Financial Intelligence Unit

ZOLL

Annual Report 2019

Financial Intelligence Unit

Annual Report 2019

Financial Intelligence Unit

Table of Contents

Dear Readers,

In the report year 2019, the Financial Intelligence Unit (FIU) continued its work under the umbrella of the Central Customs Authority (GZD) for the third year in a row and expanded it further. As ever, I am convinced that constant adaptation and advancing development are the keys to successfully and efficiently combating money laundering and countering terrorist financing.

With regard to the increase in the incoming suspicious transaction reports (STRs), the trend of the previous years continued in 2019. For the first time, the amount of STRs received was in the six-figure region. This trend progressed, and the FIU sought to respond to it by increasing its staff and also continuing to implement risk-based processing.

As part of its role as a central agency, the FIU further strengthened the configuration of its filter function and the risk-based approach of its activities in 2019 in order to collate the information that it received centrally as well as additional recorded information in a targeted manner and process it in a risk-based manner. In this context, the FIU established key risk areas in the range of money laundering and terrorist financing based on the information and findings available to it and under consideration of the National Risk Analysis. In this regard, I wish to draw your attention specifically to the “Typologies and Trends” section in this annual report.

The decision to restructure the FIU, creating seven divisions from the previous two divisions, was also made in order to absorb the increase in the incoming STRs, to provide for the risk-based orientation and to deal with the steady increase in personnel.

Cooperation with national partner authorities was further consolidated over the past year and expanded via new measures, such as a concerted campaign with the supervisory authorities and mutual work shadowing. By founding a public-private partnership (the Anti Financial Crime Alliance, AFCA), which had never been done before in the field of financial crime, the FIU was also able to set up a permanent exchange with the private sector. Within the scope of international cooperation, the FIU continued its success both in its operational cooperation and in its committee work.

The 2019 annual report from the FIU is being published in an extraordinary time. The spread of the SARS-CoV-2 virus and the fight against it is dominating world events and changing politics, the economy and the financial markets. The FIU will also face new challenges due to these changes. Thanks to the concrete changeover to a risk-oriented working approach, expanding effective national and international cooperation with partner authorities and reporting entities and constant expansion of staff, the FIU will be equal to these tasks in the future.

Christof Schulte
Head of the FIU

Overview of the FIU

A Risk-oriented Approach

Further Development of the FIU – Implementation of a New Organisational Structure

Overview of the FIU

The FIU is the German national central agency for the receipt, collection and analysis of reports on unusual or suspicious financial transactions that could potentially be related to money laundering or terrorist financing. It is established within the Central Customs Authority (GZD) as an independent and administrative authority.

In accordance with international provisions, all countries are obliged to establish such Financial Intelligence Units. In the Federal Republic of Germany, the FIU receives all suspicious transaction reports issued by reporting entities, as it is the national central agency for investigating financial transactions. The FIU then collects and analyses them. Using national forms of cooperation and a growing international network of other FIUs, the German FIU contributes to a global pool of expertise and creates significant synergies worldwide. It acts as a real hub, bringing all relevant information and data together so that a comprehensive assessment of the suspicious instances of money laundering or terrorist financing can be executed. Only reports that are categorised as valid in the operational case-by-case analysis are subsequently forwarded to the law enforcement agencies and other responsible bodies.

By collecting information, the FIU can identify new methods and trends in the areas of money laundering and terrorist financing using non case-specific strategic analysis in addition to operational analysis. The findings obtained serve as a piece of information that can be used for operational analysis. In addition, these findings are provided to the reporting entities and partner authorities in the form of reference or typologies paper. Raising awareness among and creating a dialogue with the reporting entities and working together and coordinating with the supervisory authorities are further important preventive tasks for the FIU.

