funds and the final destination and end user of the machines were unknown

The FIU received information about a corporate client who sold construction machines to a foreign party. The client wanted to export the machines. An intermediary took care of the practical arrangements for the buyer, but the settlement came from an account belonging to a foreign third party with business operations in the Middle East.

The obliged entity provided relevant information and contributed specific additional information on request. The FIU worked the case and provided information to the relevant public authorities for further inquiries into the sale and the machines' final destination, and to investigate whether the offence represented a violation of international sanctions and export control legislation.

4.1.2. Tax fraud

Tax fraud concealed using the identities of emigrated persons

The FIU received a large number of STRs from several banks about a person who had previously emigrated to another Scandinavian country. He immigrated to Norway in winter 2021 and after this, the FIU received more than 20 STRs about him. In 2022, he registered a sole proprietorship within renovation with himself as owner. After receiving many reports about him over a short period of time, the FIU decided to map his activities. It turned out that his company received large payments from various private individuals and housing co-operatives. Over a short period, he had received multiple payments into 17 different bank accounts which appeared to be linked to his company. In all, payments amounting to NOK 10 million were received into his accounts, but no taxes or duties were ever paid.

The money paid into his accounts was immediately transferred abroad or paid out to private individuals. Cash withdrawals were made and valuables like gold, watches, cars etc. purchased. This activity appeared to be attempts to hide or launder the funds.

The man has reportedly lived abroad for the last 20 years and is linked to a criminal circle known for its involvement in tax fraud and exploitation of workers. The FIU has information that others are operating under his identity. The FIU has forwarded the information to the police and tax authorities.

In this area, the FIU's aim is to open criminal investigations in cooperation with the National Criminal Investigation Service and the police districts. In 2022, the FIU has contributed information which directly or indirectly has resulted in a number of convictions.

MO

Misuse of other people's identity has come to the fore in 2022 in connection with tax fraud and exploitation of workers. Companies were created and bank accounts opened in the names of family members, foreigners and disabled persons, but controlled by others.

Large amounts transit these accounts in a very short time. These transactions carry all the hallmarks of money laundering.

4.1.3. Sexual offences against children

Sexual offences against children – purchase of sexualised material from minors

The FIU received report of a man in his fifties who transferred money to minors. Several factors indicated that he was purchasing sexualised material. As the man was unknown to the police, it was key to the outcome that the FIU received the information. Information obtained through the STR and surrender orders uncovered that the man on several occasions transferred money to 12–17-year old children living in living in different places in Norway. The transfers were of small amounts up to NOK 200. The FIU also obtained information infomation of transfers abroad transfers abroad which we suspected were payments for child sexual abuse material. The information was forwarded to the police, who opened a file on him.

Sexual offences against children – purchase of child sexual abuse material

An obliged payment service provider reported suspicious transfers made by a man in central Norway to persons in the Philippines. The matter involved few transactions and recipients, but the man's background proved very relevant. He had recently been released after serving a sentence for sexual offences and several instances of assault. The FIU collaborated with the local police and several obliged entities to map and analyse the man's transactions. Based on this, the police opened an investigation, actioned against him and he was arreste. The police found child sexual abuse material on his electronic devices and the matter ended with conviction and a prison sentence.

4.1.4. Fraud

CEO fraud

In 2022, a Norwegian listed company became victim of a major fraud. USD 17 million was transferred from the company as a result of CEO fraud. The fraud took place in Asia as the payment was made from one of the company's subsidiaries there. The subsidiary made the transfer in the firm belief that the order came from the management in Norway. In this matter, the FIU assisted by obtaining financial evidence through the international network of FIUs, Egmont. The FIU sent a request to the FIU in the country where the money was transferred, and the replies received provided useful information about the concealment of the proceeds. It was uncovered that the funds were divided through 60 new transactions. It was also uncovered where the funds finally ended up and who controlled the companies to which the funds were transferred.

MO

Sextortion in the form of fraud and extortion takes place on TikTok and other social media. It commonly starts with the victim being contacted through a video conversation and flirted with before the conversation goes over to sexual activity. Afterwards, the victim is threatened with publication of sexualised photos on social media unless they pay the extortionists a lot of money.

The FIU is aware of cases where victims have paid more than NOK 300,000.

In extreme cases, this type of crime may have deadly outcomes for the victims.

Fraud

Through reports received about suspicious circumstances, the FIU became aware of a possibly false fundraising campaign in north-western Norway where the swindler stated that the collected funds were for the victims of the war in Ukraine. The facts, however, indicated that the swindler kept most (more than 90%) of the funds for himself and used them to make down-payments on private loans. He advertised the fundraising campaign on his private social media accounts and accounts registered to a company that he owned and managed himself.

The information was analysed and enriched before being forwarded as intelligence to the local police. Such information is also used in preparing prioritised intelligence products in the national effort to counter the effects of the war in Ukraine on crime in Norway and Norwegian society in general.

4.1.5. Financing of terrorism

Financing of terrorism in the sense of the AMLA coincides with the acts defined as financing of terrorism in the Penal Code section 135 or financing as described in the Penal Code section 136 a), cf. section 2 a). Financing of terrorism is defined as obtaining financial support for or giving financial support to terrorists or terrorist organisations. The primary aim is not profit but to finance the commission of another criminal act, i.e. the terrorist act. Financing enables terrorists to commit attacks and other acts that they would struggle to manage otherwise. Raising money is therefore an important factor in terrorism and obliged entities can by submitting STRs contribute to preventing and combating terrorism and terror-related acts. The FIU works closely with the Police Security Service and every year we forward a lot of information from STRs to them.

In November 2022 Økokrim and the Police Security Service, on assignment from the Ministry of Justice and Public Security, published a new "National Risk Assessment of money laundering and financing of terrorism" (NRA). Information from the submitted STRs forms an important part of an important part of the report's source data. The new NRA contains descriptions of several phenomena and trends in financing of terrorism.

Unlicensed payment services - "hawala"

The FIU has received reports about several private individuals who are suspected of running unlicensed private payment services through private bank accounts, an activity where there is particularly high risk of

MO

Romance scams in which Norwegians make contact online with persons who claim to be war victims who need financial support to travel to Norway.

False fundraisers claiming to raise funds to help war victims but where all or part of the funds raised are used by the fundraisers for personal ends.

New payment services are used to commit fraud, and the victims are often vulnerable people (elderly, widows and widowers). The funds are often transferred abroad to foreign banks and cryptocurrency exchanges.



money laundering and financing of terrorism. Some of these individuals have received hundreds of transactions and cash deposits of several tens of thousands of NOK. Individuals in these networks have during the course of a few years made cash transfers of millions of NOK and have over time established themselves as professional hawala agents with particular knowledge about cash transfers from Norway to certain high-risk countries where ordinary bank and financial services are subject to international sanctions.

These networks increasingly use social media to establish contact with each other to coordinate the transfer of funds from Norway.

The FIU has received many reports about such activity and will use this information to identify new actors and networks and spot new patterns and trends, which in turn will be distributed to relevant recipients.

Transactions made by an actor linked to a terrorist organisation

The FIU was made aware of suspicious activity where an actor gradually had changed the usage pattern on his bank account. The bank reacted to changes in the volume of cash deposits and transfers which did not conform with the client's own statements about his use of the bank's services. The bank also discovered that the client had started to use an online payment service to make transfers abroad which he had not availed himself of earlier. Although the total volume of deposits and transfers did not add up to a significant amount, the bank decided to carry out a Know Your Customer check. The client's reaction to this check strengthened the bank's suspicions and prompted them to them to submit an STR.

