
# Annual Report 2021

Financial Intelligence Unit

**The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim)**
PO Box 2096 Vika, 0125 Oslo
Tel. no.: +47 23 29 10 00
**Email: post.okokrim@politiet.no**

# Preface

The Financial Intelligence Unit (FIU) received 16,513 suspicious transaction reports from obliged entities in 2021. This is a substantial increase from 2020 (12,701) and, if the reporting from other FIUs is included, means that the number of reports has doubled since 2016.

The reports constitute a key element in the effort to prevent and combat money laundering and financing of terrorism. In our opinion, the increase referred to above shows that the awareness of and attention given to money laundering and financing of terrorism has increased significantly among the obliged entities. Experience has shown that data and information relating to financial circumstances generated by the reporting regime are crucial in uncovering and investigating serious crime.

More cooperation and interaction with the obliged entities is, in our opinion, an important factor in successful combating of financial crime. We are therefore very pleased with Finance Norway's initiative to establish a collaboration between the private and public sectors to combat money laundering and financing of terrorism (Norwegian: Offentlig Privat Samarbeid – antihvitvasking og terrorfinansiering, abbreviated OPS AT), see page 45. We are strongly committed to the success of this important project and will use this collaboration as a key measure in our efforts to achieve better and more targeted communication and exchange of experience with the obliged entities. The information packages about Black Wallet and Cryptocurrencies prepared and distributed by us have been well received, and we envision such guidance and sharing of experience becoming an important element in our collaboration with the obliged entities going forward.

Throughout 2021, we have worked with issues relating to development and production of a new reporting solution in the new Altinn portal. In this connection, we are very grateful for the positive and useful feedback we have received from the obliged entities. Our aim is to launch a fit-for-purpose, flexible and timely solution that will, to a far greater extent than is currently the case, meet the demands both the reporting entities and we have for such a tool. Work on this project will be prioritised going forward.

In order to handle the significant increase in the amount of information we receive, in 2021 we launched a project to develop new analysis functionality in the Ask money-laundering database in cooperation with experts at the Police ICT Services. This will rationalise selection and prioritisation of what information and which reports should be followed up and worked on.

Our activities and intelligence production have been and are risk-based, and follows up on the key government directives relating to crime-fighting priorities. The product and format are guided by who the intended recipient is and the use to which the information will be put. Our main investigation-related activity will therefore remain production of intelligence products for local and national police units, supervisory authorities and international partners.

In spite of two years of pandemic and major problems facing both individuals and society, the amount of reporting and our contact with the reporting entities via telephone conversations, email exchanges and digital conferences and lectures, show that the commitment and eagerness to prevent and combat this type of crime remains strong. This gives reason for optimism and show that together, we can make a significant and important difference.

**Sven Arild Damslora**
*Head of FIU*

# 2021 Highlights

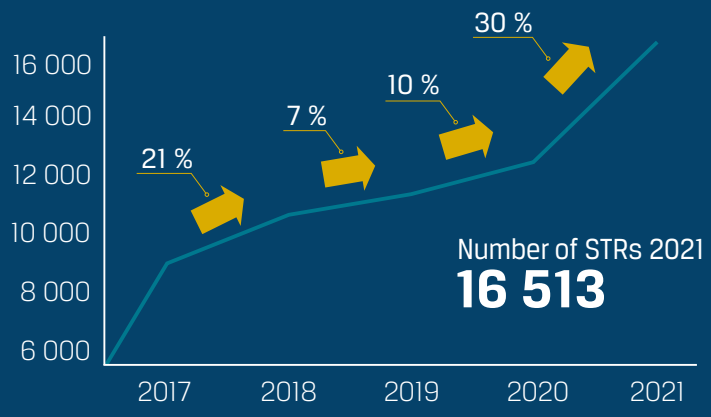
Financial Intelligence Unit – Norway

## Production and dissemination of information

| | |
|---|---|
| Intelligence products and criminal cases | 1 428 |
| Persons | 36 296 |
| Organisations | 1 784 |
| Requests for information answered | 771 |
| Freezed transactions | NOK 30 915 031 |

## Suspicious transaction reports 2021

| | |
|---|---|
| Banks | 67 % |
| Payment service providers | 16 % |
| Real estate agents | 11 % |
| Others | 6 % |




## Nationalt & international cooperation

**National**

OPS AT

Contact forum

Supervision

Supervisory authorities

**International**

FATF

EGMONT Group of FIUs

EU FIUs Platform

# Contents

**1. Introduction ..... 6**
1.1. The organisation of the FIU at Økokrim ..... 6
1.2. The FIU – roles and functions ..... 7
**2. The reporting process/Handling of STRs ..... 10**
**3. Suspicious transaction reports (STRs) ..... 12**
3.1. Source data ..... 12
3.2. Suspicious transaction reports filed ..... 12
3.3. Business groups which submit STRs ..... 13
3.4. Reporting entities ..... 14
3.5. Suspicion codes ..... 15
3.6. Crime area trends ..... 18
3.7. Who are reported? ..... 26
3.8. Reported organisations ..... 30
3.9. Freezing transactions ..... 31
**4. Communication ..... 32**
4.1. Implicated persons and organisations ..... 32
4.2. Other exchange of information etc. ..... 32
**5. Operational analysis ..... 33**
**6. National collaboration ..... 37**
6.1. OPS AT ..... 37
6.2. The Contact Forum ..... 38
6.3. Supervision ..... 39
6.4. Supervisory authorities ..... 39
**7. International cooperation ..... 41**
7.1. FATF ..... 41
7.2. EGMONT Group of FIUs ..... 41
7.3. The EU FIU platform ..... 42
**8. Guidance, supervision and communication ..... 43**

# 1. Introduction

## 1.1. The organisation of the FIU at Økokrim

In 2021, Økokrim, the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime, underwent a reorganisation that also included the Norwegian Financial Intelligence Unit (FIU). The FIU is, together with the functions/disciplines intelligence and prevention, part of the Intelligence and Prevention Department (see figure 1).

We believe this organisation and a close and positive cooperation, in particular with the rest of the Økokrim intelligence community, will see more and better use of the information generated by the reporting regime.

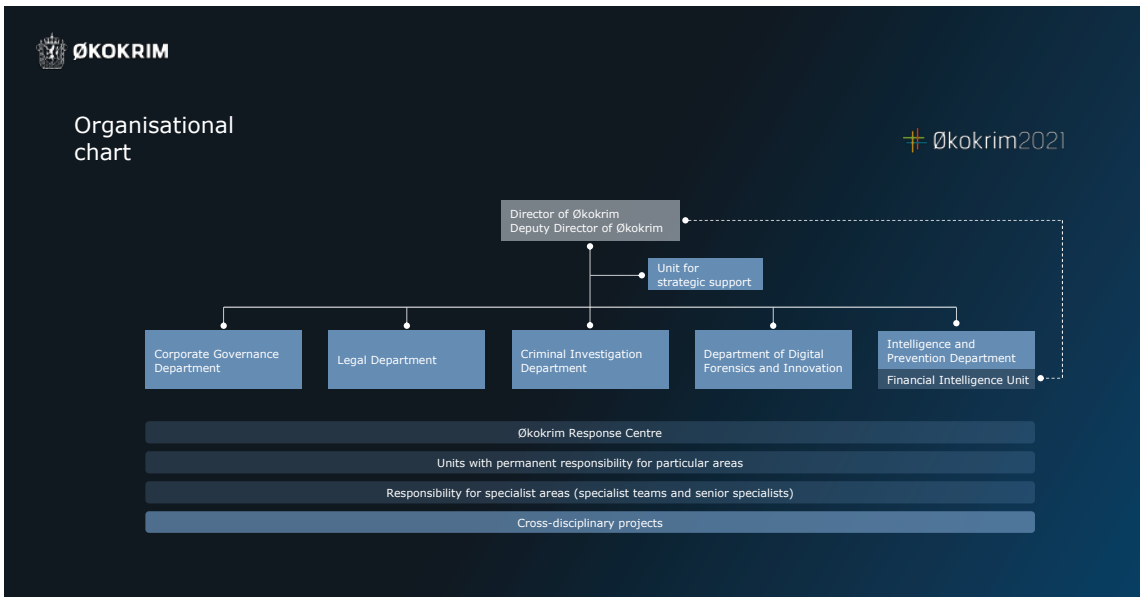



*Figure 1: Økokrim organisational chart*

At the end of 2021, the FIU had 20 employees, of which two-thirds worked with investigative and operational analysis, as well as communication and international cooperation with other FIUs. FIU employees are primarily recruited from the police, the tax authorities and the customs service. Our contact with the obliged entities mainly takes place via three staff members at the FIU's compliance function. The Unit also has employees with IT and legal expertise.

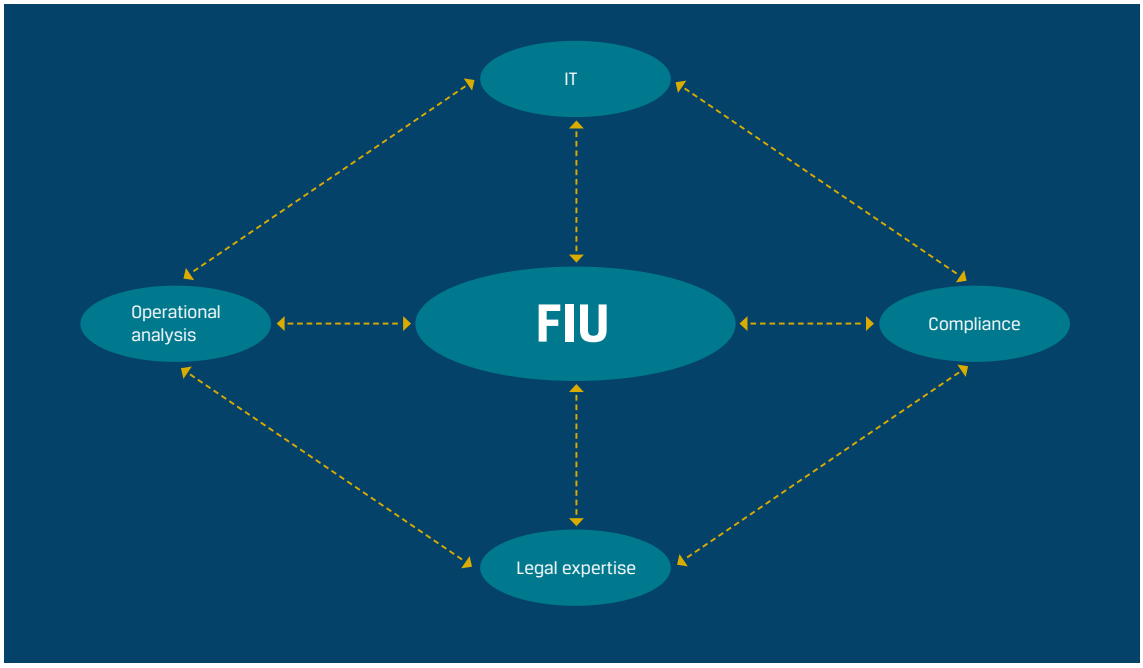



*Figure 2: Organisation – FIU.*

## 1.2. The FIU – roles and functions

According to international recommendations, guidelines and legislation, cf. article 32 of the EU's 4th Anti-Money Laundering Directive, members must establish national Financial Intelligence Units as part of the national efforts to prevent money laundering and financing of terrorism. In Norway, this unit has been placed under Økokrim. The Norwegian FIU will be organised and operate to discharge the national and international duties of an FIU.

Nationally, the FIU's primary and general function is to receive suspicious transaction reports (STRs) from obliged entities under the Anti-Money Laundering Act. This means processing, enriching and analysing this information and communicate it to police, supervisory authorities, as well as international partners.

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

### 1.2.1. Priorities and activities


*Figure 3: Priorities –FIU*

**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 we must perform, and we are constantly measured against how we perform them. Our international tasks and functions take up one-fourth of the FIU's resources. The draft for the 6th Anti-Money Laundering Directive, in its current form, will require significantly increased activity in this area.

**National legislation – the Anti-Money Laundering Act and the Police Databases Act:**
Økokrim, represented by the FIU, is data controller for the money-laundering database Ask and must ensure that current privacy and confidentiality legislation is complied with in the processing of information entered on the database. This also entails a responsibility for deletion of data, handling of requests for access etc. While the first two levels are mainly aimed at functions, roles and tasks, the next levels are more geared towards definition of crime areas, vulnerabilities and threats. It is always a fundamental principle that the FIU's activities, operations and intelligence production is based on a running assessment of the risk posed by money laundering and financing of terrorism.

**National directives:**
The Government and other authorities have issued national directives and defined national priorities which must be taken into account when preparing strategic and investigative analyses and intelligence products. One example in this regard is the Government's prioritisation of tax fraud and exploitation of workers.

**The directives of the police and the Director of Public Prosecutions:**
The directives and prioritisation orders of the National Police Directorate and the Director of Public Prosecutions highlight specific crime areas which the police and the prosecuting authority must give particular attention to and prioritise. This may include both national projects aimed at criminal networks and organised crime, and cases or matters involving serious sexual crimes, internet-related sexual abuse and financial ICT-related crime such as fraud, ID theft, computer intrusion etc.

**The risk situation in Norway:**
The National Risk Assessment, the threat assessments of the Police Security Service and other national threat and risk assessments also impact our decisions when prioritising analyses and allocation of resources for various tasks and requests etc.

**Priorities – FIU:**
In addition to the elements described above, we are also attentive to cases where there is a potential for seizing proceeds of crime and prioritise cases and areas where our information is unique and in particular demand, and where we see that this information may make a significant difference as regards prevention of crime and solving cases.

## 2. The reporting process/Handling of STRs

All reports and the information about objects (persons and/or organisations) contained in the reports are automatically processed, enriched and searched against police databases and a number of external sources. We also have various automatic and manual processes which can be used to decide and prioritise which STRs and what information to use in various projects and analyses. Our activities must be risk-based and take into account key directives as regards which crime areas our analyses and products should primarily be aimed at. In this connection, it is important to be aware that our current IT solution automatically transfers and makes available information from the STRs in the police intelligence database, subject to given parameters and rules. Furthermore, the reporting process in Norway may differ from other jurisdictions. Norwegian legislation allows for reporting of several transactions in a STR. Therefore, a single STR may contain several suspicious transactions.