A Risk-oriented Approach

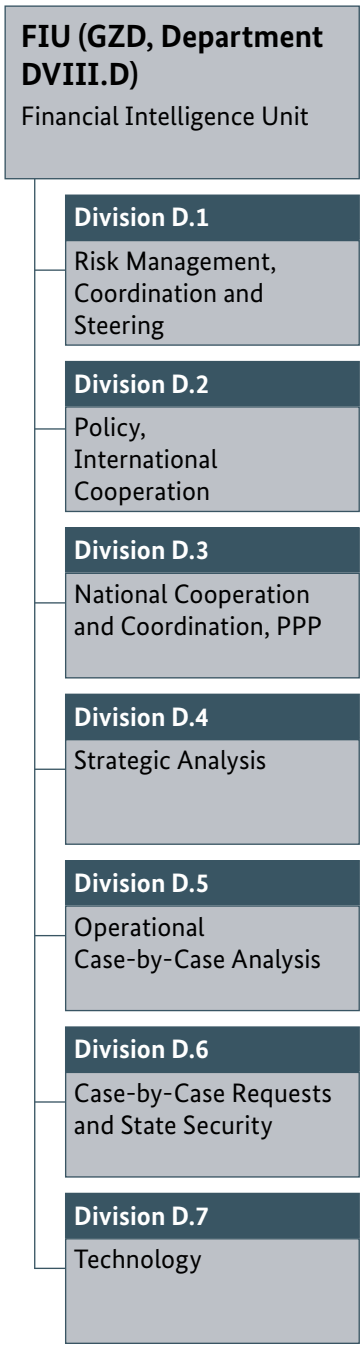
To create intermeshing with the National Risk Analysis (NRA)[1] and simultaneously identify new methods and phenomena in the areas of money laundering and terrorist financing, the orientation of the FIU has become increasingly based on risk in order to fall in line with the international provisions.[2] In this context, the FIU established key risk areas for continuous evaluation in the areas of money laundering and terrorist financing with the support of the law enforcement agencies in summer 2019. These key risk areas serve as steering and prioritisation tools for operational analysis work. In this way, the information that the FIU receives as a central body is brought together in a targeted risk-oriented manner and the focus on valid facts, as defined by the FIU filter function, is rendered even more effective.

1 The NRA's final report was published in October 2019 (it can be viewed on the website of the German Federal Ministry of Finance, see https://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2019-10-19-erste-nationale-risikoanalyse_2018-2019.html).
2 For a detailed explanation of the FIU's risk-based orientation, see the "Typologies and Trends" section.

Further Development of the FIU – Implementation of a New Organisational Structure

The FIU is set up as an independent and functional administrative authority in order to perform its duties. Since its placement within the GZD, it has been split into two divisions, with one handling general and cross-sectional affairs and the other dealing with operational analysis of suspicious transaction reports. In the course of the FIU's continuing personnel expansion, it was decided in 2019 that restructuring would be undertaken. The new structure of the FIU is to be implemented in 2020. A total of seven divisions will be created, which will be split into departments and units. The structure meets the requirements for a risk-based approach and the growing demands due to an increase in the total number of STRs received as well as the gradual increase in personnel to a target of 475 jobs (including management) that this entails. Further expansion of personnel is planned for 2020 in the course of attaining this target so that specialist tasks can be fulfilled and the predicted report volumes can be managed.

> Further specialist information and current news can be found on the FIU's web page at www.fiu.bund.de.



New Organisational Structure

The main tasks of **Division D.1** are to initiate and accompany the process-oriented further development of the FIU's fulfilment of its duties. Among other things, parliamentary and press queries are coordinated here.

Division D.2 bundles the following tasks: policy (including legal issues, business standards and development, FIU-specific organisational development and controlling) and international cooperation.

Division D.3's mission is to ensure cooperation and exchange with the national law enforcement agencies and supervisory authorities and with the reporting entities for the German Anti-Money Laundering Act. This also comprises cooperation within the scope of public-private partnerships (PPP).[3]

The Strategic Analysis department within **Division D.4** executes non case-specific evaluations and analyses. Findings on typologies and trends are forwarded to other areas of the FIU, the authorities and reporting entities, dependent on the situation.

Case-by-case analysis within the remit of combating money laundering is executed in **Division D.5**. Here, suspicious transaction reports are subject to an initial risk-based assessment, analysed and disseminated to the relevant authorities as necessary.

Division D.6 is the central contact point for all national and international partners in the field of operational cooperation. STRs related to terrorist financing or matters of state security are analysed in the "State Security" department.

Division D.7 is charged, inter alia, with centralised specialist supervision of the FIU-specific specialised IT software solution goAML and coordinating the further development of the IT landscape for the FIU.