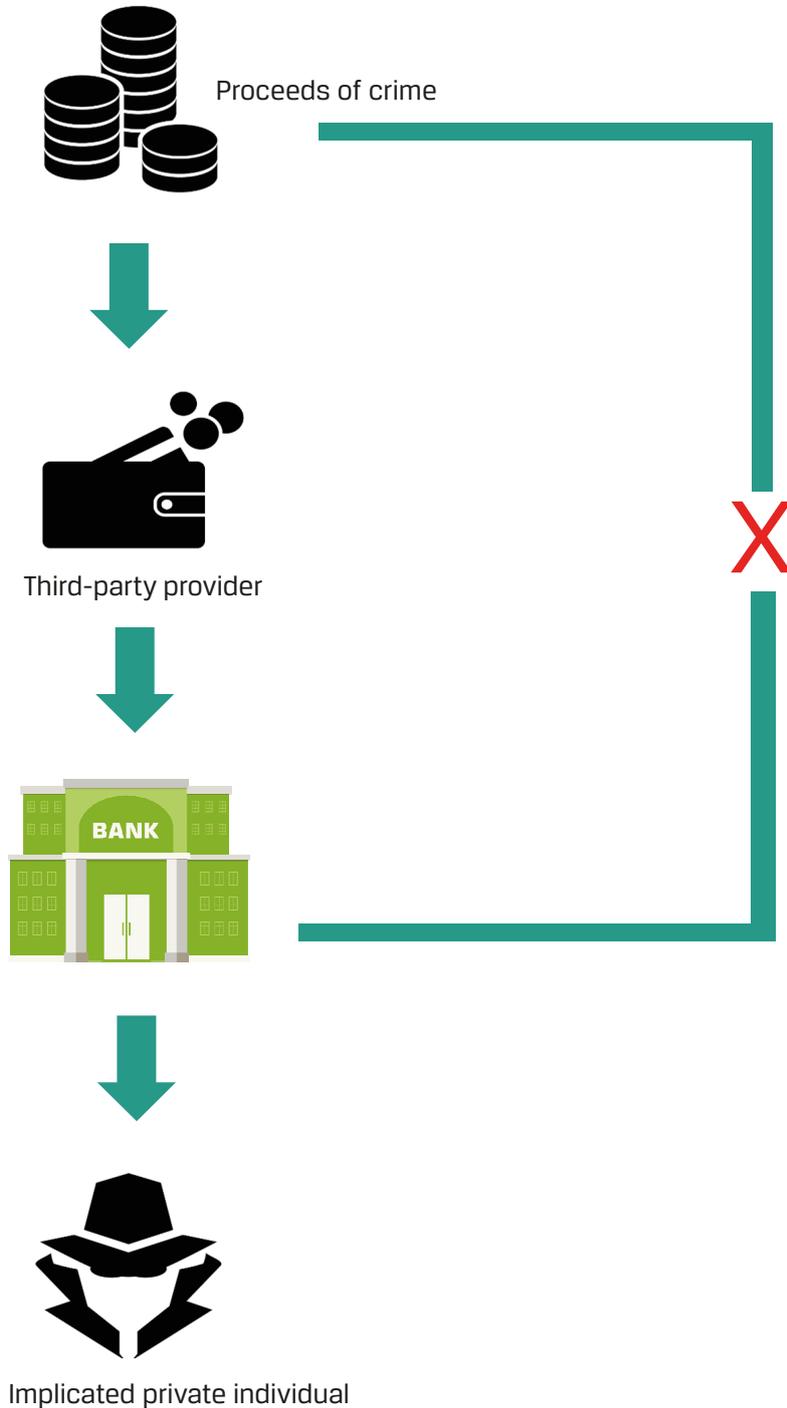
The FIU enriched and analysed the information in the STR and also found out that several foreign law enforcement and security agencies worried that the client could be linked to a terrorist organisation. The analysis was forwarded to the competent authority for further analysis and assessment.

4.1.6. Trends

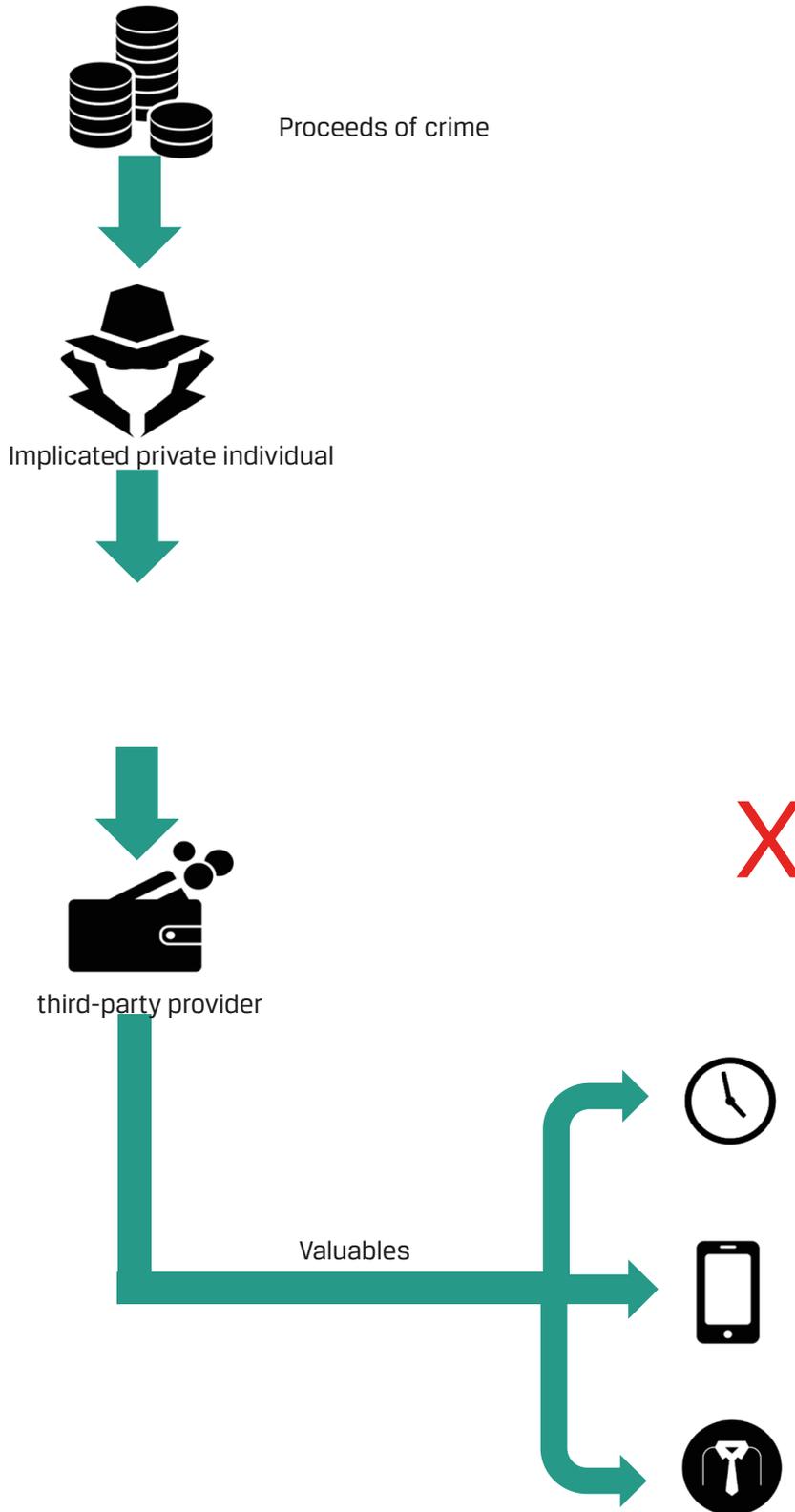
This chapter describes the most common MOs observed in 2022 based on the information in the STRs. The overview is therefore not exhaustive.

Third-party providers

Below, the term third-party provider is used to denote external actors whose services are used to make payments or transfer money, e.g. Vipps [a Norwegian payment app], PayPal, Apple Pay, banks and other licensed payment service providers.



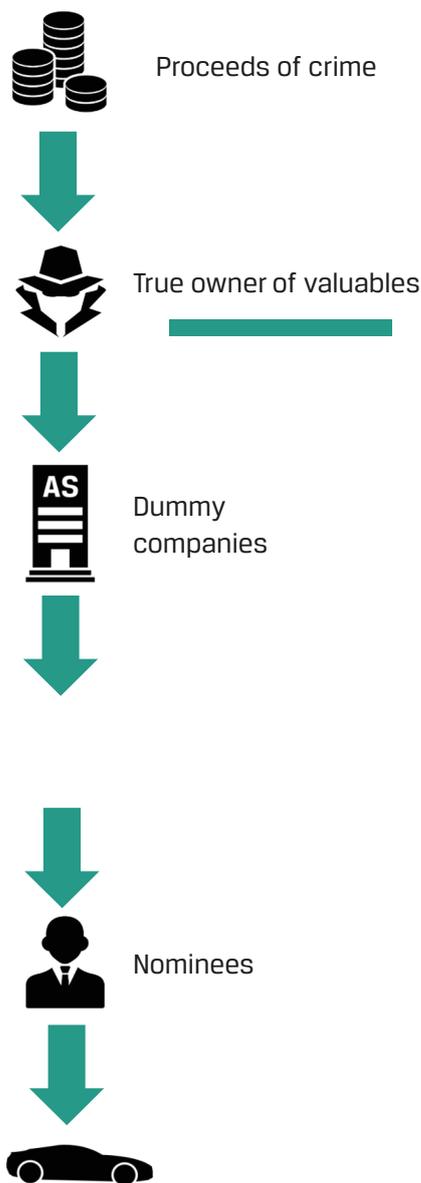
The following scenario describes how an implicated private individual uses a third-party provider to launder proceeds of crime. The person is trying to transfer the proceeds to his bank account. The money is first transferred to a third-party provider and then to his private bank account. In most cases, the bank will have limited information and possibility to detect and verify the funds' origin.