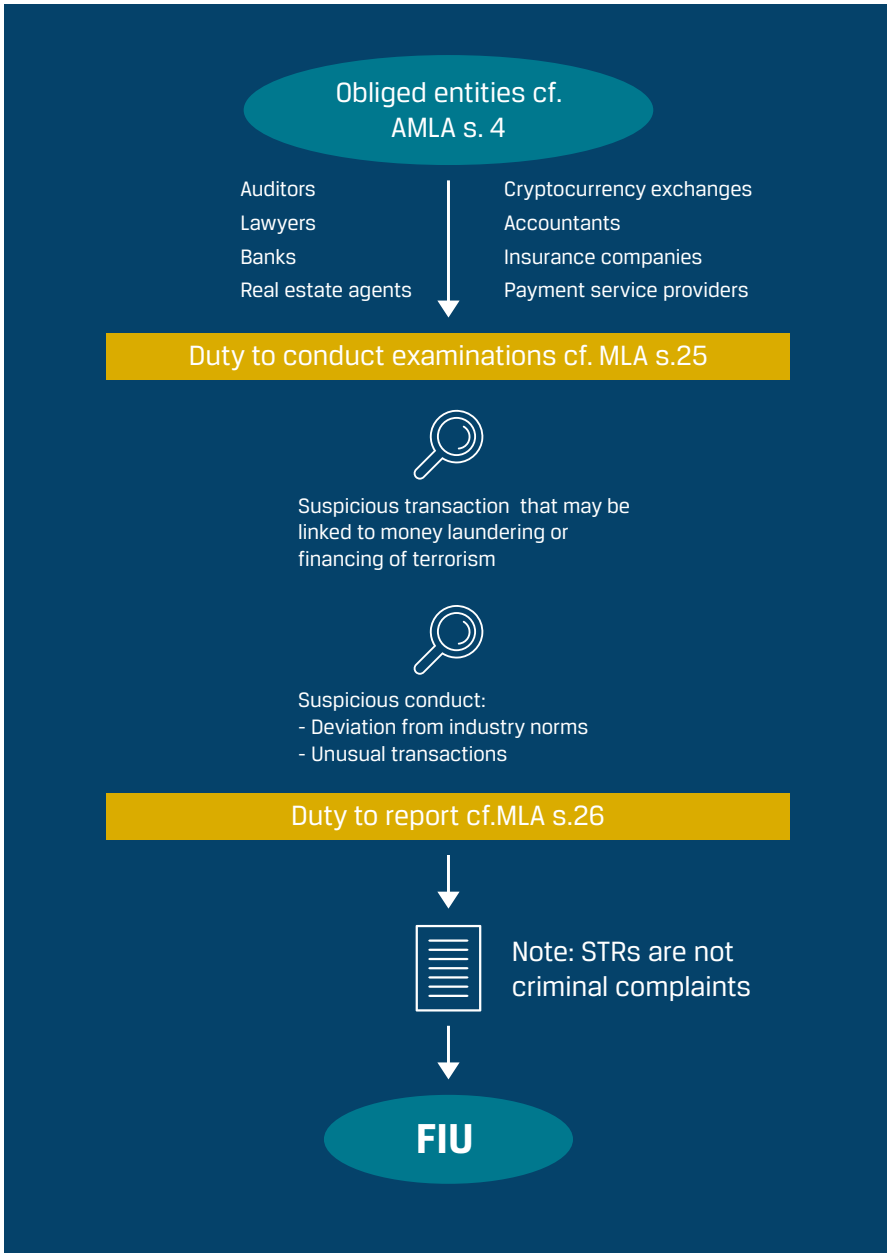



*Figure 4: The reporting process*

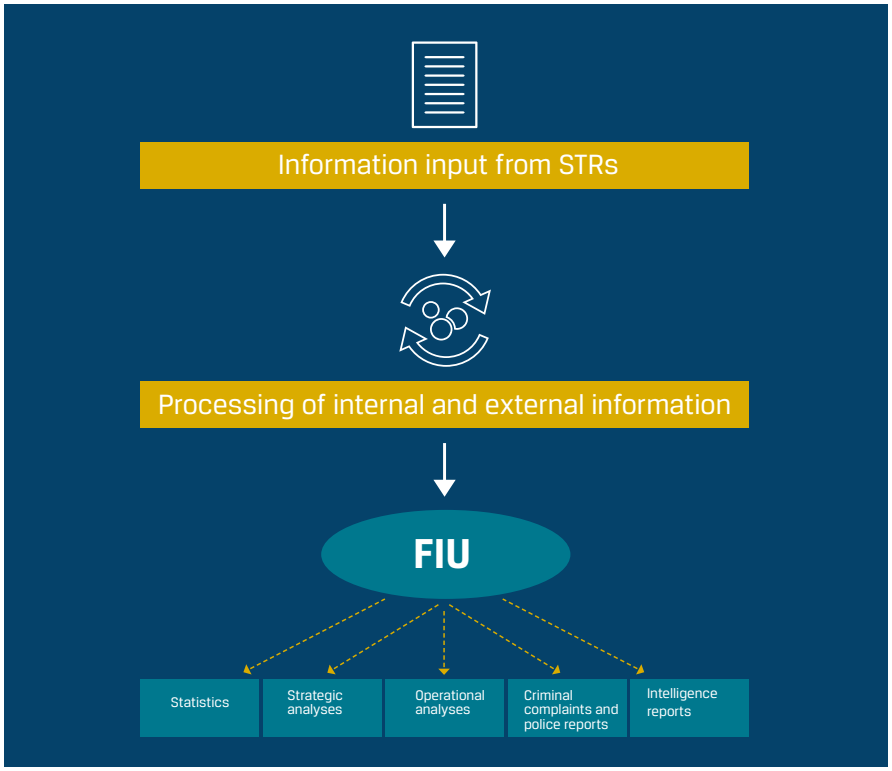



*Figure 5: The reporting process*

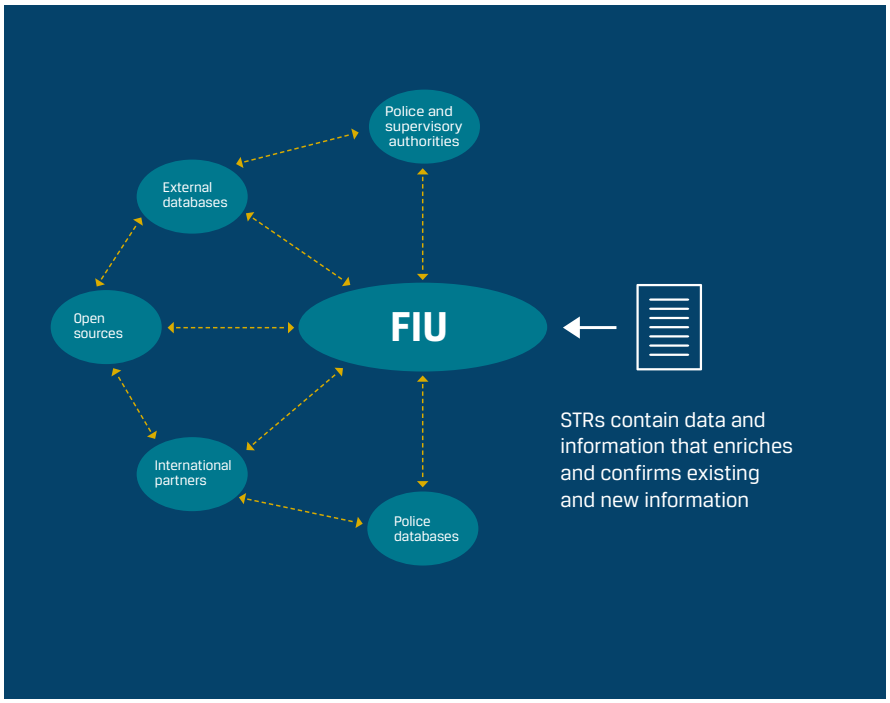



*Figure 6: The reporting process*

# 3. Suspicious transaction reports (STRs)

## 3.1. Source data

The data that forms the basis for the analysis is information from suspicious transaction reports (STRs) submitted to Økokrim under the Act relating to Measures to Combat Money Laundering and Terrorist Financing (the Anti-Money Laundering Act). The data underlying this report was mainly obtained in 2021, but also shows developments for the years 2017 through 2021. Some data subsets have limitations, and have only been obtained for the period 2017–2021. In addition, chapter 4.5 includes extracts from the source data for certain crime areas. These subsets were extracted using terms associated with the crime areas to search the text fields where the reporting entities fill in their basis for suspicion. The data subsets for these crime areas will not be 100 per cent correct, but they nevertheless give an indication of current trends.

Also note that the source data has not been conclusively confirmed and may change due to deletions, possible registration errors and updates.

## 3.2. Suspicious transaction reports filed

Chart 1 shows how there has been a gradual increase in STRs filed by the reporting entities over the last five years, from 8901 STRs received in 2017 to 16,513 in 2021. From 2020 to 2021, the number of reports increased by around 30%, the largest year-on-year increase during the last five years.

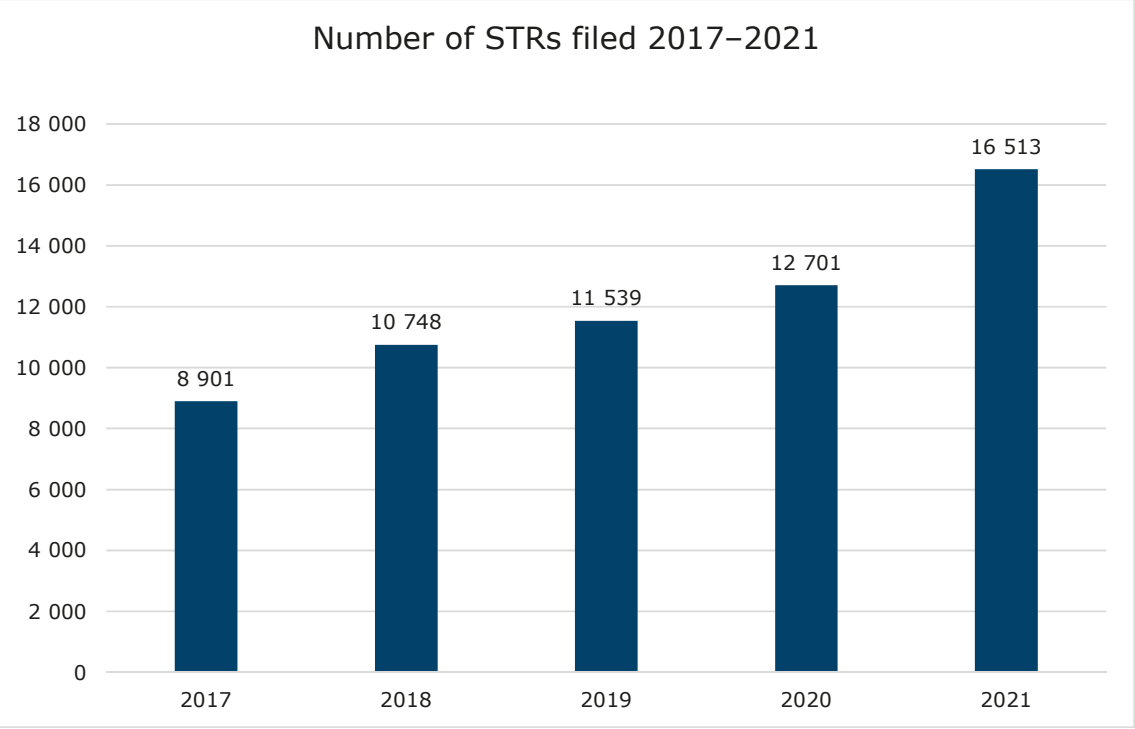



*Chart 1: Number of submitted STRs 2017–2021.*

### 3.3. Business groups which submit STRs

The Anti-Money Laundering Act (AMLA) sorts the reporting entities into 22 business groups, and these groups are then sorted into more detailed sub-groups in the Altinn form[1].

Banks and payment service providers submitted 83 per cent of all STRs in 2021. This is 5 percentage points less that these groups' share of the reporting for the period 2016–2021 (88 per cent). The decline is due to higher number of reports from the other groups.

The group comprised of real estate agents (REAs) and securities brokers, mainly REAs, clearly increased their share of submitted reports in 2021 compared with its share of reports filed during the period 2017–2021. This group, hereinafter simply referred to as REAs, has seen gradual growth over the last five years, and submitted 7 per cent of all reports from 2017 to 2021. Seen in isolation, REAs submitted 11 per cent of all STRs in 2021.

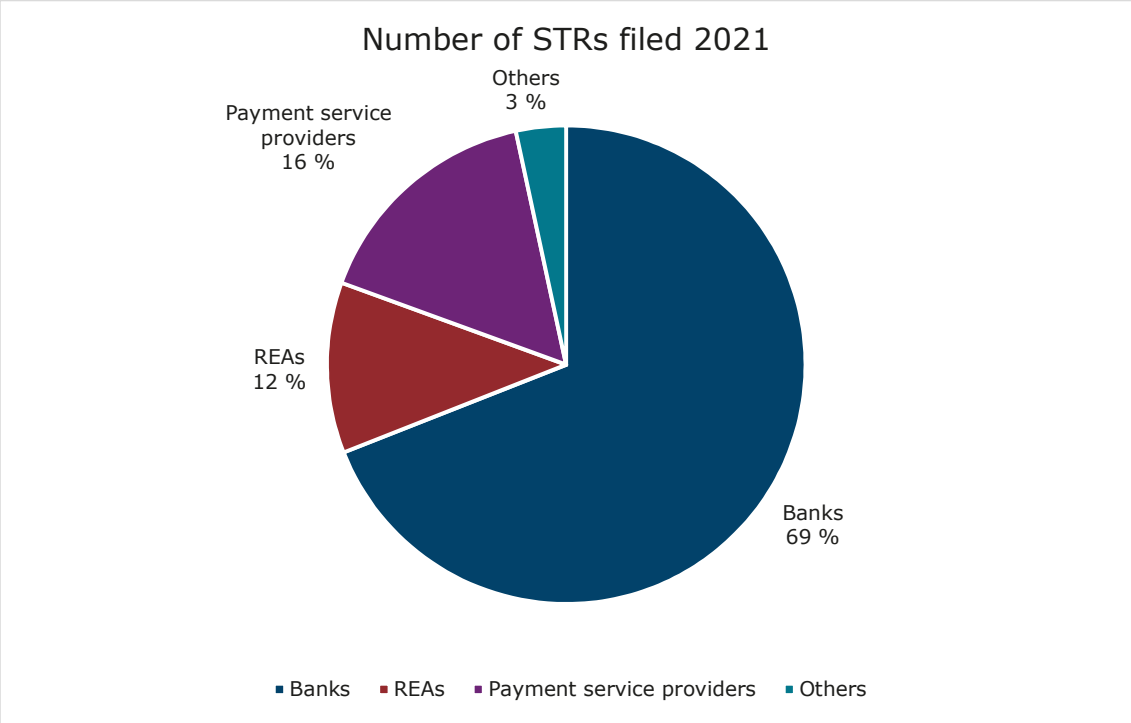



*Chart 2: Number of STRs in per cent by business group in 2021.*

Chart 2 shows that the three groups which submitted the most reports in 2021 were banks, payment service providers and REAs. Banks filed 67 per cent of STRs, payment service providers 16 per cent and REAs 11 per cent.

The "others" group consists of electronic money businesses, securities dealers etc., lawyers etc., auditors, accountants, insurance companies and others, cf. the AMLA section 4. This group contributed 6 per cent of all submitted STRs in 2021.

1 Legal professionals, others cf. the AMLA section 4, banks, electronic money businesses, traders in goods, insurance companies, real estate agents, pension funds, mail service providers, accountants, auditors, securities dealers and payment service providers.

### 3.4. Reporting entities

STRs were filed by 518 unique entities in 2021, up by 45 from 2020.

Chart 3 shows that banks and REAs were the two groups with the most unique reporting entities in 2021, followed by accountants. There were 205 unique REAs, 140 unique banks and 69 unique accountants. Real estate agents have the greatest increase from 2020, when 154 unique entities filed reports. The number of unique auditors filing reports has, however, declined, from 35 in 2020.