3 For more information on the subject of PPP, see the section on "National Cooperation".

Suspicious Transaction Reports (STRs)

Total Number of STRs for Reporting Year 2019

Total Number of STRs, Categorised by Subgroups of Reporting Entities

Assessment Results for STRs in 2019

Feedback from Public Prosecution Authorities

Temporary Freezing Orders

Transactions

Suspicious Transaction Reports (STRs)

This section illuminates the STRs that the FIU received in 2019 in detail. All reports that the FIU receives from reporting entities, fiscal authorities and supervisory authorities are relevant in this context.[4]

Figure 1 shows the individual steps of operational analysis from receipt of the STR up until it has been completely processed.

Receipt of report – Analysis – Decision

After electronic receipt of the STR, the report runs through an automated basic search, in the course of which the data contained in the report are matched with other databases in order to collate the findings in a targeted manner.

In the course of the subsequent initial assessment, the reports are prioritised, with particularly high priority being given to incidents that have one of the fixed key risk areas assigned to them as well as to facts with appropriate measures for securing assets (e.g. as part of urgent cases).[5]

If an STR is assigned to a key risk area in the course of the initial assessment, a deeper analysis is conducted. If it is established that assets have a link to money laundering, terrorist financing or other criminal acts, this is submitted to the responsible body in the form of an analysis report. If the FIU does not believe this to be the case, the report remains in the monitoring phase for the time being and can be used to strengthen a valid case at a later point in time. It is treated as a piece of information and can be collated with further information as required.

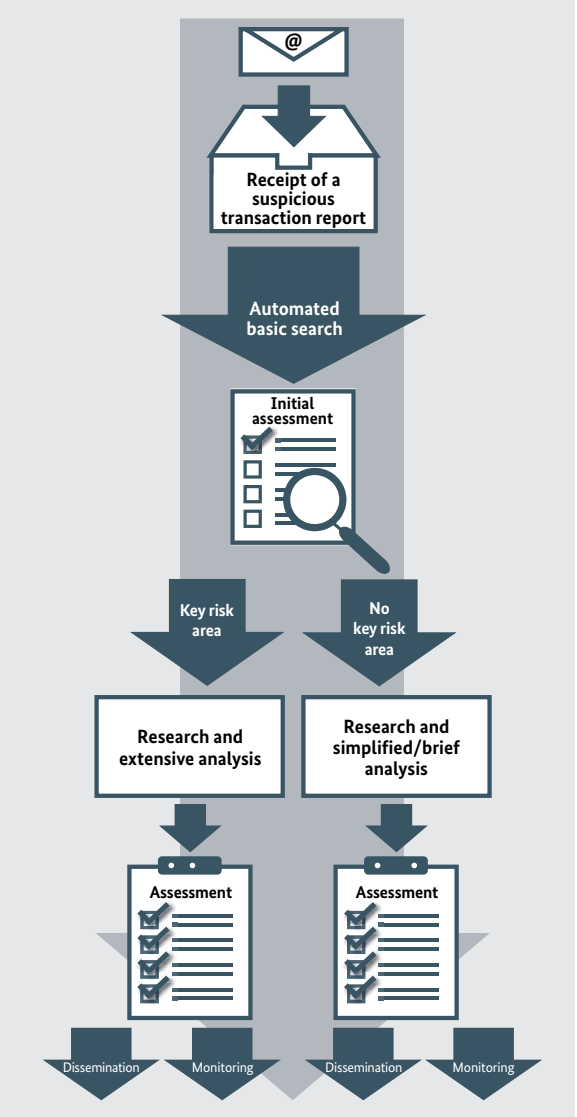


Figure 1: Process Sequence for Operational Analysis

4 Reports that have been submitted in accordance with Sections 43 and 44 of the German Anti-Money Laundering Act (AMLA) and Section 31 b of the German Tax Code (AO) are considered here. Thus, all reports and notifications that fall under Section 30 (1) No. 1-2 AMLA are listed. Information that is submitted to the FIU in accordance with Section 30 (1) No. 3-4 AMLA is not categorised here as STRs from reporting entities.

5 For a list of these key risk areas, see the "Typologies and Trends" section.

Against a backdrop of reinforcement of the risk-based approach anchored in the AMLA and the EU Money Laundering Directive and taking into account the findings of the NRA and the relevant FATF provisions in particular, the FIU will consistently maintain the comprehensive risk-based orientation of its processes in 2020 and intensify risk-oriented working methods for operational analysis.