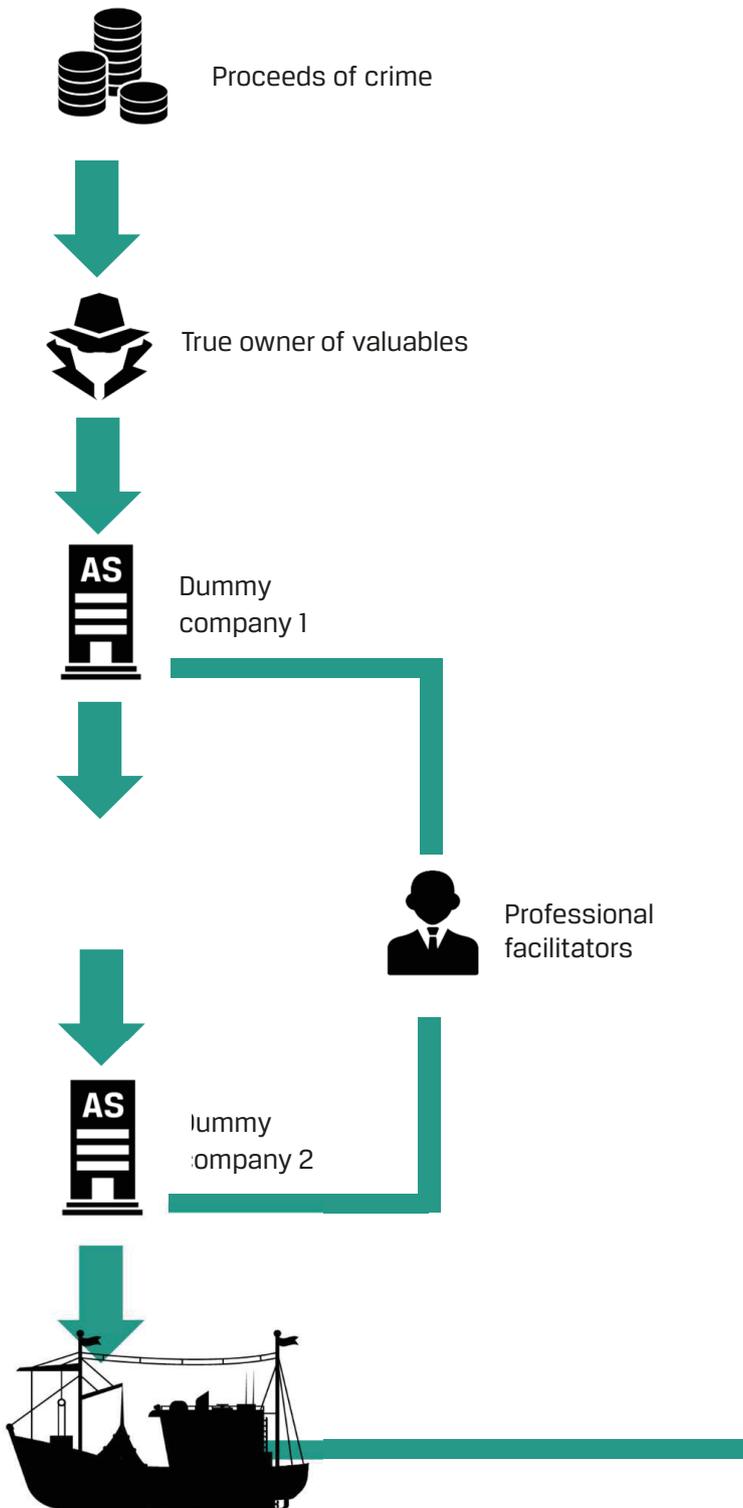
This shows how an implicated private individual transfers proceeds of crime directly to his bank account. The funds can then be transferred to an account the private individual holds with a third-party provider for storage, transfer to other private individuals or for spending. In this case, the money held with the third-party provider is used to purchase valuable items like watches, telephones and clothes. The funds are laundered through the purchase of valuables, and the bank has little chance of verifying the transactions' purpose and final destination.

Nominees and dummy companies

Nominees and dummy companies are private individuals and companies used in laundering proceeds of crime. These private individuals and companies intend to hide information about ownership and assets.



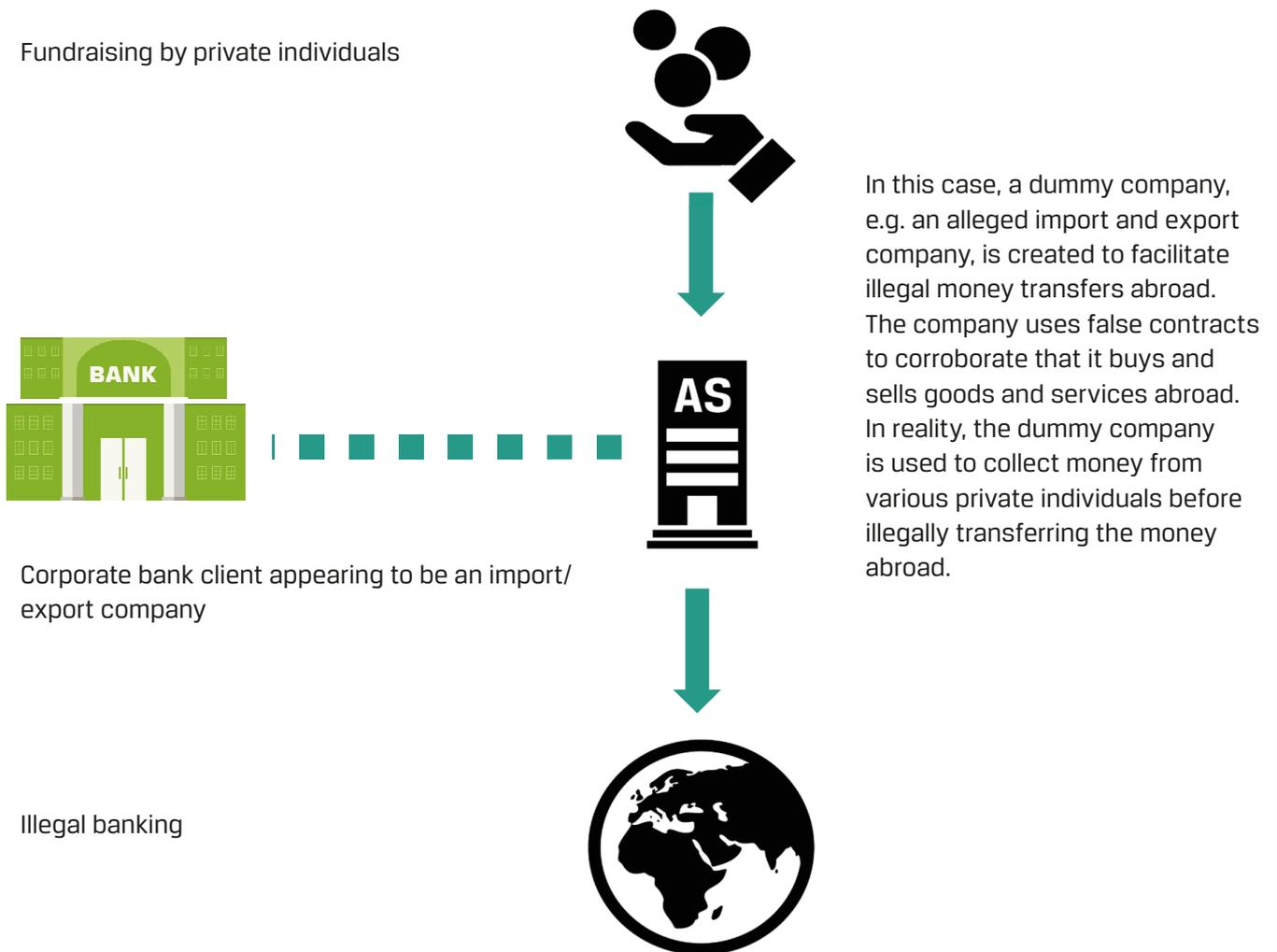
The illustration depicts a scenario in which both a nominee and a dummy company are used. The purpose is to conceal proceeds of crime by laundering them through the purchase of valuables. The scenario shows how a criminal in possession of illegal proceeds creates a dummy company that opens an account with a bank. The dummy company then uses nominees with fictitious employment contracts. Apparently, wages are paid to the nominee by the dummy company, but in reality the funds originate from the illegal proceeds. The nominee receives the money and purchases, e.g., an expensive car. The above-mentioned criminal is the true owner of the car, while the nominee is paid a fee for his services.



This illustration shows a scenario where structures are complicated through the use of several dummy companies and professional facilitators to conceal proceeds of crime. Unlike the previous scenario, several dummy companies are created. These companies may be newly established companies or companies belonging to a group of companies with a complex ownership structure. In this case, the criminal is helped by a professional facilitator to make fictitious contracts appear legitimate. The fictitious contracts refer to purchases of goods from dummy company 2 which are paid by dummy company 1. In reality, proceeds of crime are transferred to dummy company 2, which then uses the money to purchase, e.g., a sea-going vessel with the help of the professional facilitator. The vessel then becomes the property of the criminal.