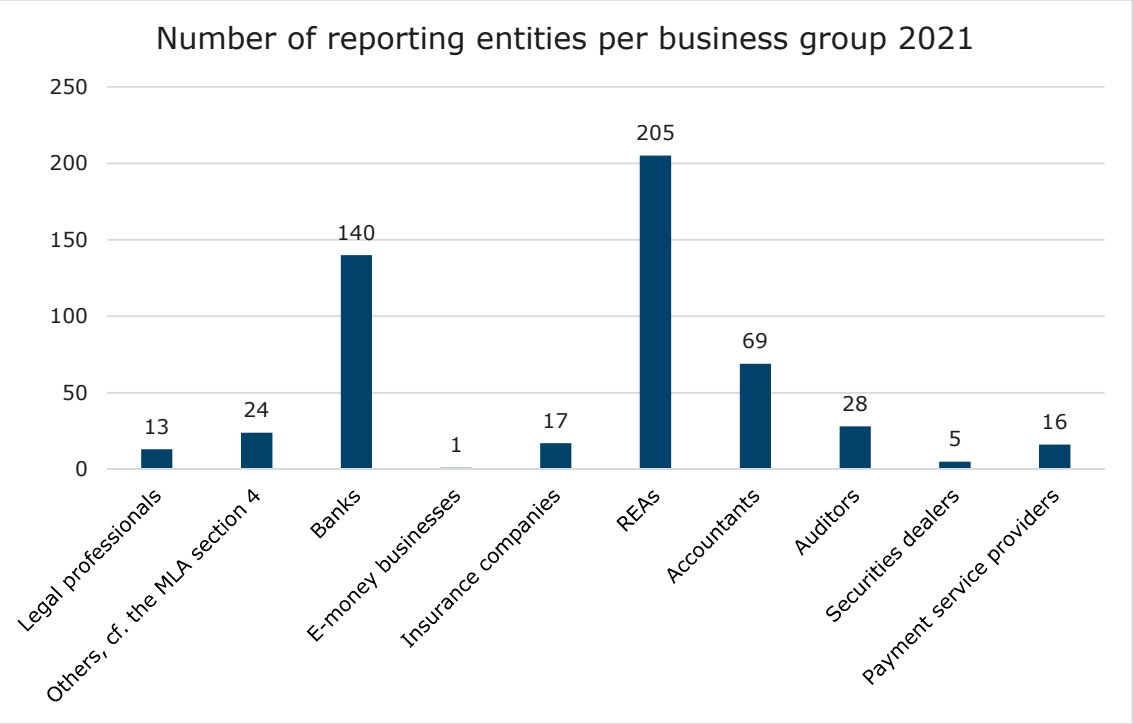



*Chart 3: Number of unique reporting entities by business group in 2021.*

Chart 4 shows the average number of STRs filed per reporting entity in 2021. Compared with Chart 3, which shows the number of reporting entities per business group, the chart changes significantly. The numbers indicate that the business groups payment service providers and banks file far more reports per entity than the other groups. Even with a high number of unique reporting entities among accountants and REAs, their reporting is still lower per reporting entity than for payment service providers and banks.

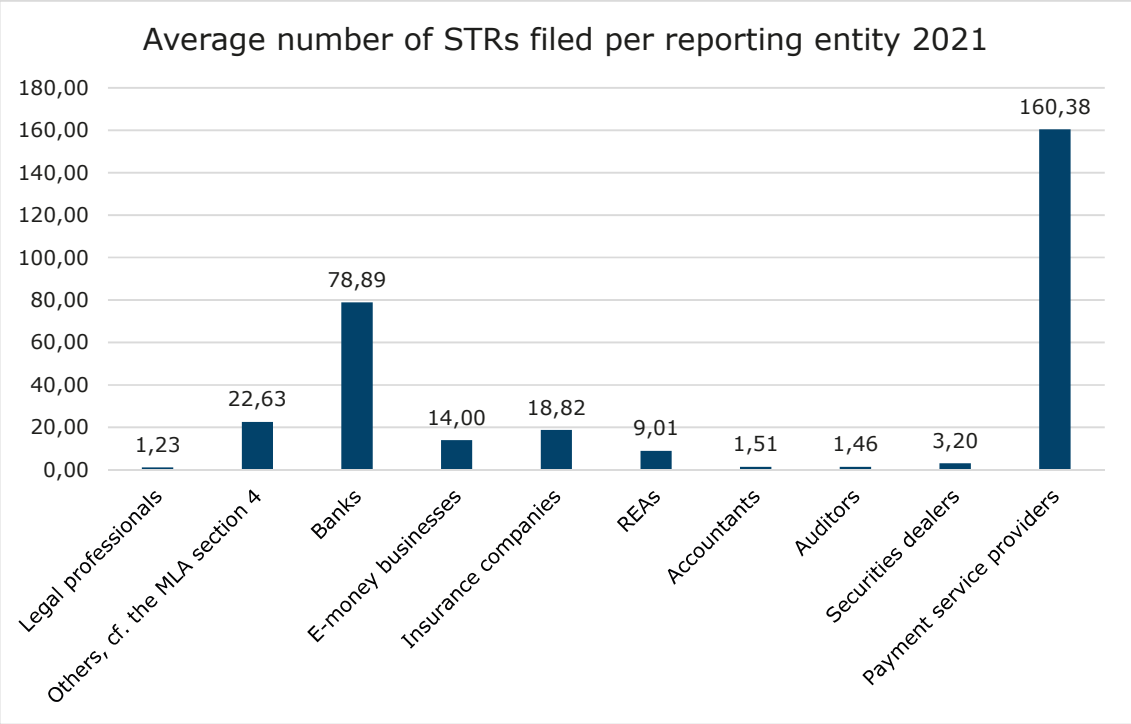



*Chart 4: Average number of STRs per reporting entity in 2021.*

### 3.5. Suspicion codes

When filing STRs, the reporting entities can select codes to categorise their suspicions (Altinn form item 4.3). Entities can tick off more than one box in a STR.

Chart 5 provides an overview of the suspicion codes used in STRs in 2021. Different business groups use different suspicion codes. Origin of the funds was the most commonly used code in STRs filed in 2021, closely followed by transfer of funds to/from abroad and suspicious account movements. This is a change from 2020, when transfer of funds to/from abroad was the most used code, followed by suspicious account movements and origin of funds. Apart from this, the most used codes were other (used when no other code fits or in conjunction with other codes), cash transaction and mixed private and company transaction.

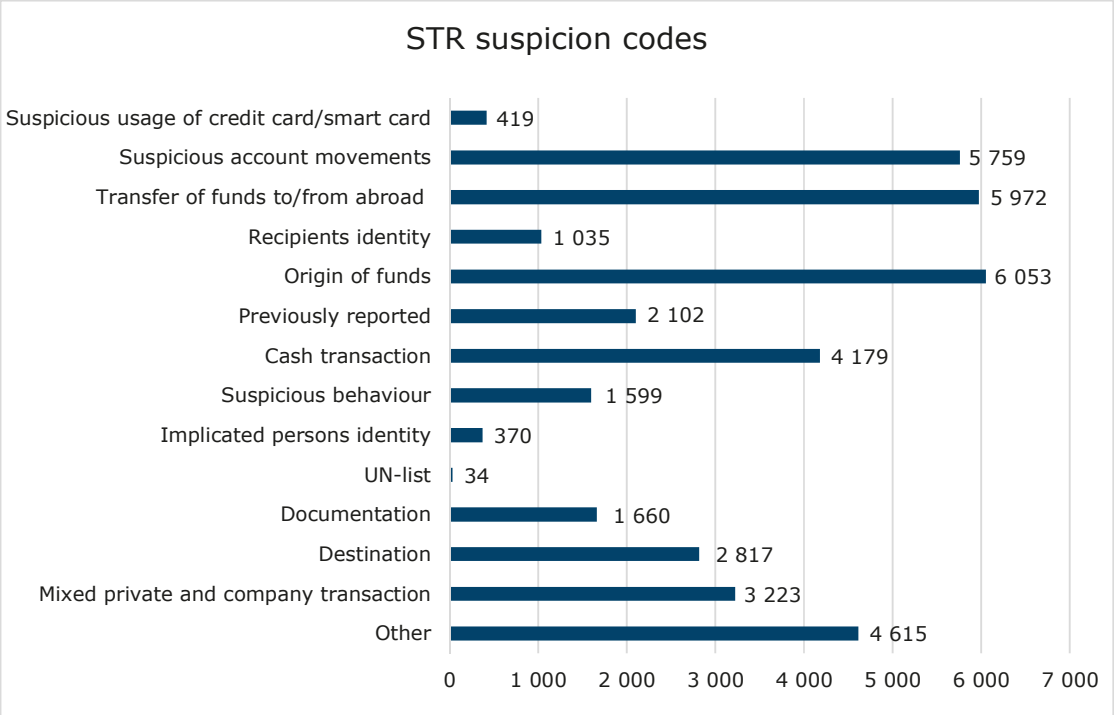



*Chart 5: Suspicion codes used in STRs in 2021*

As described in item 2.2, banks, payment service providers and REAs were the three business groups which filed the most STRs in 2021. Below follows a breakdown of the most used suspicion codes for each of the three groups.

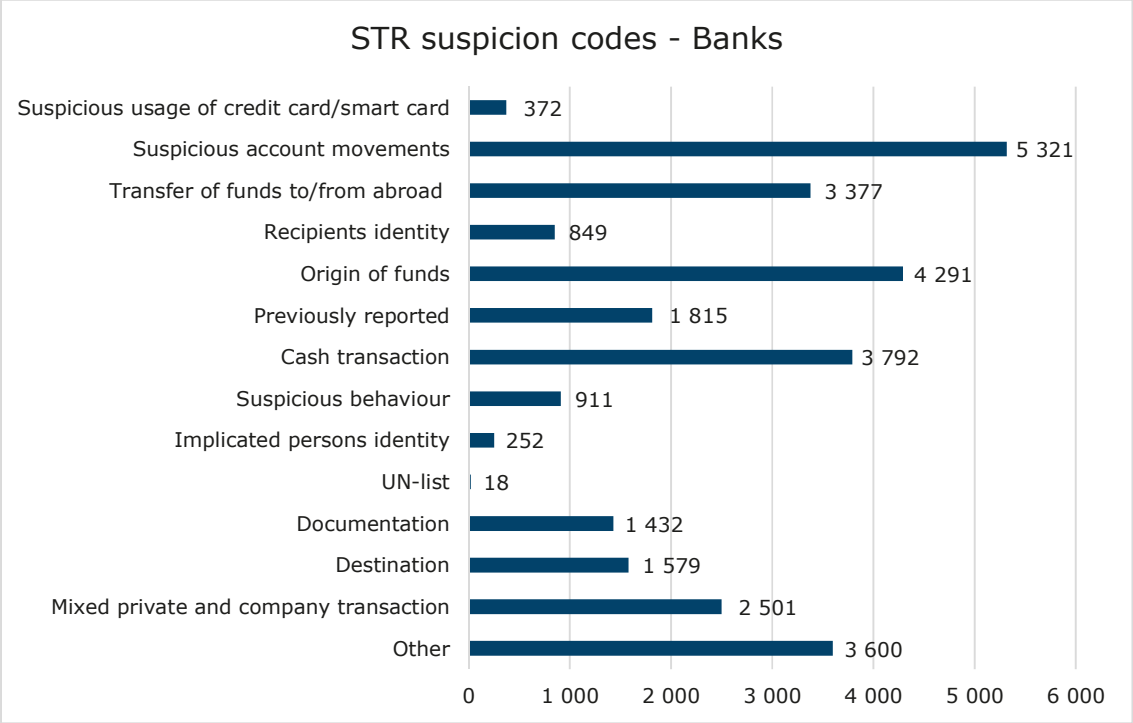



*Chart 6: Suspicion codes used by banks in 2021*

Chart 6 shows that in 2021, the suspicion codes most often used by banks were suspicious account movements, origin of the funds and cash transaction.

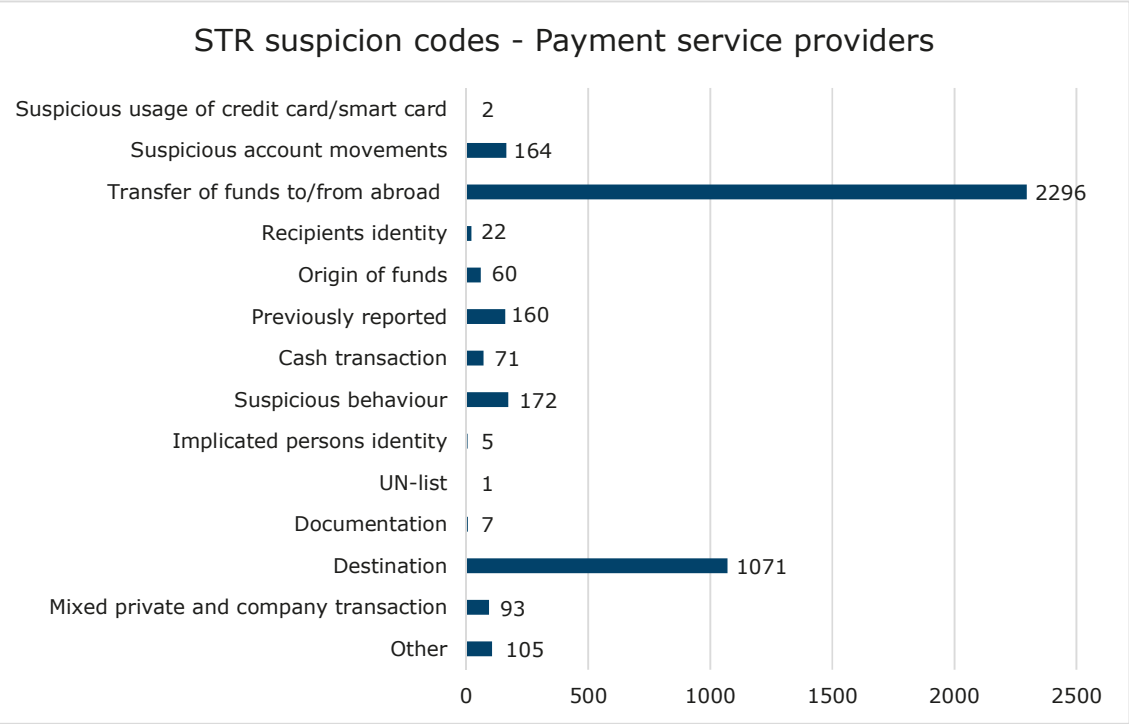



*Chart 7: Suspicion codes used by payment service providers in STRs in 2021*

Payment service providers, obviously, most often used the code transfer of funds to/from abroad, followed by destination, suspicious behaviour and suspicious account movements.

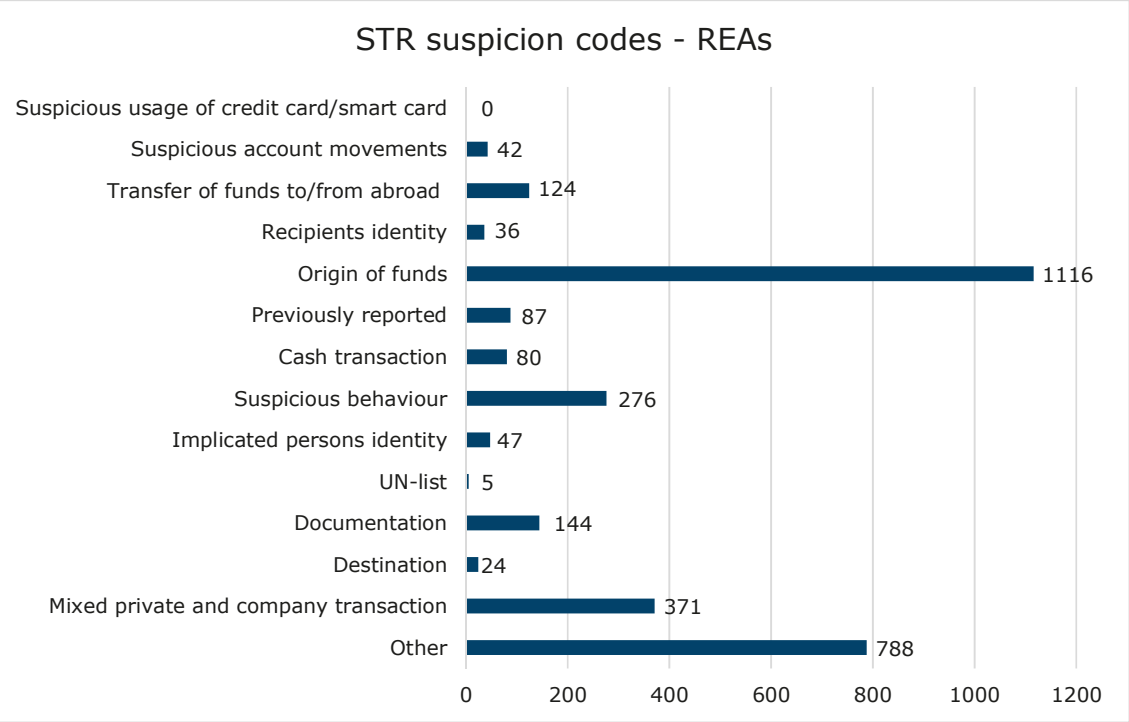



*Chart 8: Suspicion codes used by REAs in 2021*

Among REAs, origin of the funds was the most used suspicion code, followed by other, mixed private and company transaction, and suspicious behaviour.