Total Number of STRs for Reporting Year 2019

The total reporting rate again increased significantly in 2019. The FIU received a total of 114,914 STRs, an increase of 49% in comparison with the previous year 2018. In absolute terms, the increase amounts to around 37,500 reports and clearly exceeds the strong increase of the previous year of around 17,500 reports. Since 2009, the annual total number of STRs received in Germany has multiplied by a factor of almost twelve, which reflects the increased levels of awareness as well as the progressive automation of large credit institutions.

The high total number of STRs started posing a great challenge in 2017. Since then, the number of STRs received each year has almost doubled. This not only underlines the importance of exercising the filter function of the FIU more strongly, through which the valid facts are forwarded to the law enforcement agencies and other responsible bodies in a targeted manner. It also highlights that it is vital to have a risk-oriented approach that enables a targeted steering of resources to the most important issues in combating money laundering and countering terrorist financing in terms of a common understanding of risk for all actors involved.

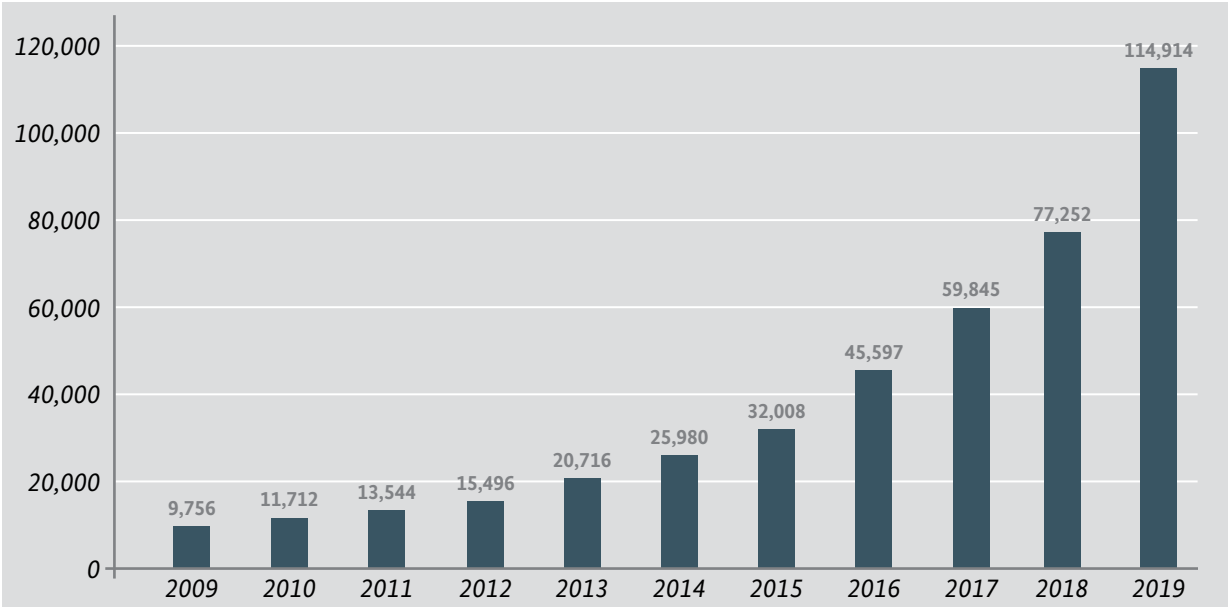


Figure 2: Development of the Number of STRs According to the AMLA (2009-2019)

In 2019, several credit institutions submitted separate STRs on the subject of the "laundromat" to the FIU for the first time. Each of these reports contained a very large number of transactions, mainly consisting of correspondent banking activities. Actors involved in these transactions had previously appeared in conjunction with large laundromats.

Laundromat
In this context, a "laundromat" describes a set of uncovered methods that are used to launder money on a grand scale which are made up of complex international company networks and transaction patterns. For example, information came to light in conjunction with a big Danish bank which involved several large German corporations and a wide variety of other German companies from different sectors acquiring goods from abroad using funds from allegedly criminal activities and then exporting them. Funds from criminal activities were thus integrated into the legitimate economy.

Total Number of STRs, Categorised by Subgroups of Reporting Entities

The increase in the total number of STRs extends to both the financial and non-financial sectors and to the authorities and other reporting entities. As before, around 98% of all reports came from the financial sector, which submitted over 35,000 STRs more than it had in 2018. Here, credit institutions are the most active group, submitting 90% of the total number of STRs. The total number of STRs for the second most active reporting group, financial service institutions, dropped from a previous total of over 10,000 reports to around 7,500 reports, thus going against the trend.