Illegal payment services

The scenario below shows how an actor, on behalf of private individuals, transfers money abroad without licence. Both the volume of payments and total amounts indicate that the business is subject to licensing requirements.



4.2. Strategic analyses

In 2022, the FIU prepared an number of strategic analyses and contributed to the production of other strategic products in the other departments at Økokrim. The recipients of these strategic reports are mainly obliged entities.

Indicators – Circumvention of sanctions and foreign ownership of real estate in Norway

The list of indicators is meant as a guide to help prevent and uncover misuse of services provided by obliged entities and attempts to circumvent sanctions.



Annual Report 2021

The report provides an overview of the FIU's operations and output that year. The report also discusses the FIU's cooperation with the obliged entities.



2021 Trend Report

The report analyses and summarises the information submitted by the obliged entities.





Corruption – types and indicators

The report, with a list of indicators, provides an overview of MOs and types of corruption. The report was prepared by Økokrim's Corruption Team in collaboration with the FIU and a number of obliged entities.



Memo on mixing services

The FIU and Økokrim's Cryptocurrency and New Payment Methods Team prepared this memo as an aid for the obliged entities. The memo describes how mixing services operate and provides advice to obliged entities on how they should relate to clients who use such services.



NRA – National Risk Assessment

National Risk Assessment – Money laundering and financing of terrorism 2022 provides a comprehensive assessment of the risks facing Norway in these fields. The report was prepared by Økokrim and the FIU in collaboration with a number of obliged entities.



Theme report – Cash handling in shops

The report discusses cash handling services in shops based on received STRs.

5. Knowledge sharing and guidance

5.1. First quarter

5.1.1. JUC seminar

In order to strengthen anti-money laundering work, the FIU held a talk at a financial regulations seminar organised by the Judicial Education Center (JUC). The purpose of the talk was to inform about trends and MOs and to provide guidance on the many challenges that obliged entities face in their anti-money laundering efforts when dealing with cryptocurrencies.

5.1.2. Guidance on sanctions rules and the Anti-Money Laundering Act

After the Russian invasion of Ukraine and the Government's decision to implement sanctions against the Russian economy, the FIU has published updated information and guidance about the sanctions rules and how to act if one has customers who are affected by the sanctions and where there is suspicion of money laundering. In order to assist the obliged entities with such issues, a list was prepared with indicators of circumvention of sanctions and foreign ownership of real estate in Norway.

5.2. Second quarter

5.2.1. DSS seminar

Early in the second quarter, the FIU held a talk at a DSS seminar about anti-money laundering. DSS is a cooperation between nine savings banks which have established a joint anti-money laundering expert group. The purpose was to share information about indicators, trends and other developments in different crime areas and to give advice about particular challenges faced by local savings banks.



*Fagseminar anti-hvitvasking og terrorfinansiering 2022
Heidi Lesteberg and Mohammad Ahsen Qureshi Finance Norway's seminar in 2022.*

5.2.2. JUC - annual anti-money laundering course

The FIU was represented with a speaker at the JUC's annual anti-money laundering course. The course gave an update on key legislation. Key elements in risk and risk assessment were presented, in addition to an update on current risks within money laundering and financing of terrorism.

5.2.3. Finance Norway seminar

On 16 June, the FIU was present at Finance Norway's anti-money laundering seminar, where other public authorities also held talks about current issues, among them the Ministry of Foreign Affairs and the Police Security Service. The target group was employees of obliged entities, particularly in banking and finance, but also investigators, case handlers and others in the insurance industry whose remits include anti-money laundering. The seminar attracted over 400 attendants.

5.3. Third quarter

5.3.1. Guidance for estate agents

The FIU prepared a report with guidance for estate agents with the aim of improving the quality or the STRs submitted by the industry, particularly of what to report and what an STR should contain.

5.3.2. OSCE - the Organization for Security and Co-operation in Europe

The Organization for Security and Co-operation in Europe (OSCE) visited Norway in September. The OSCE showed particular interest in the FIUs work.

5.3.3. IMF (International Monetary Fund)

The International Monetary Fund (IMF) visited relevant authorities in Norway in autumn 2022. The purpose was to gain insight into the biggest threats facing Norway and the drivers of change in cross-border payments. The FIU met with representatives of the IMF to provide information about transaction flows in Norway.





5.4. Fourth quarter

5.4.1. The Laundry - Podcast

Early in the fourth quarter, the FIU was a guest on the podcast The Laundry's episode about "monitoring corporate transactions – how well does this work?", in which challenges and vulnerabilities were discussed.

5.4.2. Real Estate Norway seminar

In cooperation with Söderberg & Partners, Real Estate Norway held a seminar in October. The FIU held a talk presenting trends and MOs in the estate agent industry.

5.4.3. The Money Laundering Conference

The Money Laundering Conference was held at Clarion Hotel & Congress Oslo Airport on 17–18 November. The conference is organised by Finance Norway, the Financial Services Authority and Økokrim in conjunction. More than 900 attendants was a new record. It was also possible to attend parts of the conference digitally.



6. National collaboration

6.1. The Norwegian police

The FIU works with the police districts and the National Criminal Investigation Service to share information that can result in prosecution and confiscation. We have collaborated on a number of projects, among them a project to identify persons who order live distant child abuse (LDCA). Also, the FIU attended a seminar with the police's business sector contacts where the purpose was to share knowledge about the use of virtual currencies in money laundering and financing of terrorism.

The FIU has for many years worked closely with the Police Security Service to prevent and detect financing of terrorism. This cooperation was strengthened in 2022, when some of our employees were deployed to the PSS' offices. Working from the same location has already provided operational and knowledge-sharing benefits.

6.2. OPS AT

Cooperation between the private and public sectors to prevent money laundering and financing of terrorism – abbreviated OPS AT in Norwegian – was formally launched on 25 August 2021. OPS AT is a project launched under the auspices of the Public-Private Digital Interaction Programme (abbreviated DSOP in Norwegian). OPS AT was launched in order to strengthen cooperation between obliged finance institutions and relevant authorities, which in turn will strengthen Norway's ability to prevent and uncover money laundering and financing of terrorism. By sharing information about trends, challenges and risk-mitigation measures, the obliged entities and the authorities can provide a better and more targeted effort against money laundering and financing of terrorism.

The FIU is represented on the steering group, the core group and a working group on current trends and threats. The steering group adopts the overall strategy and framework for the cooperation while the core group identifies threats and assesses and prioritises measures which can improve cooperation in combating money laundering and financing of terrorism. The working group contributes expertise and knowledge on various topics and works to resolve specific issues. Relevant issues and topics will be presented to the core group and, if relevant, the steering group.

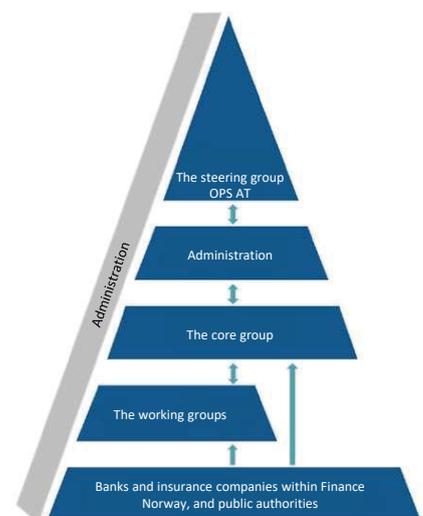


Figure 5: OPS AT management model.

6.2.1. STRs from large companies

The FIU has reason to believe that large companies can become better at reporting suspicious activity. OPS AT has therefore set up a project to look into this issue with an aim to improve understanding of relevant MOs and detection of suspicious activity by entities in this segment. The project is carried out in cooperation between select obliged entities and government agencies.

The project is limited to the shipping and fisheries industries, as they are considered to be at high risk of money laundering. Furthermore, the project is limited to large companies, as we assume that the MOs for laundering money in large companies differs from the MOs used by small companies. It is assumed that preventing money laundering in large companies will be socio-economically beneficial.

These are the project's aims:

Aim 1: Increase the banks' knowledge about how to investigate and report suspicious activity in the corporate market.

Aim 2: Contribute to uncovering more suspicious activity, e.g. with the use of lists of indicators.

Aim 3: Ensure good reporting to Økokrim and appropriate use of resources by the obliged entities. This can be done by evaluating the quality of the cases already reported.

6.3. The Contact Forum

The FIU represents Økokrim on the Contact Forum for Combating Money Laundering and Financing of Terrorism.

The Forum was created by Government decision in October 2014. Its purpose is to help ensure a coordinated national effort against money laundering, financing of terrorism and proliferation of weapons of mass destruction. The Forum is chaired by the Ministry of Justice and Public Security.

6.4. Supervisory authorities

Effective combating and prevention of money laundering and financing of terrorism and weapons of mass destruction require close collaboration between all involved authorities. Information sharing between the FIU and the supervisory authorities is essential for the various government

The main tasks of the contact forum

Help identify new threats and vulnerabilities through communicating threat and risk information prepared by the operational agencies.