## 3.6. Crime area trends

Below follows a trend analysis of selected crime areas that stood out in 2021 based on developments or prevalence among the business groups.

### 3.6.1. Suspicion of financing of terrorism

When filing STRs, the reporting entities can flag suspicion of financing of terrorism (Altinn form item 4.4).

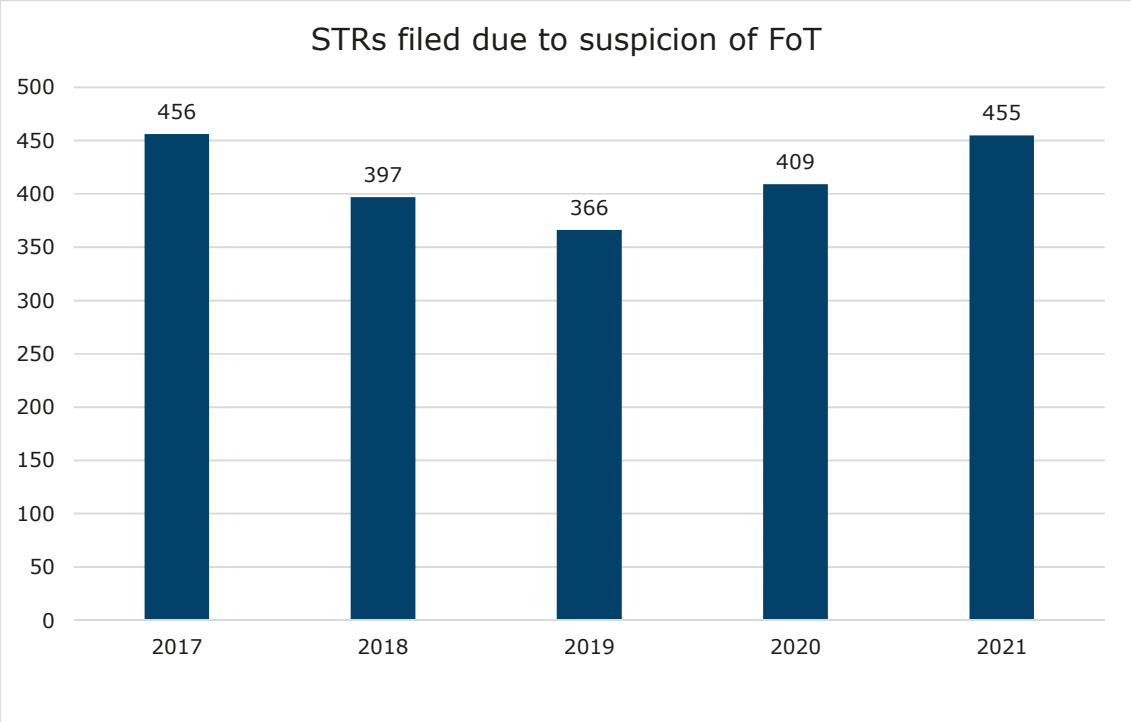



*Chart 9: STRs filed due to suspicion of financing of terrorism per year*

Chart 9 provides an overview of STRs filed due to suspicion of financing of terrorism 2017–2021. The chart shows that 2017 saw a peak in STRs flagging suspicion of financing of terrorism and a decline in 2018 and 2019. In 2020 and 2021, the numbers rose again, reaching parity with 2017 in 2021. However, the percentage of STRs filed due to suspicion of financing of terrorism among the total number of submitted STRs is declining, as shown in table 1.

| | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|
| STRs with suspicion of FoT | 456 | 397 | 366 | 409 | 455 |
| Total number of STRs | 8 901 | 10 748 | 11 539 | 12 701 | 16 513 |
| Financing of terrorism in per cent of total number of STRs | 5,1 % | 3,7 % | 3,2 % | 3,2 % | 2,8 % |

*Table 1: STRs filed due to suspicion of financing of terrorism in per cent of the total number of STRs filed*

In 2021, the majority of the STRs filed due to suspicion of financing of terrorism was filed by banks, 79 per cent. Payment service providers filed 15 per cent of these reports and the other groups the remaining 6 per cent.

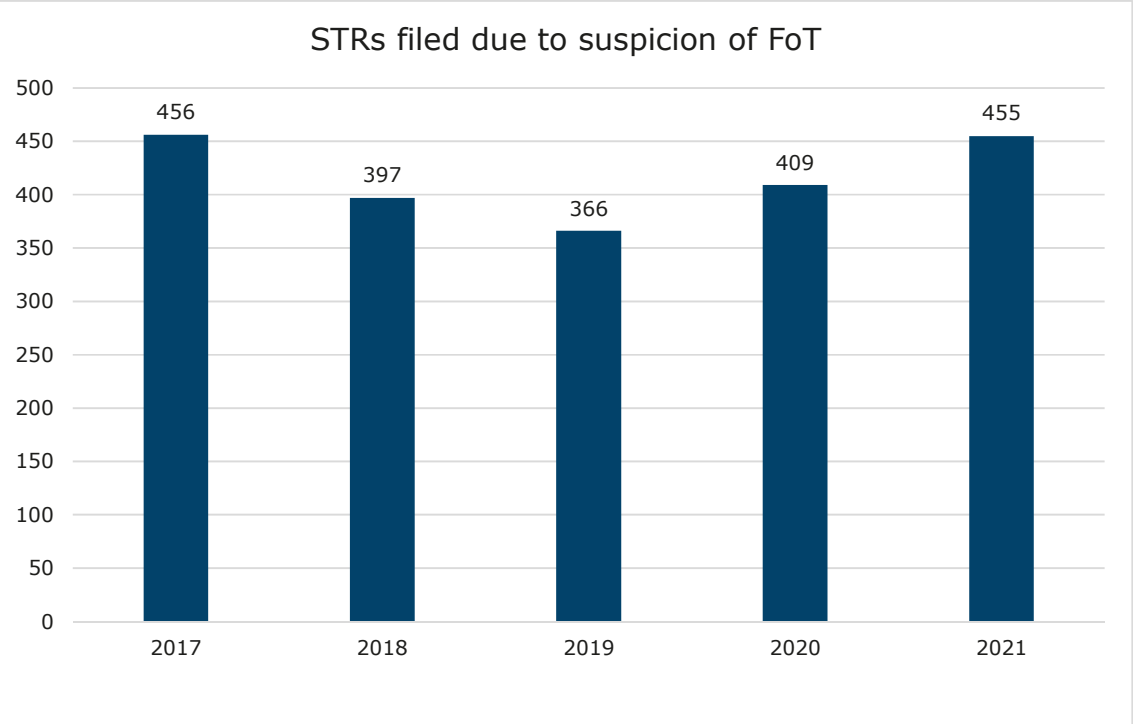



Chart 10: STRs per business group in 2021 – suspicion of financing of terrorism

### 3.6.2. Suspicion of tax fraud and exploitation of workers

During the period 2017–2021, 3446 STRs were filed 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 business groups and amounts. All STRs relating to tax fraud and exploitation of workers are therefore not captured by these statistics, and it is likely that the number of STRs that can be linked to tax fraud and exploitation of workers is higher than the number indicated by the extracted data. However, Chart 11 shows that the number stays relatively stable at around 600–700 during the period 2017–2020, rising to 823 in 2021.

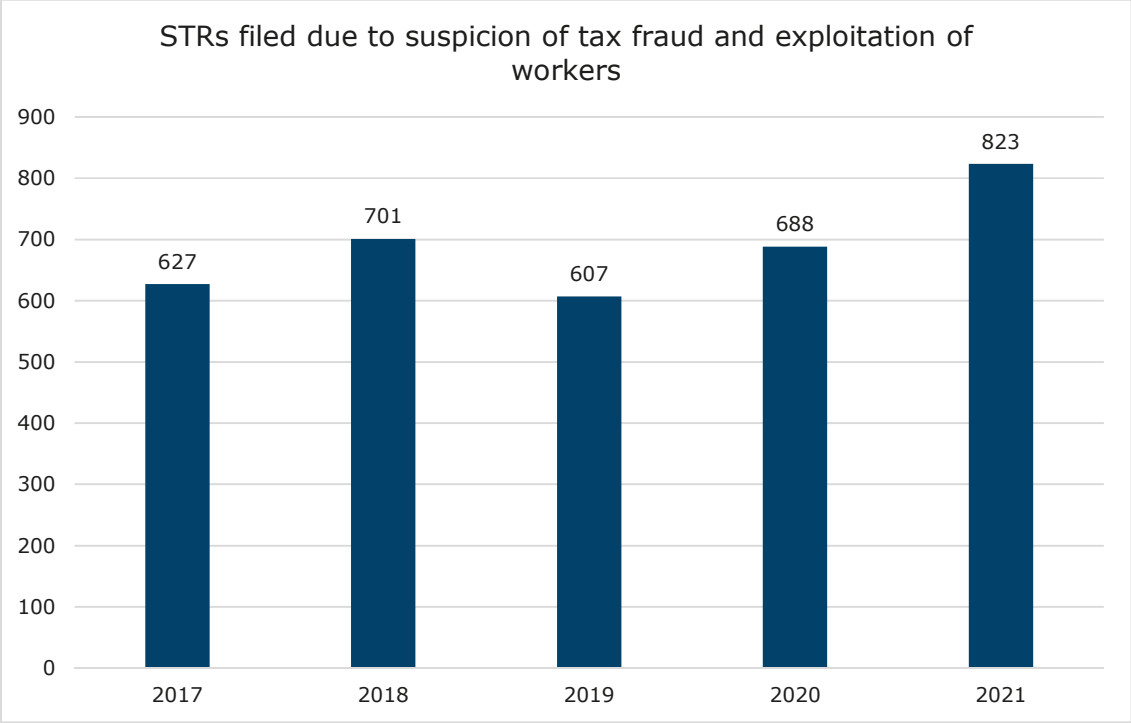



*Chart 11: STRs filed due to suspicion of tax fraud and exploitation of workers per year*

Banks, both commercial and savings banks, reported the most suspicions of tax fraud and exploitation of workers among all the business groups in 2021.

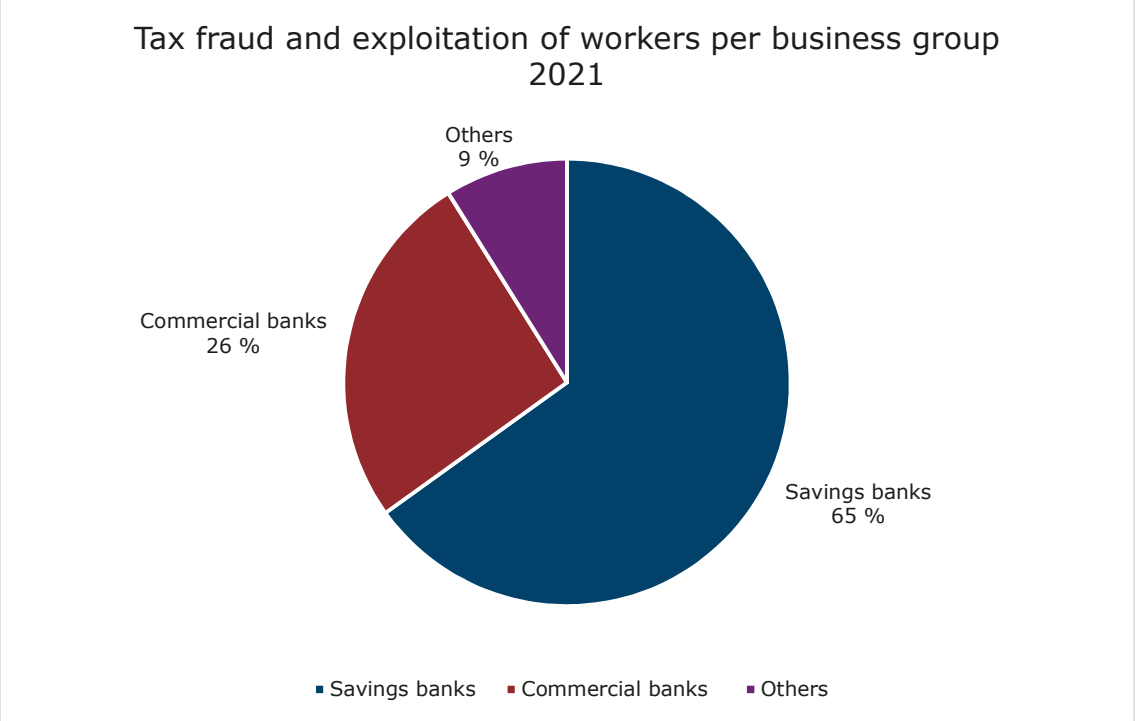



*Chart 12: STRs per business group – tax fraud and exploitation of workers*

### 3.6.3. Suspicion of fraud and money mule activity[2]

During the period 2017–2021, 8102 STRs were filed due to suspected fraud and money mule activity (excluding insurance fraud). These activities have shown a significant increase during the period. From 2020 to 2021, the reporting increased by around 30 per cent. This may be due to a growth in fraud during the corona pandemic.

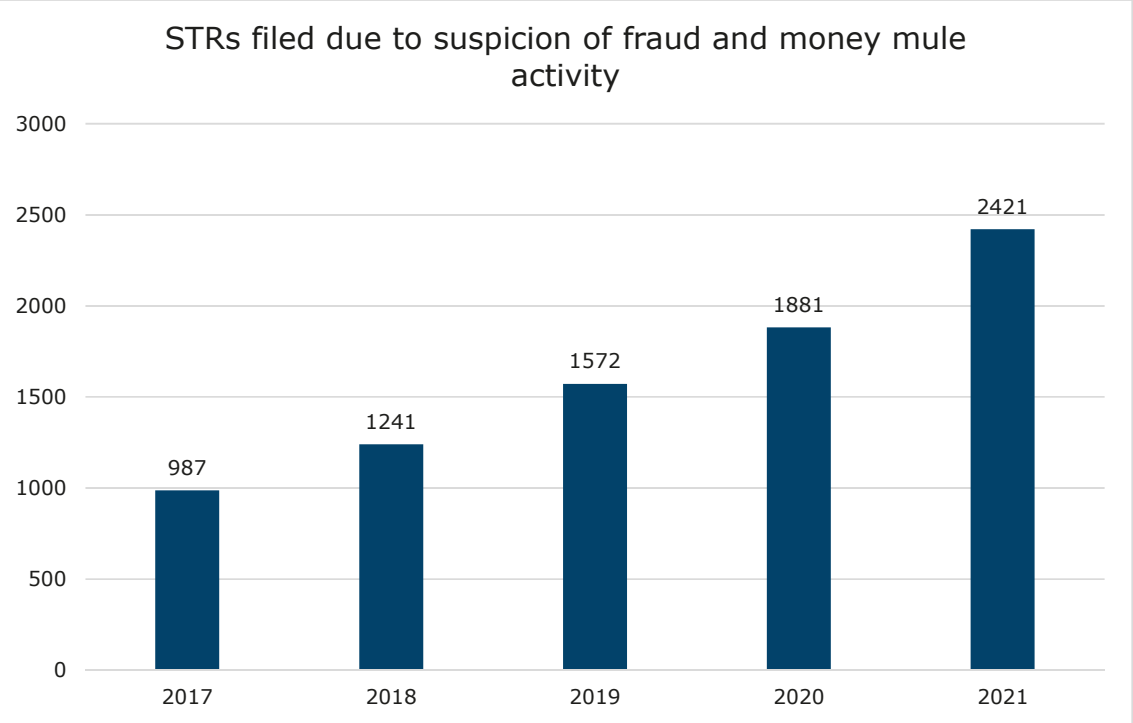



*Chart 13: STRs filed due to suspicion of fraud and money mule activity per year*

Banks, both commercial and savings banks, file the most STRs due to suspicion of fraud and money mule activity, followed by others cf. the AMLA section 4, of which cryptocurrency exchanges make up a large share after they became obliged entities. Further, payment service providers also file a fair share of reports with suspected fraud and money mule activity.