	Reporting entities	2018	2019	
Financial sector	Credit institutions	65,132	103,697	↗
	Financial service institutions	10,552	7,528	↘
	Payment institutions and electronic money institutions	264	290	↗
	Agents	35	650	↗
	Independent business persons	0	0	→
	Insurance undertakings	137	232	↗
	Asset management companies	17	42	↗
	Total of STRs from the financial sector	**76,137**	**112,439**	↗
Non-financial sector	Financial companies	7	39	↗
	Insurance intermediaries	4	17	↗
	Lawyers	22	21	↘
	Legal advisors who are members of a bar association	0	0	→
	Patent attorneys	0	0	→
	Notaries	8	17	↗
	Legal advisors	0	3	↗
	Auditors and chartered accountants	2	0	↘
	Tax advisors and authorised tax agents	4	8	↗
	Trustees, service providers for trust companies	1	15	↗
	Estate agents	31	84	↗
	Organisers and brokers of games of chance	150	754	↗
	Traders in goods	368	554	↗
	Total of STRs from the non-financial sector	**597**	**1,512**	↗
Other	Supervisory authority	54	149	↗
	Fiscal authorities	414	697	↗
	Other STRs	50	117	↗
	Total	**77,252**	**114,914**	↗

Table 1: Number of STRs According to Subgroups of Reporting Entities

The number of STRs from the non-financial sector increased disproportionately by over 150% in comparison to the previous year, while the total number of STRs overall increased by around 49%. Organisers and brokers of games of chance are the main drivers behind this increase in the non-financial sector. Significantly more reports were also received from the goods trading sector this year, where the percentage increase correlated roughly with the overall trend at just over 50%. The number of STRs from estate agents and financial companies also increased significantly. While the proportion of reports from the non-financial sector comprised just under one percent of all STRs in the previous year, this rate has now risen to just over 1.3%. Although the FIU believes that this confirms the efficacy of its previously undertaken awareness-raising and coordination measures in this sector, a significant increase in the numbers of reports from the non-financial sector is still planned and expected.

The authorities and other reporting entities also submitted far more reports than were received in the previous year. The STRs submitted by the supervisory authorities almost tripled between 2018 and 2019. For example, supervisory authorities informed the FIU of abnormalities related to money laundering which they had identified when auditing supervised companies, thus expanding the information collated by the FIU with another perspective. The proportion of reports in this area amounted to under 1% of the total number of STRs received. Further awareness raising and an increase in the proportion of reports is also an objective here.

Registered and Active Reporting Entities

In 2017, the year that the electronic reporting system for STRs regarding money laundering was put into operation, around 2,000 reporting entities registered in the system, with the clear majority of the registrations coming from the financial sector. In 2018, over 1,100 more reporting entities joined them, and high growth in registrations was seen from traders in goods, estate agents, financial service institutions and agents. In 2019, there were approx. 2,000 new registrations. In the financial sector, there were few new registrations (with the exception of agents) because the registration rate is already very high for this sector. However, in the non-financial sector, the registration numbers increased significantly for the notaries (over 500) and estate agents (over 400) by the end of the year due to numerous awareness raising measures and with a view to the upcoming legal obligation[6]. In the gambling sector, the number of registered reporting entities increased seven-fold within a year, jumping from 45 to over 300. Reporting entities also used the registration to access the internal area of the FIU website and view the information published by the FIU (including typologies papers). Thus, the registration of a reporting entity does not necessarily presuppose that suspicion of money laundering or terrorist financing must be present.

While Table 1 breaks down the number of STRs received by individual subgroups of reporting entities, Table 2 below shows the number of reporting entities that actually submitted a report in 2019 (active reporting entities).

6 The reporting entities must register with the FIU in accordance with Section 45 (1) No. 2 AMLA, regardless of whether they submit an STR or not. The registration obligation shall come into force upon the launch of the new information network for the FIU and on 1/1/2024 at the latest, in accordance with Section 59 (6) AMLA.