Coordinate efforts to develop strategies and measures to meet threats and vulnerabilities, with a particular focus on cross-sector and cross-agency measures.

Coordinate efforts to update Norway's national risk assessment of money laundering and financing of terrorism.

Encourage development of procedures for collaboration between government agencies and between these agencies and the private sector.

Identify what developments in international legislation needs to be implemented in Norway.

Identify needs for research and strategic analysis work into money laundering and financing of terrorism.



agencies' ability to fulfil their tasks and for targeted supervision and follow-up of the obliged entities.

In the first quarter of 2022, the FIU invited all the supervisory authorities, the Financial Supervisory Authority, the Gambling Board and the Supervisory Council for Legal Practice, to a meeting. The purpose of the meeting was to improve cooperation.

Improved cooperation is also the subject of the bi-annual meetings between the FSA and the FIU, where we share information and experiences and discuss various issues within our respective anti-money laundering remits. These meetings are a supplement to the day-to-day operational cooperation where rapid clarifications and feedback are required. The FIU has in 2022 also prepared topical and intelligence reports for the FSA and proposed subjects for audits and supervision.

In 2022, the Gambling Board and the FIU signed a cooperation agreement for regular review of current MOs in gambling, discussion of issues related to the gambling legislation and exchange of information.

6.5. Regulatory authorities

A representative from the Tax Administration has been seconded to the FIU since autumn 2021. The purpose is to strengthen cooperation between the two organisations and to ensure good exchange of information.

Also, regular meetings are held throughout the year between the Tax Administration, the FIU and Økokrim's intelligence departments.

7. International cooperation

7.1. FATF

The Financial Action Task Force (FATF) is an international organisation established by the G7 countries in 1989. The FATF plays a leading role in the international effort to combat money laundering and financing of terrorism and weapons of mass destruction, and issues the international "FATF Forty Recommendations" standard. Large parts of the EU's and Norway's rules and regulations were first formulated in FATF's recommendations.

Despite the pandemic, the FATF has continued to maintain a strong focus on combating money laundering and financing of terrorism. The FATF carried out a number of country evaluations in 2022. A representative from Norway's FIU took part in the FATF's evaluation of Germany's AML & CTF efforts. The evaluation report was discussed and finalised at the FATF's plenary meeting in Berlin in June 2022.

The FATF has published a report on laundering proceeds from smuggling of migrants: "Money laundering and terrorist financing risks arising from migrant smuggling". It has also published reports on how technology can be used to detect suspicious transactions, carry out analyses and provide better understanding of associated risks. The standard for how to uncover and prevent the problems associated with hidden ownership has also been improved and strengthened, and a guide has been published for the estate agent industry's work against money laundering and financing of terrorism, and a guide on cryptocurrencies and the providers of these.

The FATF in 2022 also initiated a project directed at the trade in antiquities and other cultural objects for the purpose of money laundering and financing of terrorism. Økokrim, the FIU and the Ministry of Culture and Equality have participated actively in the project. The final report can be found on the FATF's, Økokrim's and the Ministry of Culture and Equality's websites.

FATF

The FATF was created in 1989

Norway has been a member since 1991

39 member countries

Independent international organisation

Combats money laundering and financing of terrorism

Prepares and updates the international standard «FATF Forty Recommendations»

Evaluates the member countries' money laundering regimes



7.2. Egmont Group of FIUs

The Egmont Group of Financial Intelligence Units (Egmont Group) is a global association of 166 FIUs⁹. In addition, a number of international organisations have status as observers. The purpose is to combat money laundering and financing of terrorism, and associated crime. The FIU has been a member of the Egmont Group since 1993. The members of the Egmont Group work to realise the aims laid down in the Egmont Group's Charter and Principles for Information Exchange, and are obliged to cooperate and share information with the other FIUs in the groups and attend the Egmont Group's plenary meetings and other activities.

7.3. Participation in international meetings

In spring 2022, the FIU attended the annual meeting of Nordic FIUs in Iceland. The purpose of the meeting was to share experiences and discuss common challenges.

During last year, the FIU has attended the Egmont Group's plenary meeting in Riga and four EU FIU Platform meetings. The purpose of these meetings is to review joint projects and discuss issues related to money laundering and financing of terrorism. The Egmont Group has also held a number of webinars for FIUs about various subjects within money laundering and financing of terrorism in 2022. Also, several guides and theme reports on e.g. trade-based money laundering¹⁰ have been published.

The Norwegian, Swedish and Danish FIUs have identified common challenges and have launched a joint project to meet them. The FIU has actively exchanged information with other FIUs in connection with this project, and a joint report is being prepared which will be forwarded to Europol and relevant recipients in Norway, Sweden and Denmark.



⁹ <https://egmontgroup.org/about/>.

¹⁰ Trade-based money laundering takes place by concealing and misreporting prices, quantities and qualities when importing and exporting goods (NRA 2022).

8. STR statistics

8.1. Source data

The statistics presented in this chapter are based on information extracted from STRs submitted to Økokrim in accordance with the Act relating to Measures to Combat Money Laundering and Terrorist Financing etc. The data are from the period 01.01.2018–31.12.2022. Chapter 8.7 presents extracts from the source data for selected crime areas. The extracts are found by searching for specific terms in the STRs' description of the reason for the reporting. The data subsets for these crime areas will not be 100 per cent correct, but they nevertheless give an indication of current trends.

Please note that some of the source data will change in the course of the year due to statutory deletion, error correction and updates.

8.2. Submitted STRs

The number of STRs submitted by the obliged entities has increased steadily over the last five years (see figure 6). The FIU received 10,748 STRs in 2018. In 2022, that number had risen to 19,783. From 2021 to 2022, the number of reports increased by approx. 20%.

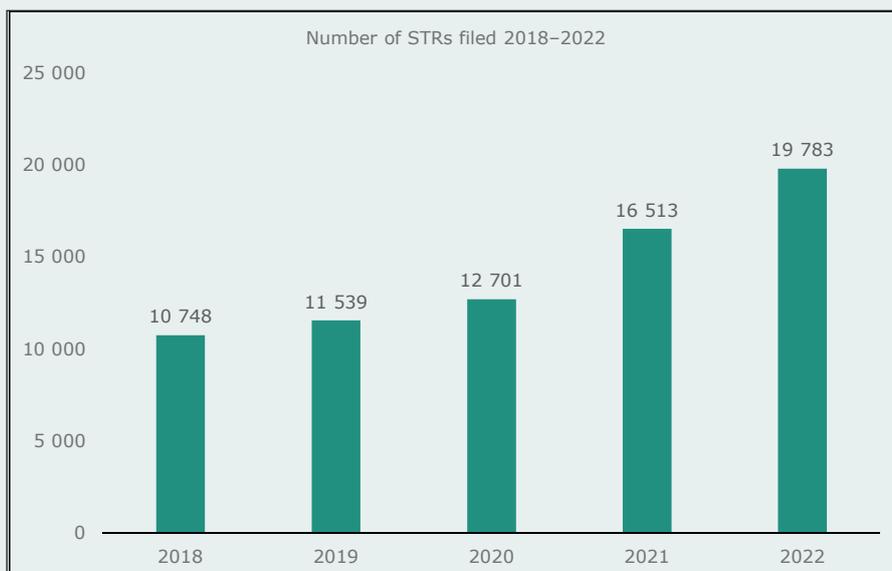


Figure 6: Number of submitted STRs 2018–2022.

8.3. Reporting industry groups

The Anti-Money Laundering Act (AMLA) divides the reporting entities into 22 industry groups, and these groups are then divided into sub-groups in the Altinn reporting form.¹¹

The industries which submitted most STRs in 2022, were banks, followed by brokers, mainly estate agents, and payment service providers. For the first time, estate agents surpassed payment services – by 0.1%. After banks, the industry to submit the most STRs has previously been payment services.

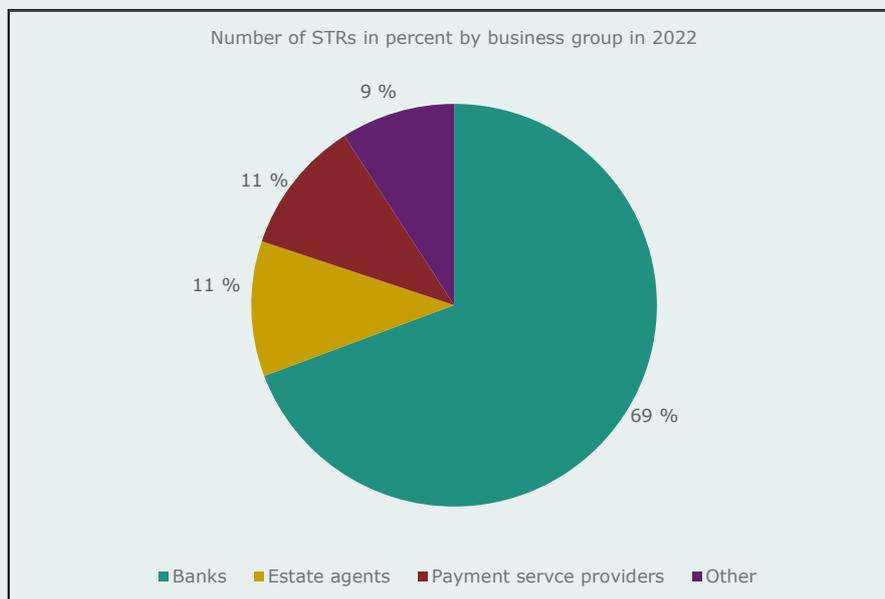


Figure 7: Number of STRs in per cent by industry group in 2022.