2 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).

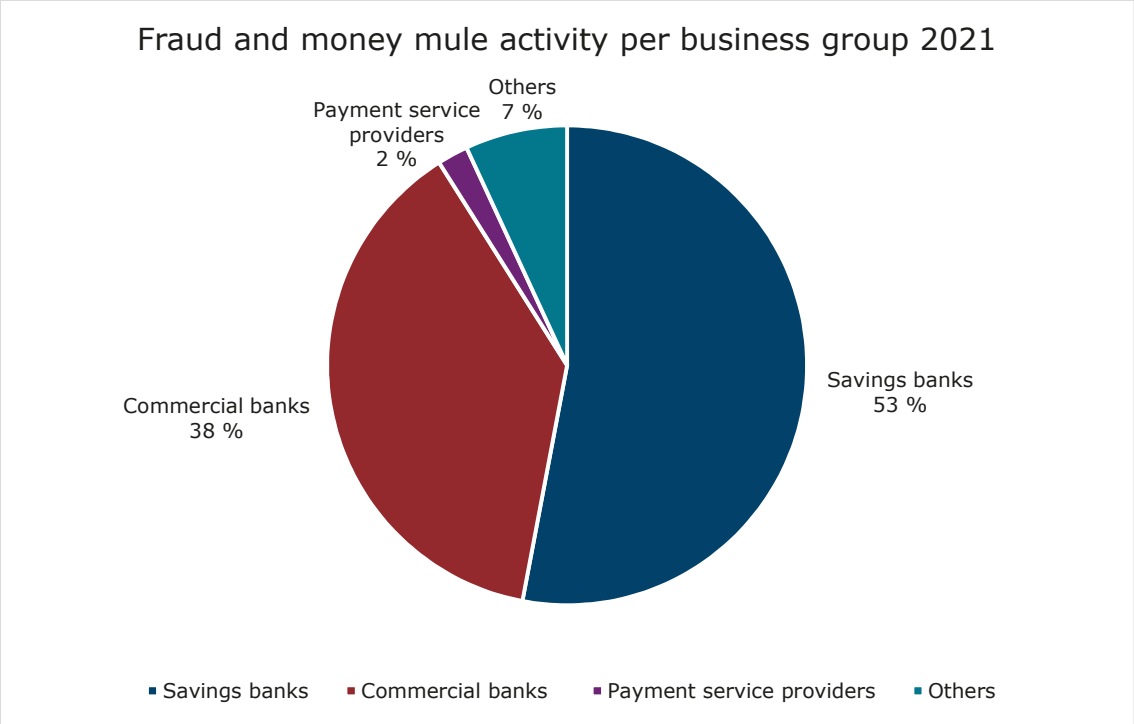



*Chart 14: STRs filed due to suspicion of fraud and money mule activity in 2021*

### 3.6.4. Suspicion of online child sexual abuse

During 2017–2021, 1277 STRs were filed due to suspicion of online child sexual abuse. The number of reports filed due to suspicion of online child sexual abuse has been growing since 2017, and with a significant increase in 2021. This may be due to the increased awareness of the significance of financial transactions in these cases, indicator lists prepared by the FIU and increased media coverage. According to Europol[3], the risk of child sexual abuse has increased during the pandemic.

The FIU's cooperation with other national FIUs through the Egmont Group has also resulted in increased exchange of information.

3 https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation

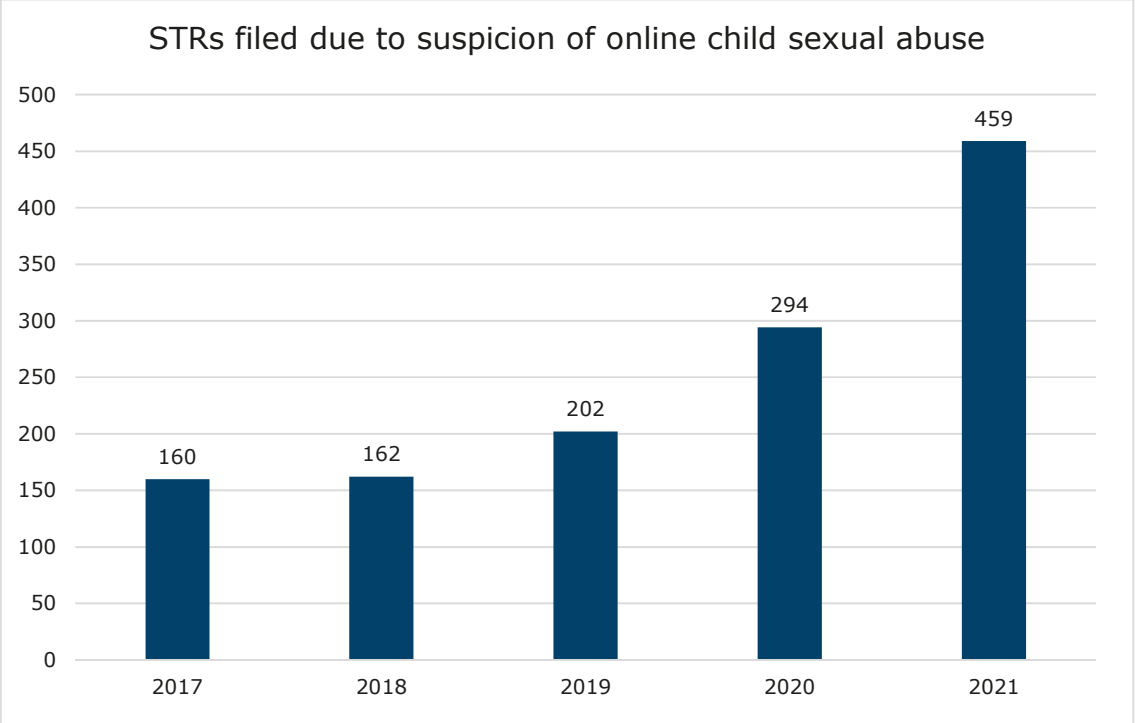



*Chart 15: STRs filed due to suspicion of online child sexual abuse per year*

In 2021, payment service providers filed two-thirds of the total number of STRs filed due to suspicion of online child sexual abuse. Banks filed 32 per cent of the reports, while other business groups filed the remaining 2 per cent.

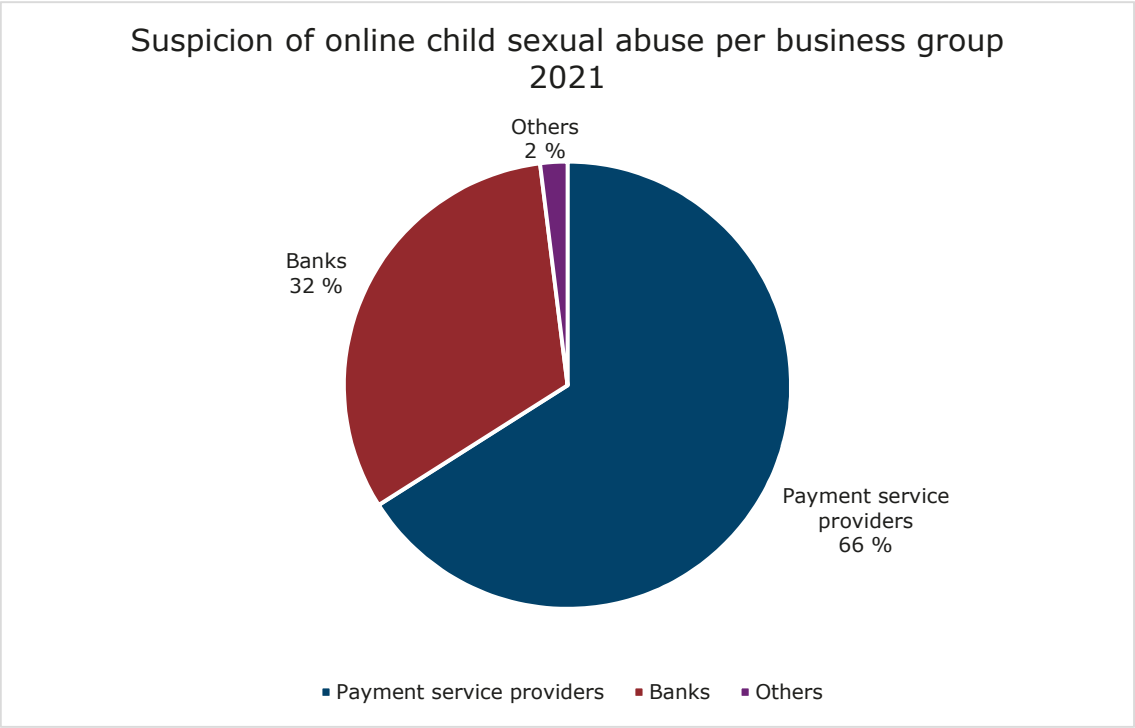



*Chart 16: STRs filed due to suspicion of online child sexual abuse in 2021*

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

In 2020 and 2021, 556 STRs were filed in connection with Covid-19[4]. In 2020, 311 STRs were filed in connection with Covid-19, dropping to 245 in 2021. STRs are mainly filed 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.

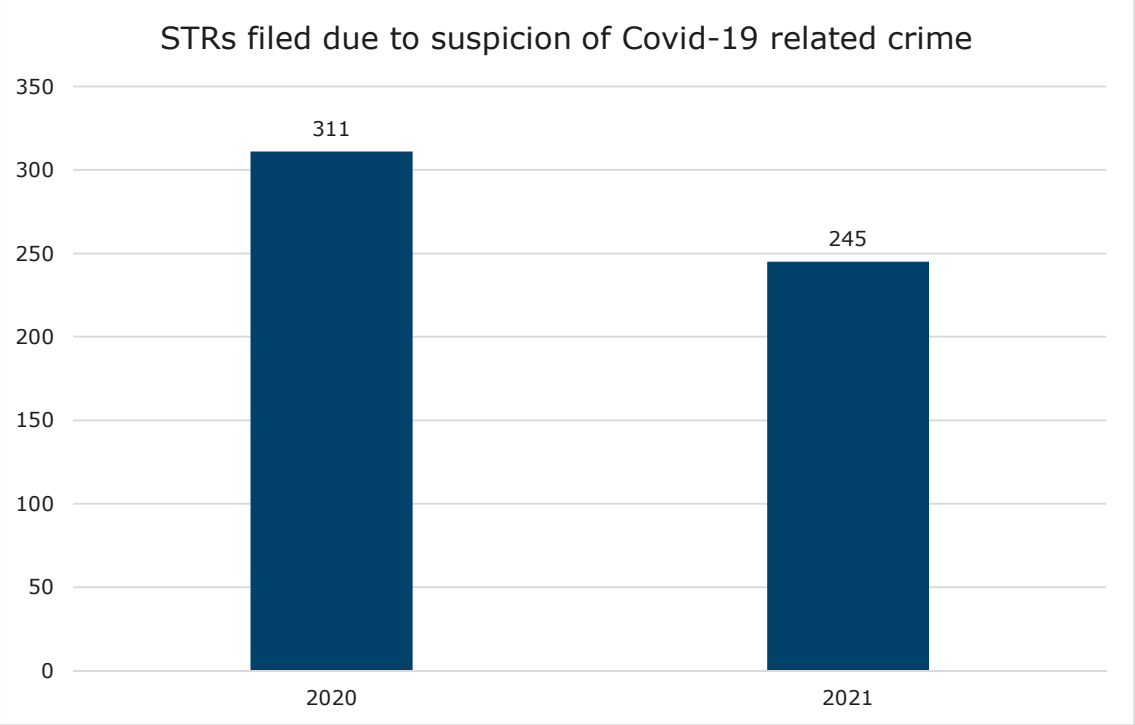



Chart 17: STRs filed due to suspicion of Covid-19-related crime per year.

The business group banks, both commercial and savings banks, filed the most Covid-19 related STRs in 2021, followed by REAs. The rest were filed by others, cf, the AMLA section 4.

4 Note that the data has been extracted using search words, and that the real figure is likely to be somewhat lower than indicated by the statistics.

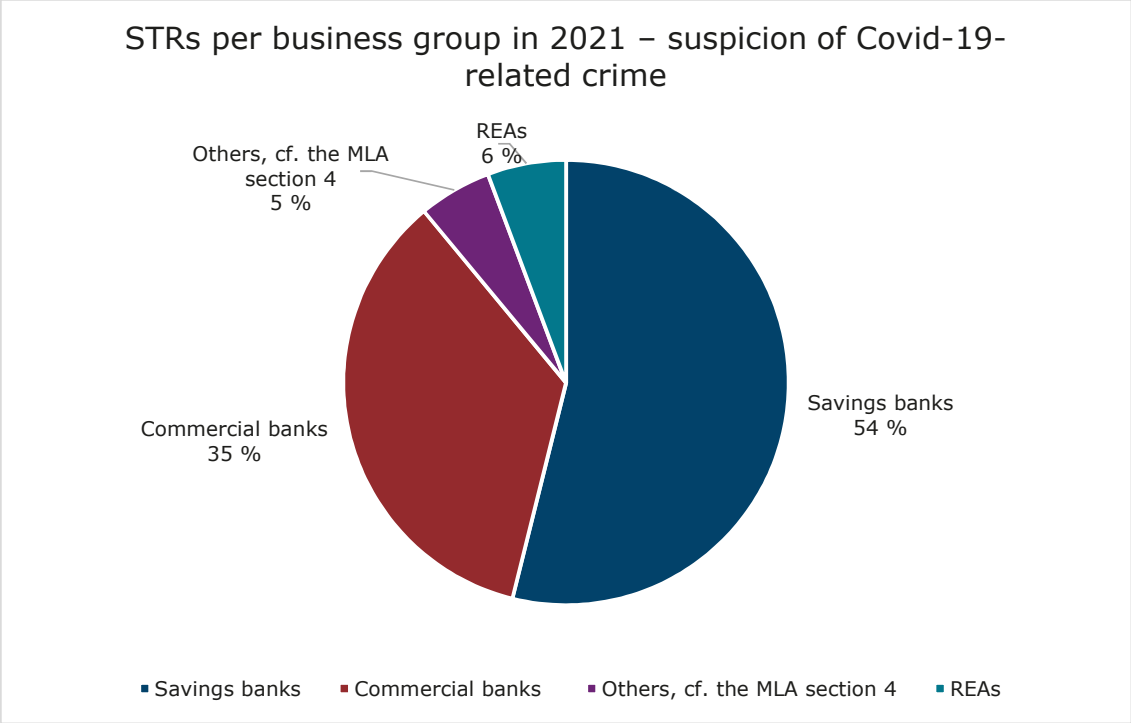



*Chart 18: STRs per business group in 2021 – suspicion of Covid-19-related crime.*

## 3.7. Who are reported?

### 3.7.1. Sex

A total of 12,897 individuals[5] were implicated in one or more STRs in 2021. This is up 24 per cent from 2020, when the number was 9786. Men make up 72 per cent of implicated individuals, with women making up 27 per cent and 1 per cent being unknown[6].