	Reporting entities	2018	2019	
Financial sector	Credit institutions	1,232	1,274	↗
	Financial service institutions	53	87	↗
	Payment institutions and electronic money institutions	22	21	↘
	Agents	9	21	↗
	Independent business persons	0	0	→
	Insurance undertakings	41	57	↗
	Asset management companies	14	13	↘
	Total of reporting entities from the financial sector	**1,371**	**1,473**	↗
Non-financial sector	Financial companies	4	4	→
	Insurance intermediaries	2	5	↗
	Lawyers	13	18	↗
	Legal advisors who are members of a bar association	0	0	→
	Patent attorneys	0	0	→
	Notaries	5	15	↗
	Legal advisors	0	2	↗
	Auditors and chartered accountants	2	0	↘
	Tax advisors and authorised tax agents	3	4	↗
	Trustees, service providers for trust companies	1	4	↗
	Estate agents	20	47	↗
	Organisers and brokers of games of chance	24	116	↗
	Traders in goods	146	174	↗
	Total of reporting entities from the non-financial sector	**220**	**389**	↗
	Total	**1,591**	**1,862**	↗

Table 2: Number of Active Reporting Entities

In 2019, the number of reporting entities that submitted at least one report within the year increased from 102 to 1,473 for the financial sector. The non-financial sector added 169 active reporting entities to the previous figure (making a new total of 389 active reporting entities). Thus, the reporting entities from the financial sector submitted, on average, around 76 STRs in 2019, whereas the non-financial sector submitted an average of just under 4 reports per active reporting entity to the FIU. The evaluation of the absolute reporting figures shows that the most active reporting entity from the financial sector submitted around 18,000 STRs and the most active reporting entity from the non-financial sector submitted over 80 STRs.

One explanation for the differing reporting behaviour in the financial and non-financial sectors is that credit institutions in particular have comparatively sophisticated, established monitoring systems whose effectiveness is subject to the central control of the German Federal Financial Supervisory Authority (BaFin). In addition, the structure of a typical company in the non-financial sector differs greatly from the structure of a company in the financial sector. While handling large quantities of transactions constitutes a core activity for credit institutions and financial service institutions, the majority of the reporting entities from the non-financial sector are often relatively small companies.

Assessment Results for STRs in 2019

If sufficient evidence for connections with money laundering, terrorist financing or other crimes is established in a case analysis, all relevant STRs are disseminated in a bundle, e.g. to the competent State Office of Criminal Investigation (LKA). This was the case for slightly more than a third of the fully analysed STRs in 2019, while in 2018, over half of all STRs were disseminated in a bundle. Thus, the FIU performed its filter function even more efficiently under the strain of the constantly increasing total number of STRs. As part of performing its duties and with its risk-based approach, the FIU concentrated on complex, valid facts and transferred these to the competent authorities.

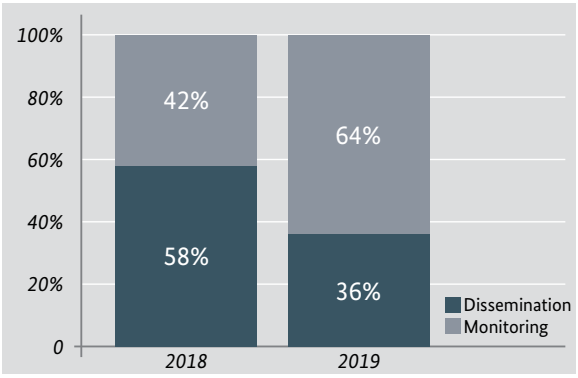


Figure 3: Breakdown of Reports Following Assessment[7]

Figure 4 shows a differentiation according to the recipients of the FIU's dissemination.