Figure 7 shows that the three groups which submitted the most reports in 2022, were banks, estate agents and payment service providers. Banks submitted 69% of STRs, estate agents 10.9% and payment service providers 10.8%. The group "others" consists of electronic money businesses, securities dealers, legal professionals, auditors, accountants, insurance companies and others cf. AMLA section 4. This group contributed 9% of all submitted STRs in 2022. In the group "others", more than half of all STRs were submitted by the sub-group "others cf. AMLA section 4". This sub-group consists mainly of online exchange and storage services and other finance and credit institutions.

¹¹ The industry groups are: legal professionals, others cf. AMLA section 4, banks, electronic money businesses, traders in goods, insurance companies, brokers, pension funds, mail service providers, accountants, auditors, securities dealers and payment service providers.

8.4. Obligated entities

A total of 574 unique entities submitted STRs in 2022, 56 more than in 2021. On average, the number of unique entities has increased by 40 each year since 2018. The increase is mainly due to more estate agents submitting STRs than before.

Estate agents and banks were the two industry groups with most unique entities in 2022, followed by accountants (figure 8). There were 235 unique estate agents, 141 unique banks and 80 unique accountants. Estate agents showed the largest increase in 2022, up 30 from 205 unique entities in 2021. Even though the number of accountants and estate agents is high, the number of STRs submitted by each entity is, on average, lower than the number for banks and payment service providers.

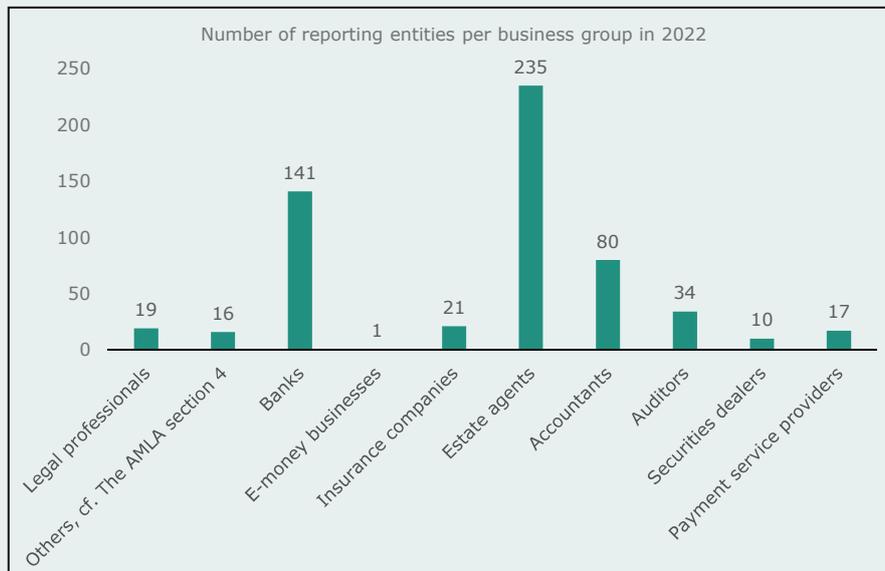


Figure 8: Number of unique entities by industry group in 2022.

8.5. Reporting time

Figure 9 shows the number of days it takes from an obliged entity has carried out a transaction to an STR is submitted¹². Most STRs are submitted 2–30 days after a transaction has gone through. We quote from the FSA's guide to the AMLA: "In order to fulfil the statutory obligation to report suspicious activity, it is necessary to investigate indications of money laundering and financing of terrorism in a timely manner. As a general rule there should be no backlog of suspicious activity pending investigation. Investigation should be initiated without undue delay, i.e. within two days. Even though investigations are launched without delay, they may take time to carry out. In such cases, an STR must be forwarded to Økokrim immediately after the obliged entity has concluded that the suspicion is not unfounded."

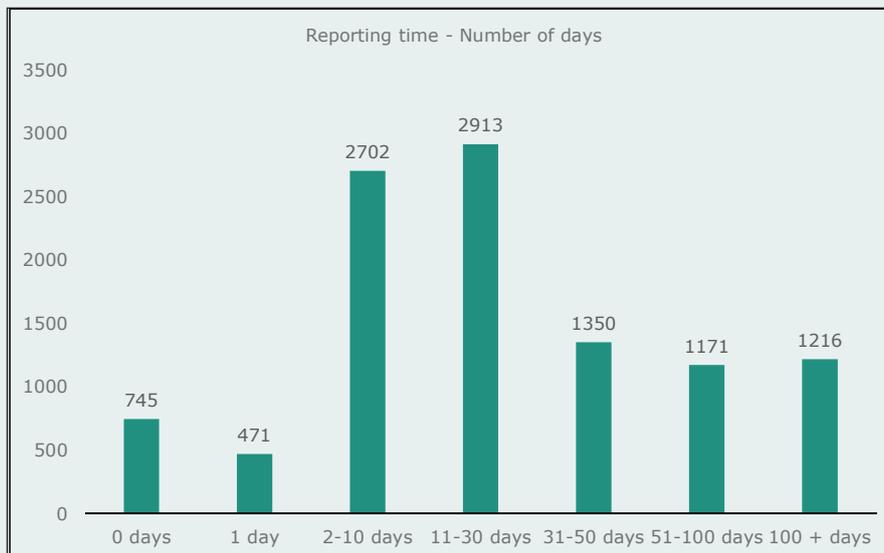


Figure 9: Reporting time in 2022.

¹² Reporting time is calculated as follows:

- The starting point is the most recent transaction (most recent date).
- Calculation: Number of days from date of last transaction to the STR's time stamp.
- If the STR contains no transaction, or no dated transaction, it will not be included.
- For STRs which report future (planned) transactions or which report the suspicious activity on the day of the transaction, the number of days is set to zero.

8.6. Suspicion codes

When filing STRs, the reporting entities can categorise their suspicions by ticking relevant codes (Altinn reporting form item 4.3). Entities can tick more than one box in an STR.

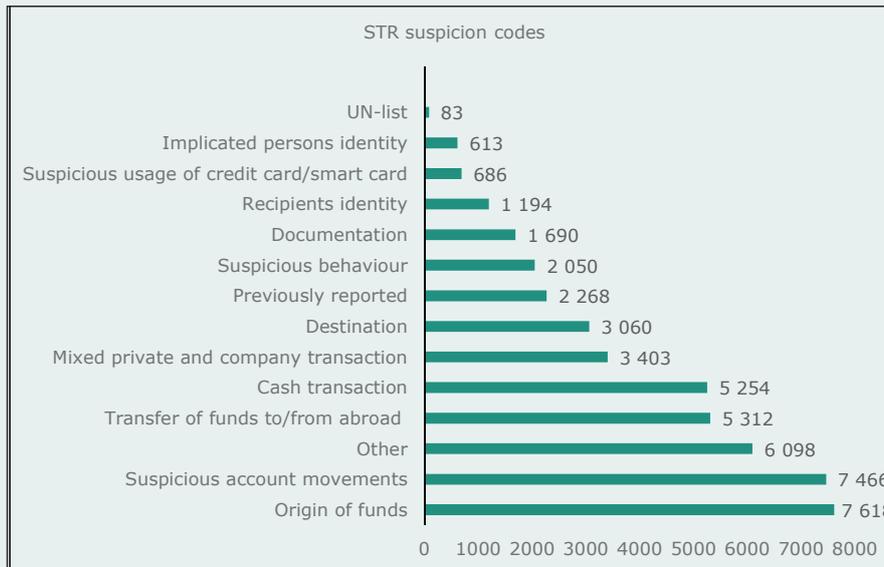


Figure 10: Suspicion codes used in STRs in 2022

Figure 10 provides an overview of the suspicion codes used in STRs in 2022. Different industry groups use different suspicion codes. There was an increase in the use of all suspicion codes compared with 2021, except transfer of funds to and from abroad, which saw a reduction of 660 from the year before. Origin of the funds was the most used code in the STRs submitted in 2022, closely followed by suspicious account activity and other. These are the same top three as the year before and in the same order.

8.7. Crime trends

The FIU has prepared an analysis of trends in select crime areas which have stood out in 2022:

8.7.1. Suspicion of financing of terrorism

When filing STRs, the reporting entities can tick a box for suspicion of financing of terrorism (Altinn reporting form item 4.4).