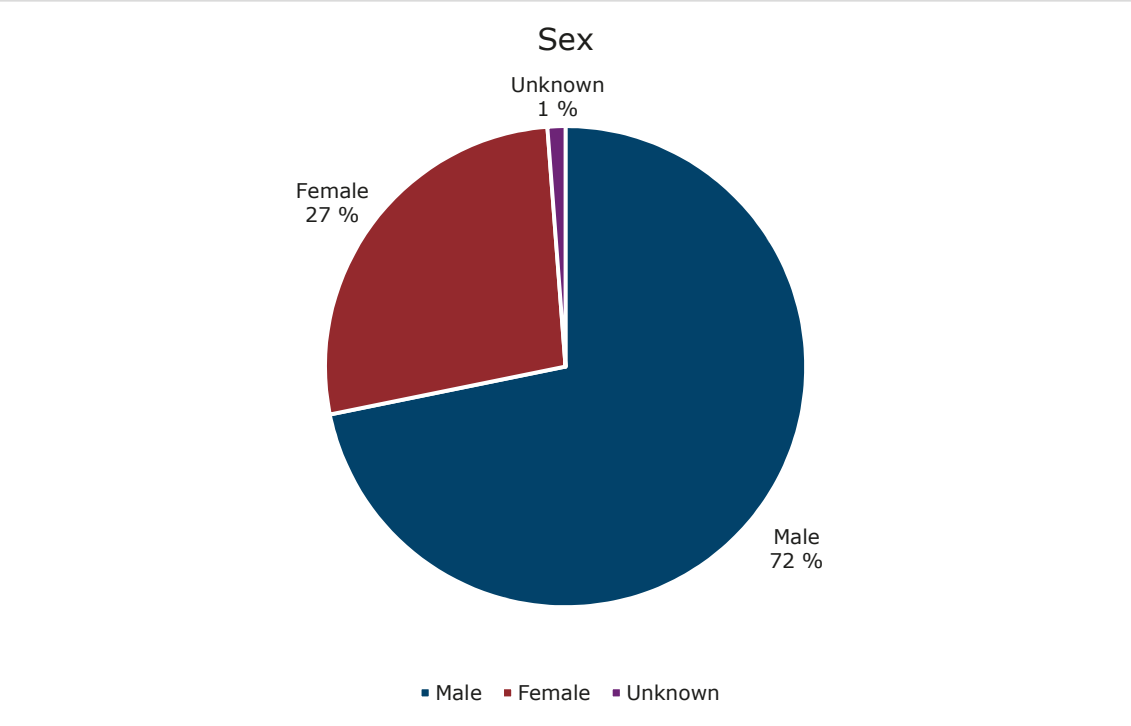



*Chart 19: Individuals implicated in STRs 2016–2021, by sex.*

5 The person the reporting entities suspect is the principal offender (individual or organisation) behind the suspicious activity.

6 The category unknown contains both STRs in which the sex is unknown and transactions for which the "sex" field in the money laundering database is blank.

### 3.7.2. Age

Persons implicated in STRs in 2021 were mostly in the 30–49 age group. This age group made up approx. 48 per cent of the total, of which 25 per cent were in the 30–39 age group and 23 percent in the 40–49 age group. The 50 and up age group made up 33.5 per cent, with 17.3 per cent in the 50–59 age group and 16.2 per cent in the 60 and up age group. Persons under 30 made up 18.5 percent of the total number of implicated persons, and they were mainly in the 20–29 age group.

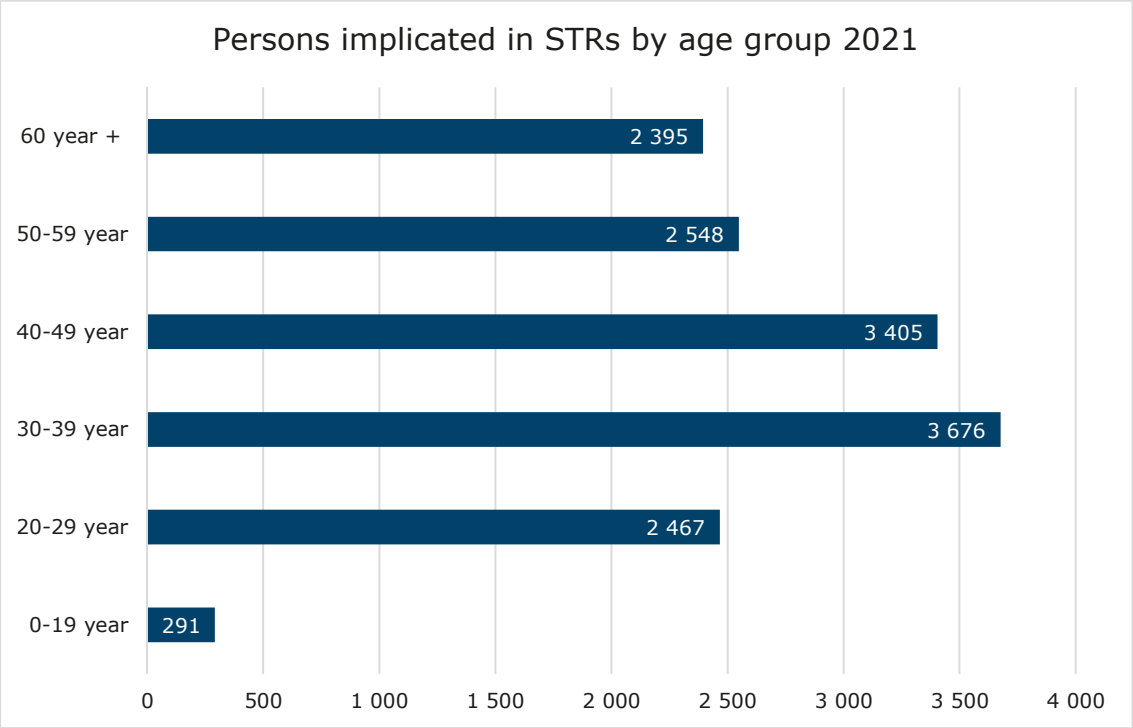



*Chart 20: Persons implicated in STRs in 2021, by age group.*

### 3.7.3. ID type

92 percent of all persons mentioned in STRs in 2021 were recorded with Norwegian national identity numbers[7]. Further, Chart 21 shows that 6 percent were recorded as unknown[8] and 2 percent were recorded with a Foreigner's Norwegian Identity Number (D number)[9].

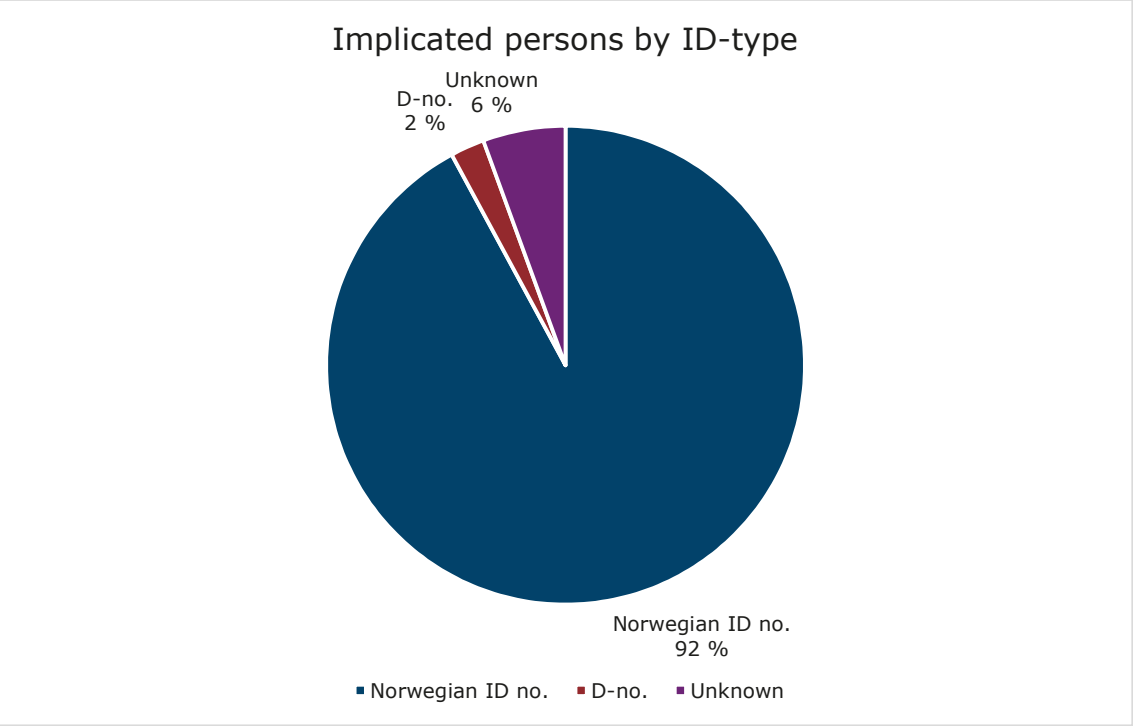



*Chart 21: Persons implicated in STRs in 2021, by ID type*

7 A national identity number is an 11-digit identification number. Everyone listed in the National Population Register, born in Norway or living in Norway, as well as Norwegian nationals born or living abroad who need a national identity number to be issued a Norwegian passport, have a national identity number (skatteetaten.no).

8 In the category "unknown", no identity or D number is recorded.

9 People intending to work and stay in Norway for less than 6 months need a Foreigner's Norwegian Identity Number to be listed in the National Population Register. A D number is needed to obtain an employee's tax withholding card (skatteetaten.no).

### 3.7.4. Nationality

Chart 22 shows the nationalities of implicated persons in 2021. In 2021, 108 different nationalities were represented among implicated persons. The corresponding figure in 2020 was 107. Implicated Norwegian nationals made up 75 per cent of the total. Swedish and Polish nationals were the second-most represented groups, both at 3 percent, followed by Syrian and Lithuanian nationals at 2 per cent. Romanian nationals made up 1 per cent, and other nationalities 14 per cent.

A comparison with 2021 shows an almost identical percentage of implicated Norwegian nationals for 2020. The percentage of Polish nationals declined in 2021, while the percentages for Swedes, Syrians, Lithuanians and Romanians remained stable.

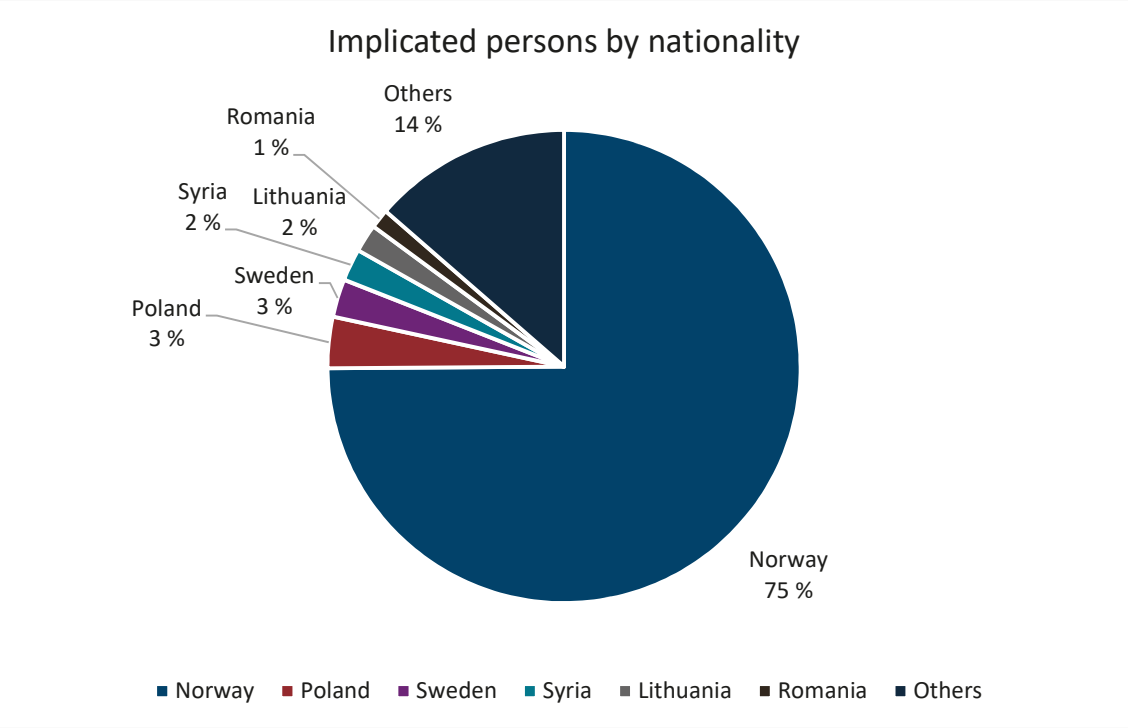



*Chart 22: Individuals implicated in STRs 2021–2021, by nationality*

### 3.8. Reported organisations

In 2021, 1411 organisations were implicated in one or more STRs. Chart 23 shows that this is an increase of 209 compared with 2020.

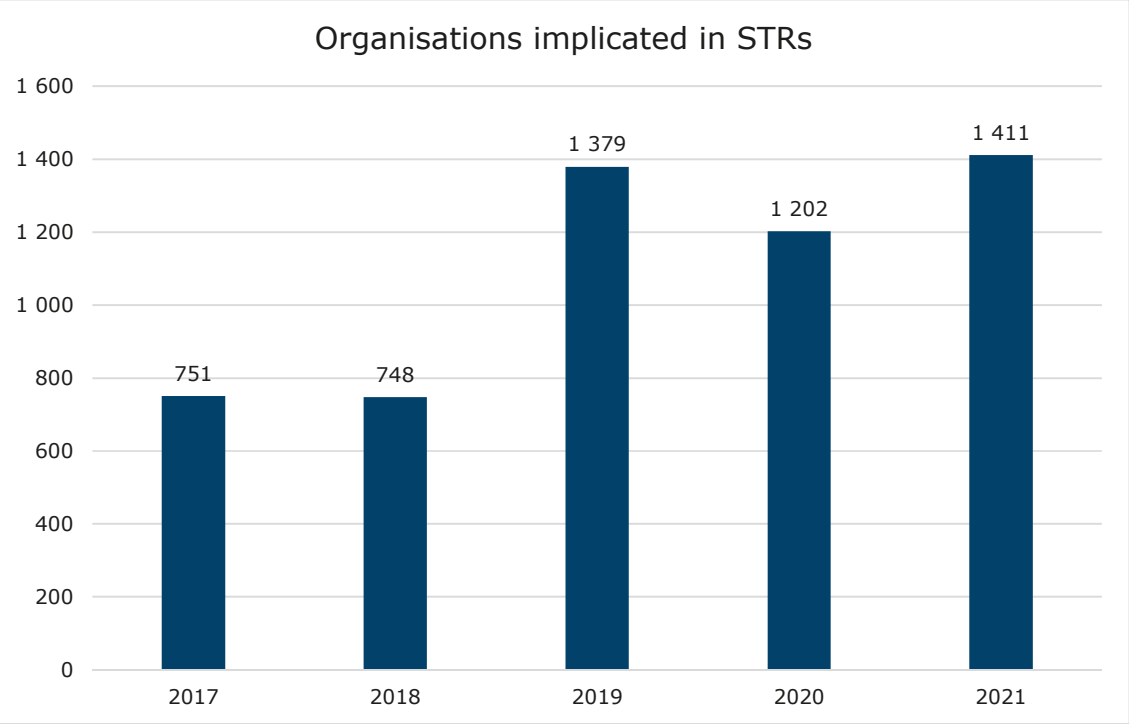



*Chart 23: Organisations implicated in STRs 2017–2021*

The number of implicated organisations almost doubled from 2017 to 2021. However, table 2 shows that the percentage of implicated organisations remains quite stable at slightly less than 10 per cent of the total STRs, with 8.5 per cent in 2021, down from 9.5 per cent in 2020.

| Year | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|
| STRs with implicated organisations | 751 | 748 | 1379 | 1202 | 1411 |
| Total no. of STRs | 8 901 | 10 748 | 11 539 | 12 701 | 16 513 |
| In % of total number of STRs | 8,4 % | 7,0 % | 12,0 % | 9,5 % | 8,5 % |

*Table 2: Organisations implicated in STRs in percent of total number of STRs filed in 2021*

#### 3.8.1. Industry codes

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 standard[10]. In 2021, the implicated organisations represented 67 different industry codes. Chart 24 shows the number of unique implicated organisations by the 15 most common industry codes in STRs in 2021. The industry code "Real estate activities" was the most frequently reported, with 233 STRs.