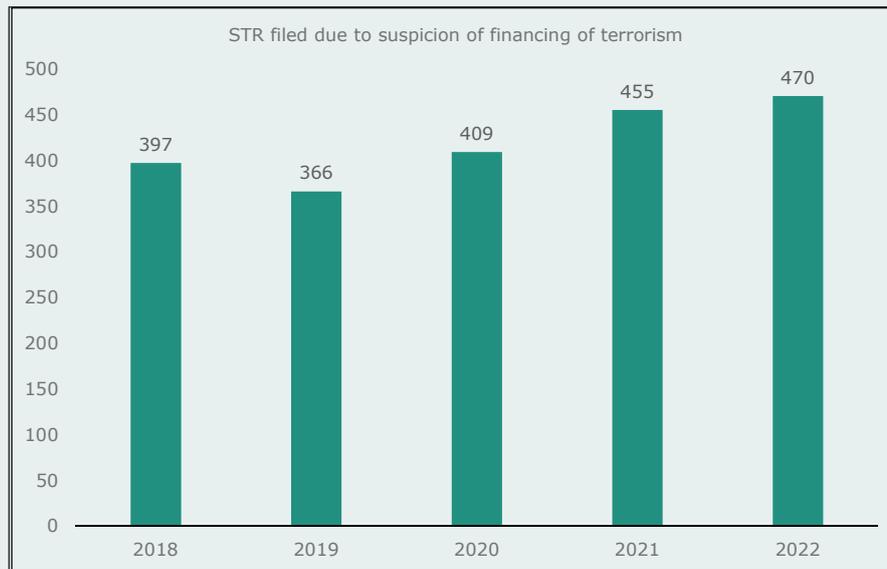


Figure 11: Number of STRs submitted on the basis of suspicion of financing of terrorism per year 2018–2022

Figure 11 provides an overview of the number of STRs submitted on the basis of suspicion of financing of terrorism per year 2018–2022. It shows that the number of STRs submitted on suspicion of financing of terrorism fell in 2019 only to rise in subsequent years. In 2022, the majority of the STRs submitted due to suspicion of financing of terrorism was submitted by banks, 86%. Payment service providers submitted 3% of these reports and the other groups the remaining 11%.

8.7.2. Suspicion of tax fraud and exploitation of workers

During the period 2018–2022, 3762 STRs were submitted due to suspicion of tax fraud and exploitation of workers. The numbers for STRs relating to tax fraud and exploitation of workers were extracted using predefined search criteria for industries and amounts. For this reason, not all STRs relating to tax fraud and exploitation of workers are included and it is likely that the actual numbers are higher than this statistic indicates.

Nevertheless, figure 11 shows that the numbers stayed relatively stable at around 600–700 during the period 2018–2020 before rising. Among the industry groups, banks, both commercial and savings banks, reported most suspicions of tax fraud and exploitation of workers in 2022.

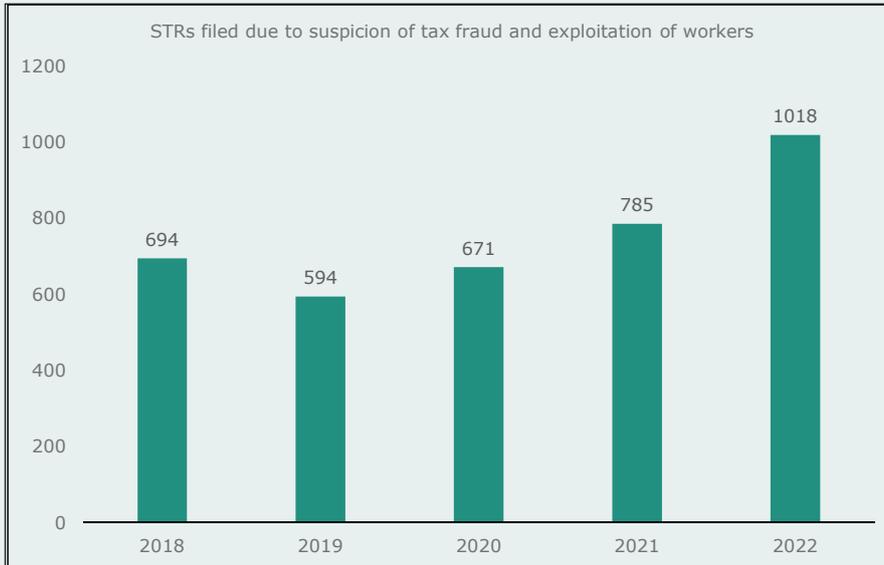


Figure 12: Number of STRs submitted due to suspicion of tax fraud and exploitation of workers per year 2018–2022

8.7.3. Suspicion of fraud and money mule activity¹³

From 2018 to 2022, 10,841 STRs were submitted on suspicion of fraud and money mule activity, and we see a significant increase. From 2021 to 2022, the number of reports increased by more than 50%. The explanation may be an increase in fraud during the pandemic. Banks, both commercial and savings banks, submit most STRs grounded in suspicion of fraud and money mule activity, followed by the group others cf. the AMLA section 4, of which cryptocurrency exchanges make up a large share after they were made obliged entities.

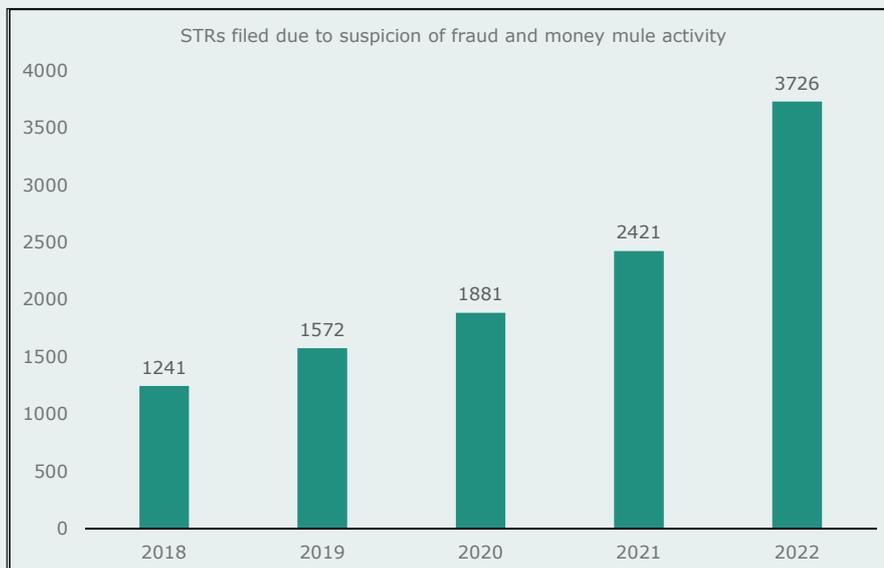


Figure 13: Number of STRs submitted on suspicion of fraud and money mule activity per year 2018–2022

¹³ A money mule is a person who receives money from one person and then transfers the money to a second person (either electronically or in cash).

8.7.4. Suspicion of sexual offences against children

During 2018–2022, 1651 STRs were submitted on suspicion of sexual offences against children. The number of reports has shown a steady increase, but it was markedly higher in 2021. In 2022, payment service providers submitted half of the total number of STRs submitted due to suspicion of sexual offences against children versus 66% in 2021. This change may be due to the banks increasing their share of the total, from 32% in 2021 to 43% in 2022.

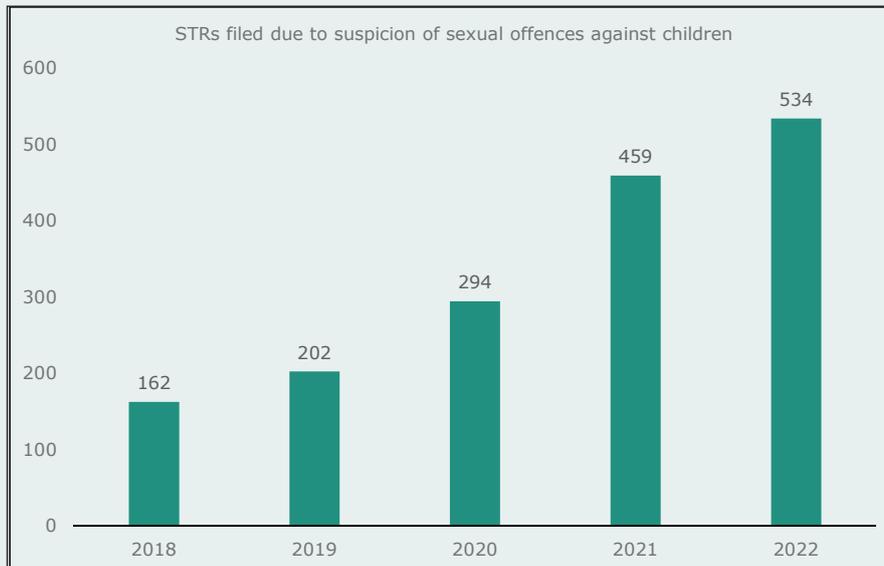


Figure 14: Number of STRs submitted on suspicion of sexual offences against children per year 2018–2022

8.7.5. Suspicion of fraud and exploitation of Covid-19-related support schemes

From 2020 to 2022, 708 STRs have been received on suspicion of suspected Covid-19-related violations¹⁴. Most reports were received in 2021. STRs are mainly submitted due to suspected abuse of publicly funded support schemes established in connection with the pandemic, sale of non-approved protection gear and fraud of individuals. Banks, both commercial and savings banks, submitted the most Covid-19-related STRs in 2022, followed by estate agents and others cf. the AMLA section 4.

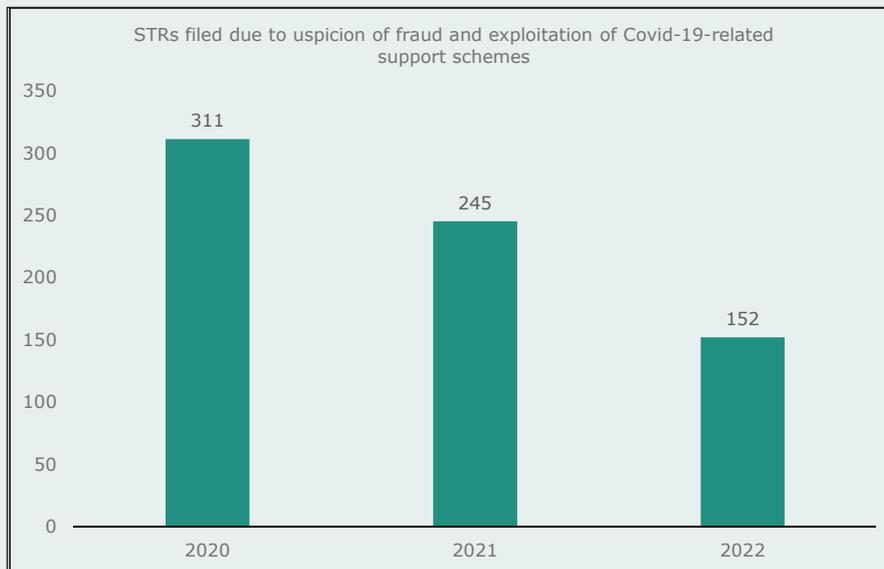


Figure 15: Number of STRs submitted on suspicion Covid-19-related violations per year 2020-2022

¹⁴ Note that the data has been extracted using search terms, and that the true number is likely to be somewhat higher than indicated by the statistic.

8.8. Who are reported?

8.8.1. Number of private individuals and organisations

Figure 17 shows the number of private individuals and organisations mentioned in STRs each year. These are individuals and organisations who, directly or indirectly, are linked to the suspicious activity reported. From 2018 to 2022 the numbers total 155,712 individuals and 29,614 organisations¹⁵. The number of private individuals mentioned in the STRs increased by 33% in 2021 and stayed at the same level in 2022. The number of organisations has increased gradually.



Figure 16: Number of private individuals and organisations mentioned in STRs each year 2018–2022.

¹⁵ Note that there are duplicates and that the same person or organisation may be reported every year.

8.8.2. Implicated private individuals and organisations

In the present reporting form, the obliged entity indicates whether they believe that a private individual or organisation is implicated in the suspicious activity. To be implicated means to play a key role in the suspicious activity.

The number of implicated private individuals and organisations has increased by 47% and 107%, respectively, from 2018 to 2022¹⁶. The share of implicated organisations stays steady at just under 10% of the total number of STRs. In 2022, their share was 9.5%.



Figure 17: Number of implicated private individuals and organisations in STRs each year 2018–2022.

¹⁶ Note that there are duplicates and that the same person or organisation may be reported every year.

8.8.3. Age of implicated private individuals

Private individuals implicated in STRs in 2022, were mostly in the 30–49 age group. This age group made up approx. 66% of the total, of which 25% were in the 30–39 age group and 21% in the 40–49 age group. The 50 and up age group made up 33%, with 17% in the 50–59 age group and 16.5% in the 60 and up age group. Persons under 30 made up 17% of the total number of implicated persons, and they were mainly in the 20–29 age group.

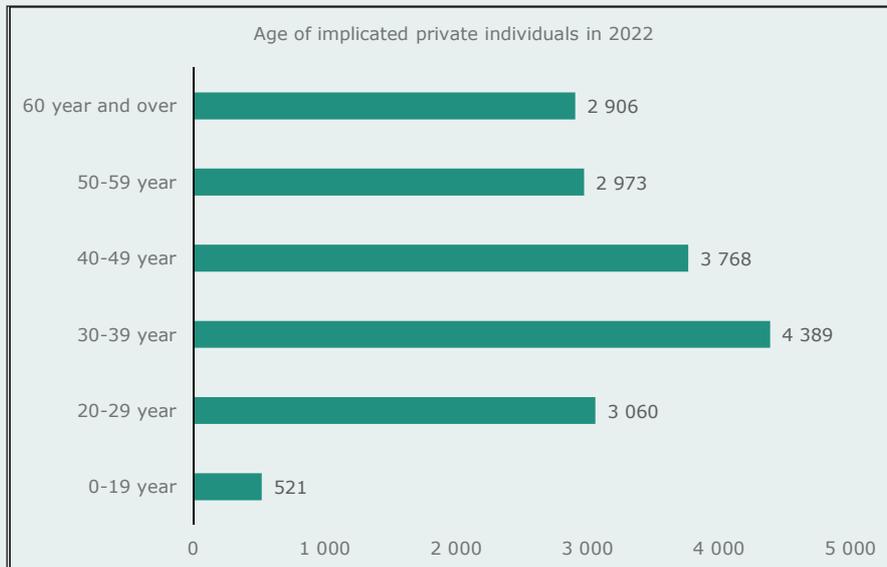


Figure 18: Private individuals implicated in STRs in 2022, by age group.

8.8.4. Nationality of implicated private individuals

Figure 19 shows how the nationality of the implicated persons in 2022 was distributed over 110 different nationalities. In 2021, that number was 106. Norwegians made up 75% of all implicated persons. Swedish and Polish nationals were the second-most represented groups, both at 3 percent, followed by Syrian, Lithuanian and Romanian nationals, at 2% each. Other nationalities made up the remaining 14%.

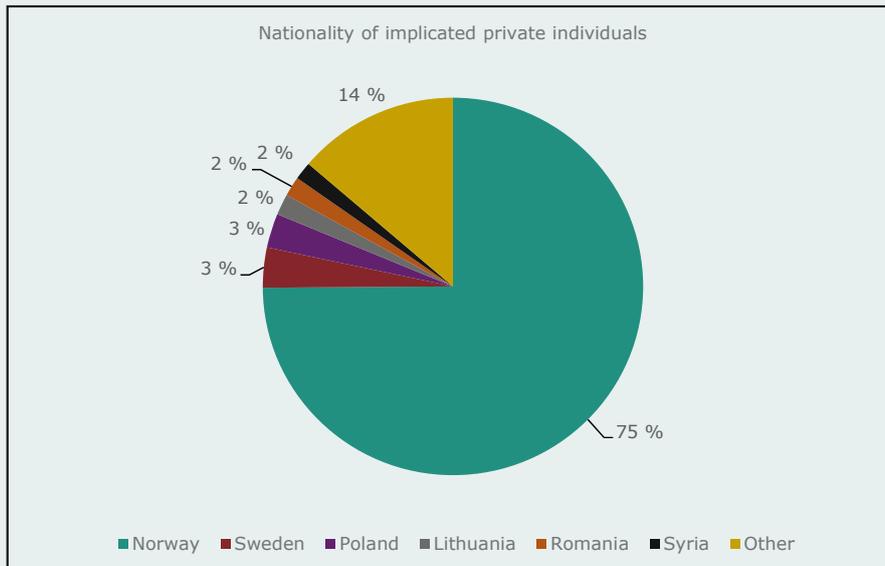


Figure 19: Private individuals implicated in STRs in 2022, by nationality.

8.8.5. Implicated organisations – industry codes

Implicated organisations are registered with industry codes in the companies' register. An organisation's industry code reflects its main business activity and is determined using the Norwegian industrial classification standard¹⁷. In 2022, 75 different industry codes were represented among implicated organisations, an increase of 12 from 2021. Figure 21 shows the 10 most reported industry codes in STRs in 2022. The industry code "Real estate activities" was the most frequently reported, with 288 STRs, followed by "Construction of buildings".



Figure 20: Number of implicated organisations by the most frequently reported industry codes in 2022

¹⁷ <https://www.ssb.no/virksomheter-foretak-og-regnskap/nace>.

Økokrim

PO Box 2096 Vika, 0125 Oslo

Tel. no.: +47 23 29 10 00

Email: post.okokrim@politiet.no