10 https://www.ssb.no/virksomheter-foretak-og-regnskap/nace

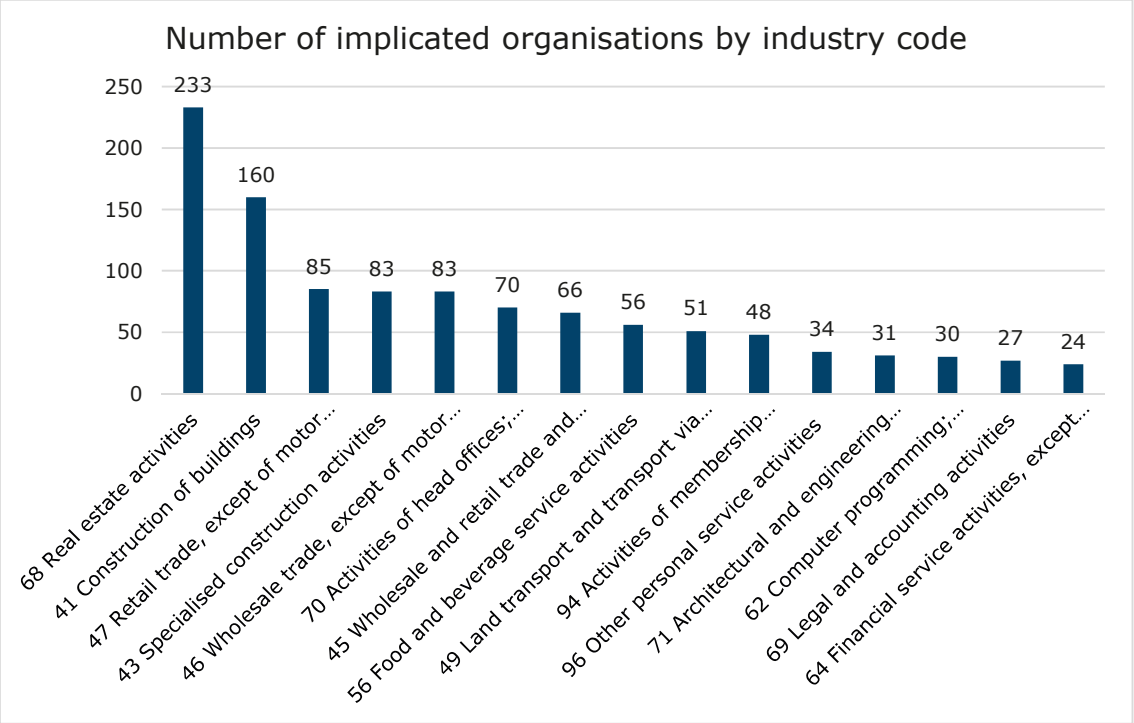



*Chart 24: Number of implicated organisations by the most frequently reported industry codes in 2021*

### 3.9. Freezing transactions

The FIU may in special cases stop a transaction from being carried out, cf. the Anti-Money Laundering Act section 27. Freezing a transaction means that it is stopped. In 2021, the FIU received 62 requests to freeze transactions, of which 16 were recorded as projects in the FIU money-laundering database.

| Freezing transactions | 2021 |
|---|---|
| Number of requests to freeze transactions: | 62 |
| Number of frozen transactions: | 16 |
| Total amount frozen transactions: | NOK 30 915 031 |

*Table 3: Frozen transactions 2021*

Freezing a transaction is an invasive measure, and the FIU makes a thorough assessment before deciding to freeze a transaction. Normally, the FIU engages in communication and dialogue with the reporting entities before deciding to freeze a transaction. In several of the cases, the conclusion is that that freezing the transactions would constitute a disproportionate measure, that the conditions for doing so are not present and/or that further customer-related measures must be taken to gather sufficient information to make a decision. Our experience from the past year is that a number of reporting entities increasingly apply the legal authority provided them by section 21 and 24 of the Anti-Money Laundering Act to not carry out transactions, and that the FIU therefore in many cases does not have to freeze transactions pursuant to section 27 of the act.

# 4. Communication

It is a key aim for the FIU to enrich, process and analyse information from STRs and communicate the results. In addition to communicating the information to the police districts and other specialist agencies, information is communicated to supervisory authorities and foreign FIUs. The products communicated and their formats, depend on the recipient and the recipient's intended use of the information.

Table 4 shows products communicated to the police, supervisory authorities, industry associations, foreign FIUs and foreign law-enforcement authorities in 2021. Products may include intelligence reports, replies to requests and other exchange of information. A product may include data and information from multiple STRs and sources.

| Intelligence products and criminal cases communicated to: | 2021 |
|---|---|
| The police | 1 165 |
| Supervisory authorities | 159 |
| Foreign FIUs and law-enforcement authorities | 103 |
| TOTAL | 1 427 |

*Table 4: Products communicated in 2021.*

## 4.1. Implicated persons and organisations

The FIU updates the police intelligence database with the information it receives. This includes information about implicated persons and organisations, from submitted STRs in the money-laundering database. The information is entered either automatically or manually. Table 5 shows the status as per 31.12.2021, i.e. not in the number entered per year. At the end of 2021, 36,296 unique persons and 1784 unique organisations had been entered in the police intelligence database.

| Implicated persons and organisations entered in the police intelligence database | Status |
|---|---|
| Persons – entered automatically | 29 376 |
| Persons – entered manually | 6 920 |
| TOTAL PERSONS | 36 296 |
| Organisations – entered automatically | 740 |
| Organisations – entered manually | 1 044 |
| TOTAL ORGANISATIONS | 1 784 |

*Table 5: Implicated persons and organisations entered as per 31.12.2021.*

## 4.2. Other exchange of information etc.

The FIU has extensive contact with national and international actors, and received and replied to 771 requests in 2021, which is a significant increase on previous years. In 2021, the FIU received 3323 information messages through FIU net and Egmont Secure Wed. A substantial share of this information was received from other European FIUs.

# 5. Operational analysis

This chapter concerns anonymised cases the FIU has been working in 2021. Information from the reporting entities has been decisive and has helped uncover suspicious circumstances.

**Freezing of assets – misappropriation and money laundering**
One person was charged with aggravated misappropriation of movables and tax evasion. He was also at risk of going bankrupt, partly due to unpaid taxes.

The FIU received information that at least NOK 3,000,000 had been transferred to an account registered to his spouse. The funds originated from a private loan from a third party intended to cover the suspect's credit card debt.

The FIU froze the funds in the spouse's account to cover any damages, a decision later upheld by the local police district, as it was considered likely that the suspect would be convicted and damages awarded.

Information also emerged that the suspect was the de facto holder of and had use of his spouse's account, and there was reason to believe that the transaction was routed through this account to conceal the funds to avoid confiscation and payment of damages.

**Financing of terrorism**
In 2021, the FIU received a STR concerning a person the reporting entity feared was undergoing radicalisation. The suspicion was based on online purchases and the stated purposes of the transactions, as well open-source searches the suspect had made.

The information in the STR was enriched and analysed by the FIU, and the information was communicated to the local police. The person was previously unknown to the police. Further follow-up corroborated the impression that the person was undergoing radicalisation, and firearms and a large amount in cash were seized from his home.

**Financing of terrorism**
In 2021, the FIU received a STR about a foreign national living in a country in Eastern Europe who had an account with a Norwegian bank. This person's transaction history substantiated the hypothesis that he was selling right-wing extremist paraphernalia to persons in Norway.

The FIU analysed and enriched the information, revealing indications that this person was also selling weapons-related goods. The information was communicated in an intelligence report to the FIU in the country where the person lives. The relevant FIU replied that further enquiries would be made and preventive measures implemented as a result of the intelligence received from the Norwegian FIU.

**Seizures made in cases involving exploitation of workers, tax and other fraud**
Over the course of May 2021, transactions originating in fraud and totalling NOK 1,600,000 were stopped. The funds were the proceeds of fraud in connection with exterior house renovation and other maintenance work.

Six persons and two enterprises with accounts in six different banks were involved in the frauds and associated money laundering. The FIU supplied information which helped expand the criminal cases against the perpetrators.

The banks' communicated with each other to uncover the scope and organisation of the frauds, in particular to trace the funds and stop the transactions, was decisive.

**Criminal networks**

As in previous years, 2021 saw the FIU receive valuable information about laundering of proceeds from serious profit-motivated crime for others. The proceeds appear to be linked to organised criminal networks engaging in several types of crime, including tax fraud and exploitation of workers, fraud of individuals, financial institutions and public support schemes, illegal loan brokering and threats and extortion.

To a large extent, the information concerns transactions where the origins are hard to determine, and the funds are quickly forwarded to many accounts held by different persons. The purpose of the transactions is often unknown or stated as loans and/or trading in valuable objects such as watches, art and real estate. In addition, the funds are forwarded to buy cryptocurrency or to recipients abroad via foreign payment transfer platforms.

The FIU has noted that it has become increasingly common to use incorrect or false documentation to legitimise the origin of the funds, a fact which may be due to more attention to and higher quality in the customer-related measures of the reporting entities.

As a result of such information, the FIU found that actors from different networks can be linked via financial transactions. In this way, the FIU is increasingly able to uncover relationships previously unknown to the police. We also find that the lines between the networks are blurred.

In 2021, the FIU has shared information with the police about more than ten persons with key roles in such networks. The information has been used in several ongoing investigations, and as intelligence and for prevention purposes.

**Tax fraud and exploitation of workers**

The FIU received several STRs implicating two brothers due to suspected organised tax fraud. The brothers operated several construction enterprises and received large payments into their private bank accounts, totalling around NOK 5 million. Information received indicated that invoices had been issued from several different enterprises and that no VAT had been paid. Funds received into the brothers' accounts were quickly forwarded in the form of large cash withdrawals and transfers to other family members etc. No taxes were paid. The brothers had no recorded income in recent fiscal years.

Based on information from reporting entities and other sources, the above was communicated to the police and the tax authorities in spring 2021. The tax authorities have later formally reported the matter to the police, and the case is currently under investigation.

**Tax fraud and exploitation of workers**

In 2021 the FIU received several STRs about a woman linked to a grouping known for fraud, tax fraud, exploitation of workers etc. There were suspicions that family members were using the woman's identity, establishing house-painting enterprises in her name. Bank accounts had also been opened in her name with several different banks, receiving payments exceeding NOK 4 million over a few months. The payments appeared to be settlements for work and services provided. The funds were quickly transferred out of the accounts in the form of e.g. large cash withdrawals and transfers to various payment service providers. A review of the accounts showed that taxes had not been paid. The woman had no recorded income in recent years.

Based on information from reporting entities and other sources, the above was communicated to the police and tax authorities. The tax authorities have later formally reported the matter to the police, and the case is currently under investigation.

**Money laundering and corruption**

From 2016 to 2021, the FIU received almost 20 STRs from reporting entities in connection with transactions made by Norwegian nationals employed by or affiliated with international corporations. Analysis and exchange of information with other FIUs have uncovered possible cases of aggravated laundering of proceeds from crime and corruption. The cases are being investigated by the police.

**Transaction frozen – fraud**

In late April 2021, an elderly couple received a visit from persons offering to renovate the exterior of their house. These persons invited themselves into the couple's home and a "work contract" was signed. An agreement was also made for the couple to pay NOK 90,000 in advance for materials etc. The victims were helped by the fraudsters to transfer NOK 60,000 from their online bank. This enabled the fraudsters to acquire their online bank login information. The couple also paid the fraudsters NOK 30,000 in cash. The NOK 60,000 electronic transfer to the fraudsters' account with bank B was stopped and the amount returned to the couple, as the bank suspected that the transaction was the result of fraud or similar.

In early May, the couple's bank, bank A, detected withdrawals from their account that could not be explained. Two transfers, of NOK 500,000 and NOK 25,000, to different accounts, were identified. The two recipient accounts, in banks C and D, were both in the names of the suspects. Another transfer of around NOK 90,000 was also made, but this transfer was returned by bank B. In addition, bank A had prevented another two transfers from the victim's account, of NOK 300,000 and NOK 60,000. Meanwhile, the banks involved had started communicating with each other about the matter. They had also filed STRs and alerted the FIU via emails and telephone conversations.

The new proceeds totalling NOK 525,000 were immediately forwarded as soon as they landed in the suspects' accounts with banks C and D, both to another account they had use of in bank E and directly to two other individuals. The transfers later turned out to be payment for two different valuable objects from two different private individuals. In effect, this laundered the proceeds as the suspects bought valuable objects with documents of authenticity, something which could give the

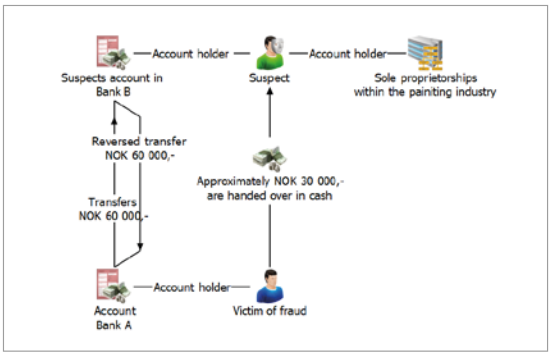



*Figure 7: Illustration of the money trail*

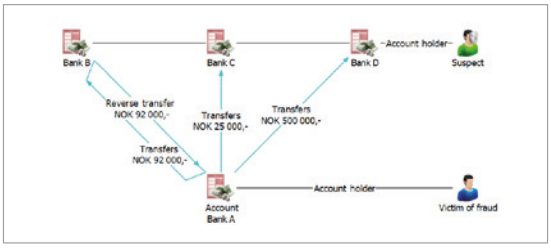



*Figure 8: Illustration of the money trail*

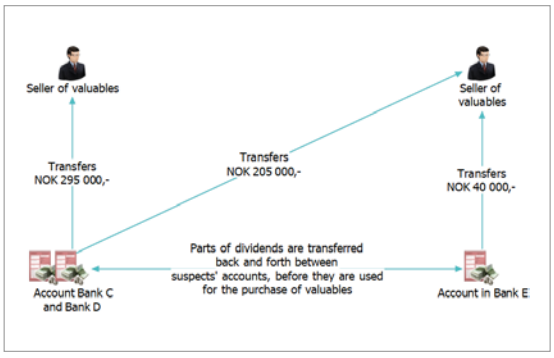



*Figure 9: Illustration of the money trail*

appearance that the criminal proceeds had legitimate origins. This happened before the FIU or the banks were able to react and stop the money transfers.

However, with a joint effort and understanding of the situation on part of the banks, as well as good contact with the FIU analysis team, the money could quickly be traced to identify the criminal proceeds and intercept them. This resulted in orders freezing transactions involving five accounts and NOK 650,000. The FIU's order to freeze the transactions has now been transferred to the local police, which have confiscated the funds in the course of the criminal investigation.

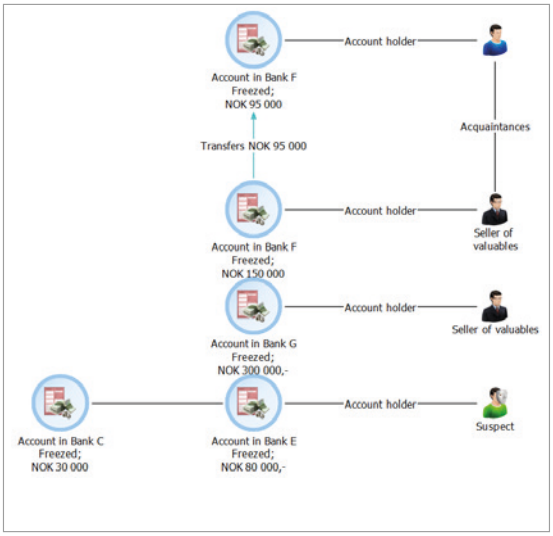



*Figure 10: Illustration of the money trail*

**Child sexual abuse, sexual crime – convictions**

In this area, the FIU's aim is for the National Criminal Investigation Service and the police districts to open criminal investigations and obtain convictions based on information provided by us. Examples of cases resulting in convictions:

- Man in his 50s sentenced to 5.5 years in prison for commissioning online sexual abuse.
- Man in his 60s sentenced to 13 years in prison for commissioning online sexual abuse.
- Man in his 40s sentenced to 13 years in prison for commissioning online sexual abuse.
- Man in his 30s sentenced to 13 years in prison for commissioning online sexual abuse.
- Man in his 70s sentenced to 120 days in prison.

# 6. National collaboration

## 6.1. OPS AT

The OPS AT project was formally launched on 25 August 2021 under the auspices of the Public-Private Digital Interaction Programme (abbreviated DSOP) to prevent money laundering and financing of terrorism in collaboration between the private and public sectors, abbreviated OPS AT in Norwegian. The idea behind OPS AT is that closer national collaboration between the reporting entities and relevant authorities will strengthen society's ability to prevent and uncover money laundering and financing of terrorism. The purpose of OPS AT is improved protection of the financial and economic system and society overall. The objective is to establish better coordination and information sharing between the financial industry and public authorities. By sharing information about developing trends, issues and risk-mitigation measures, the reporting entities and the authorities can direct a better and more targeted effort against money laundering and financing of terrorism.

OPS AT aims to improve efficiency and quality of the efforts to combat money laundering and financing of terrorism. This will be achieved by

- increased interaction, communication and exchange of information between actors in the financial industry and the public sector
- share information about trends and threat levels
- discuss and put forward proposals for risk-mitigation measures
- coordinate the use of resources where possible and practical
- raise anti-money laundering expertise among the reporting entities and public authorities
- initiate and carry out projects to improve the anti-money laundering efforts

OPS AT is organised with an administration consisting of two staff members employed by Bits AS. The administration plans and holds regular meetings and develops the interaction platform. OPS AT works closely with relevant boards and committees in Finance Norway, the main financial industry association. OPS AT furthermore consists of a steering group, a core group and three working groups made up of representatives from banks, insurance companies and relevant public authorities. The groups are managed by Bits. The figure below shows the management model and the flow of information between the different groups.

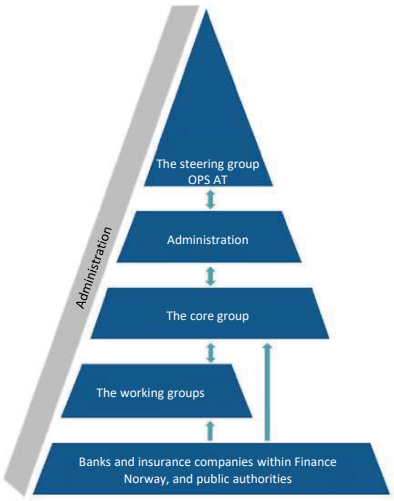



*Figure 11: OPS AT management model.*

**The steering group**
The steering group defines the strategy and framework for the collaboration and is composed of representatives from relevant authorities, reporting entities and the FIU.

**The core group**
The core group will identify threats and assess and prioritise measures to strengthen the efforts against money laundering and financing of terrorism. Issues identified by the working groups are raised with and discussed in the core group. The FIU's core group representative has made two presentations: a review of the information package and a general review of the FIU's processing and review of STRs.

**The working groups**
Participants in the working groups will use their expertise to shed light on topics and resolve specific issues in the relevant working group. Relevant issues and topics will be presented to the core group and, if relevant, the steering group. Three working groups were established in 2021: cryptocurrencies, trends and threats, and insurance. The FIU has one representative in the cryptocurrencies working group and one in the trends and threats group. The FIU representatives have held two presentations in 2021: a review of cryptocurrency tracing tools and a review of relevant trends and threats.

| OPS AT participation | |
|---|---|
| Financial industry reporting entities | 18 |
| Public authorities | 5 |
| Entities not subject to reporting requirements | 2 |

*Table 6: OPS AT participation.*

## 6.2. The Contact Forum

A representative from the FIU meets on behalf of Økokrim in the Contact Forum for Combating Money Laundering and Financing of Terrorism.

The Forum was created by cabinet order in October 2014. Its purpose is to help ensure a coordinated national effort against money laundering, financing of terrorism and financing of dissemination of weapons of mass destruction.

The Forum is composed of representatives from

- The Ministry of Justice and Public Security
- The Ministry of Finance
- The Ministry of Foreign Affairs
- The Norwegian Financial Services Supervisory Authority
- The National Police Directorate
- The Norwegian Police Security Service
- The Office of the Director of Public Prosecutions
- The Tax Administration
- The Norwegian Customs Directorate
- The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim)

The Forum is chaired by the Ministry of Justice and Public Security. The head of the Norwegian delegation to the Financial Action Task Force (FATF) attends the meetings. Depending on need and the topics raised in the meetings, representatives of the following agencies may be invited to the meetings:

- The Supervisory Council for Legal Practice
- The Norwegian Gaming Board
- The National Joint Analysis and Intelligence Centre
- The Norwegian Police University College

Other ministries and agencies are invited if needed, and representatives of the reporting entities can attend with observers when relevant topics are raised.

The Forum has the following duties in the effort to combat money laundering, financing of terrorism and financing of dissemination of weapons of mass destruction:

- 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 the effort to prepare necesSTRy updates to Norway's national risk assessment for money laundering and financing of terrorism
- encourage development of procedures for collaboration between agencies and between agencies and the private sector
- identify needs to follow up international developments in regulations and norms in Norway
- identify needs for research and strategic analysis work into money laundering and financing of terrorism

## 6.3. Supervision

Effective combating and prevention of money laundering and financing of terrorism and weapons of mass destruction require close collaboration between all involved authorities. Sharing information between the FIU and the respective supervisory authorities will therefore be decisive in enabling the agencies to fulfil their duties and achieve national objectives.

In order to optimise cooperation, the Financial Supervisory Authority of Norway and the FIU hold meetings every six months to share experience and information. In addition, the FIU is in continuous dialogue with the Financial Supervisory Authority about various issues and challenges that concern both. In 2021, these meetings were held in January and September. The meetings with the Financial Supervisory Authority in 2021 have, among other things, covered the preparation of a new collaboration agreement, which was ready to be signed at the end of 2021. Furthermore, the FIU has prepared eight topical reports for the Authority's supervisory activities over the course of 2021. The FIU has also prepared intelligence reports and proposed audits.

In 2021, the FIU has also worked to prepare collaboration agreements with the Norwegian Gaming Board and the Supervisory Council for Legal Practice. These agreements aim to strengthen collaboration and flow of information between the FIU and these two supervisory bodies.

## 6.4. Supervisory authorities

The overall follow-up of the government's action plan against money laundering and financing of terrorism also entails a clear expectation of productive and close interaction between all involved public-sector actors.

To live up to this and strengthen the FIU's and Økokrim's collaboration with the Tax Administration, as well as ensure a good flow of information between agencies, a representative from the Tax Administration has been embedded with the FIU since autumn 2021. We hope the experience gained from this project will also inform collaboration and collaboration methods with other supervisory authorities.

In addition, several meetings are held every year between the tax authorities' intelligence department, the FIU and Økokrim's intelligence function.

# 7. International cooperation

## 7.1. FATF

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

In spite of the pandemic, the FATF has continued to maintain a strong focus on combating money laundering and financing of terrorism. Most of the scheduled meetings were held digitally in 2021. FATF has carried out several country evaluations in 2021. Some of them were carried out in person, while others were carried out in a combination of physical visits and digital meetings.

### FATF

- FATF was established in July 1989
- Norway has been a FATF Member since 1991
- 39 Members
- FATF is the global money laundering and terrorist financing watchdog.
- The FATF has developed the FATF Recommendations, or FATF Standards, which ensure a co-ordinated global response to prevent organised crime, corruption and terrorism
- The FATF monitors countries to ensure they implement the FATF Standards fully and effectively

*Source: FATF*

In cooperation with the Egmont Group of Financial Intelligence Units, the FATF has published a report analysing opportunities and issues arising from new technology: Digital Transformation of AML/CFT for Operational Agencies. An updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers has also been published, as has a report titled Money Laundering from Environmental Crime.

The latter concludes that many countries fail to fully consider the risk of this type of crime as part of their national risk assessments in relation to money laundering and financing of terrorism. It is estimated that up to USD 281 billion are laundered through this sector every year, often through shell companies and trade-based money laundering. Norway was represented on the project group by staff from the FIU, Økokrim's environmental crime team and the Ministry of Climate and Environment.

The FATF also initiated a new project about the trade in antiquities: Antiquities and other Cultural Objects as a tool for ML/TF. Norway participates in this project with representatives from the FIU, Økokrim's environmental crime team and the Ministry of Culture and Equality. The plan is to complete this work in 2022.

In the field of financing of terrorism, the FATF published a report about financing of terrorism motivated by right-wing extremism.

A representative from Norway's FIU participates in the FATF's evaluation of Germany's AML & CTF efforts. The evaluation report will be discussed and finalised at the FATF's plenary meeting in June 2022.

## 7.2. EGMONT Group of FIUs

The Egmont Group of Financial Intelligence Units (Egmont Group) is an international association of 167 national FIUs. In addition, a number of international organisations have status as observers. The national FIUs in the Egmont Group share skills, knowledge and financial intelligence, in part through a closed and encrypted infor-

mation channel. The purpose is to combat money laundering and financing of terrorism and associated crime. Norway's FIU has been a member of the Egmont Group since 1993. The members of the Egmont Group of FIUs commit to work to achieve the aims laid down in the group's Charter and Principles for Information Exchange. This requires cooperation and sharing of information with the other member FIUs. Members are also required to take part in the group's meetings and other activities.

**National promotion of international information sharing**
In autumn 2021, the FIU organised a digital lunch conference with participants from Økokrim and the police districts' financial crime teams. At the conference, the FIU informed about international information sharing via the Egmont Group as an efficient way of obtaining information.

In addition to this, the FIU promotes international information sharing via the Egmont Group through the Norwegian Police University College's podcast series.

**International meetings**
Due to the Covid-19 pandemic, all international meetings between FIUs in 2021 were held digitally. The FIU participated in Egmont Group meetings in February, June, July, September and December. A representative from Norway's FIU has chaired one of the Egmont Group's four working groups (Policy and Procedures Working Group) and has also served on the Egmont Committee, which is the group's board. The Policy and Procedures Working Group has finished a number of important projects in 2021, inter alia the report Addressing Impediments to Information Exchange Between FIUs (about efficient information exchange) and a GlosSTRy for Key Egmont Group Terminology to define the most common terms within money laundering and financing of terrorism.

**International projects**
In autumn 2021, Norway's FIU started a project in cooperation with our Danish and Swedish counterparts. Meetings have been held digitally and in Copenhagen. We expect to complete the project in 2022.

**Requests for and sharing of information with other FIUs**
In 2021, Norway's FIU has shared information in one way or another with 60 national FIUs. Last year we also forwarded 194 requests for information to other national FIUs, of which we received replies to 182 by the end of the year. We received 68 requests for information from other FIUs in 2021, and we replied to all of them within the deadlines established by the Egmont Group.

We also received 3097, mainly automatically generated, information messages from European FIUs.

It is also worth noting that the number of requests issued by the Norwegian police increased 177 %. This is probably due to our promotion of the possibilities for obtaining information through the Egmont Group. We have also seen an increase in the number of replies received, but this is a natural consequence of the Norwegian police issuing more requests.

## 7.3. The EU FIU platform

In 2006, the EU Commission established the EU FIU Platform to facilitate information exchange between European FIUs and cooperation between them. The platform is a decentralised computer network supporting the national FIUs in the EU and Norway in combatting money laundering and financing of terrorism. All 28 national FIUs in the EU and the Norwegian FIU are linked to the platform. The main purpose is increased and more secure information exchange between the European FIUs, who exchange requests, share information and cross-check persons and organisations through the platform. The platform is operated by the European Commission Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA).

# 8. Guidance, supervision and communication

The FIU is a competence centre for combatting money laundering and financing of terrorism and therefore has a number of activities intended to increase the awareness of and use of financial intelligence. For this purpose, the FIU has participated at a number of seminars and conferences and given presentations about financial intelligence for various obliged entities, from one-to-one meetings to large conferences, e.g. conferences organised by Finance Norway. Also, representatives of the Norwegian FIU have held presentations for specialist police agencies, university colleges and supervising authorities.

The FIU wants, and has as its aim, to be easily available to the obliged entities, and our compliance team is in daily contact with reporting entities. This contact takes place mostly via the phone and email. In 2021, the FIU received around 800 calls to our telephone service. The information and guidance needs are many and varied. Mostly we are contacted by reporting entities who are uncertain about the extent of their investigation and reporting obligations. We have also published information and guidance about this on our web pages, and many will benefit from studying the information published there. Sometimes, errors occur in the reporting or the report(s) lack information that we want the obliged entity to provide. In 2021, we contacted 59 reporting entities to follow up such errors.

One of the most important events in 2021 was the Money Laundering Conference, which was organised in November in collaboration with Finance Norway and the Financial Services Authority. Due to Covid-19 restrictions, the conference was held at the Deichman public library in Bjørvika and streamed live. There were more than 700 attendees from both obliged entities and supervisory authorities at the conference. The Money Laundering Conference is considered the most important forum for sharing knowledge and establishing contacts between obliged entities and supervisory authorities. This year's main topic was "A changing world" and raised a number of issues related to money laundering and financing of terrorism in this context. The recently published EU package was also a topic, which contains new measures in the field.

Apart from participation at seminars and conferences, communication via our web pages and social media is very important. During the second and third quarters, the FIU published information about the Black Wallet project[11], in addition to relevant publications from FATF and other relevant information. Of particular importance was the publication of a procedure for freezing transactions. Our communication relating to the procedure has, in our experience, improved cooperation between the FIU and the obliged entities to make the procedure for freezing transactions faster and more efficiently. Our web site, okokrim.no, is viewed as an important channel for distributing information to the reporting entities on which the FIU publishes and shares news, guidance, indicator lists etc.

In 2021, the FIU prepared an information package about Virtual Asset Service Providers (VASPs). The aim was to provide information to obliged entities that they could use in combatting money laundering and financing of terrorism. The package contained a thematic report intended to map the threats and vulnerabilities encountered by the reporting entities plus information about tools and mechanisms for tracing cryptocurrency movements. The information package was forwarded to the industry associations and obliged entities in the FIU's contact list.

The development of a new and improved Altinn form has been a priority for the FIU the last few years. The aim is to improve cooperation with the obliged entities and in combatting money laundering and financing of terrorism. Our aim is that the new form will be more dynamic and provide better and more precise information. The new

11 Indicator lists prepared by the Swedish and Finnish FIUs which visualise risks for the fintech industry and which distinguish between threats, vulnerabilities and red flags.

form will also be better adapted to the different groups of obliged entities and applicable rules and regulations. Many obliged entities have been involved in the development of the new form and have contributed valuable insight and feedback. For the FIU, the new form will provide more efficient use of data in operative analyses which can be forwarded to relevant actors and preparation of products for input to strategic analyses (statistics, trend reports etc.). The project is carried out by a private consultancy company and the Police ICT Services in collaboration.

Unfortunately, the launch date for the new Altinn form has been postponed. The launch was dependent on the outcome of the Schrems II judgment[12]. While waiting for the judgment to be passed, the FIU has considered that the preparation of the new Altinn form should continue, something which would reduce the delay. A new launch date will be communicated to the obliged entities once it is fixed. More information about the Schrems II case can be found here: https://www.altinndigital.no/nytt-i-altinn/oppfolging-av-schrems-ii-i-digitaliseringsdirektoratet-og-altinn/

12 On 16 July 2020, the European Court of Justice issued its decision in a test case concerning transfer of personal data to the USA. The decision is known colloquially as "Schrems II", named after the Austrian privacy activist Max Schrems, who filed a complaint with the Irish Data Protection Commissioner to stop the transfer for personal data from Facebook Ireland to Facebook Inc. in the USA on the basis that his personal data was not sufficiently protected in the USA.