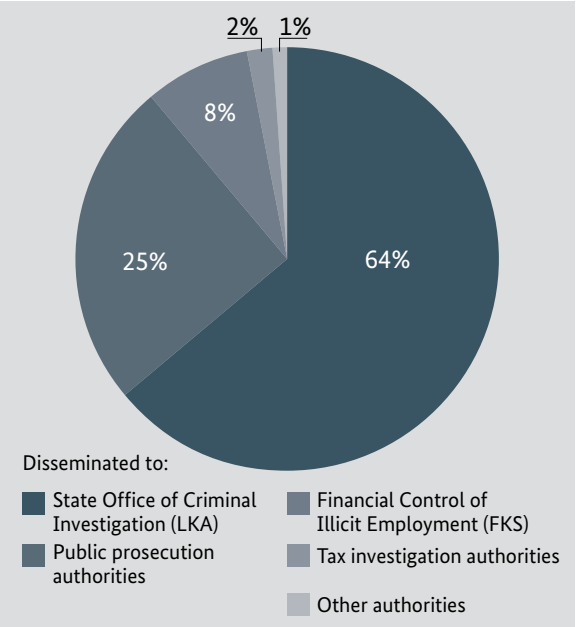


Figure 4: Breakdown of Reports by Recipients of Dissemination

The State Offices of Criminal Investigation and public prosecution authorities continue to be the main recipients of disseminations from the FIU. As in the previous year, just under 90 % of all analysis reports were sent to these two addressee groups. While the number of disseminations in 2019 decreased on the whole, a few more cases were disseminated to the Financial Control of Illicit Employment (FKS) (6 % the previous year, now 8 %) in both relative and absolute terms. The proportion of disseminations to the tax investigation authorities sank from a previous 5 % to 2 % in 2019. Other authorities, such as intelligence services, customs investigation services and the federal police, constituted around 1 % of the dissemination volume, which remains unchanged from the previous year.

7 The number of submissions for 2019 also includes some STRs that were received in 2018 and were fully analysed in 2019.

Feedback from Public Prosecution Authorities

According to the provisions of the AMLA, the competent public prosecution authority communicates to the FIU the indictment and outcome of proceedings including all decisions on withdrawal of prosecution for incidents regarding which the FIU forwarded information. This is done by sending a copy of the indictment, a penalty order, a decision on a withdrawal of prosecution or a conviction.

At 17,565 feedback reports from public prosecution authorities, an increase of 3,500 reports can be observed compared to the previous year. This represents an increase of 25 %.

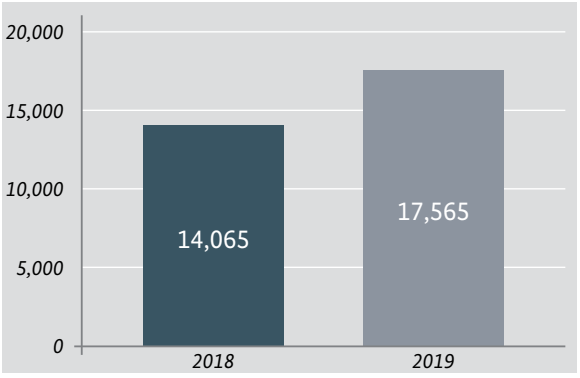


Figure 5:
Number of Feedback Reports from Public Prosecution Authorities

The greatest proportion of feedback reports received by the FIU from public prosecution authorities in 2019 concerned incidents from the period after 26 June 2017. In this period, the FIU, which had just been set up under the umbrella of the Central Customs Authority, took up its duties. Only 1,000 feedback reports, or just under 6 %, are based on STRs that were processed before this date. For 855 feedback reports, no direct connection could be drawn with the database of the FIU.

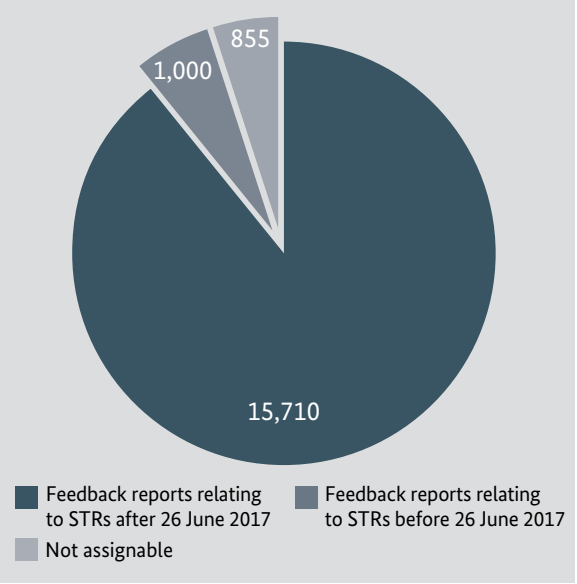


Figure 6:
Breakdown of Feedback Reports from Public Prosecution Authorities in 2019

A total of 343 of the feedback reports relating to STRs which were received after 26 June 2017 concerned convictions, penalty orders and indictments. This amounts to around 2.2 % of the feedback reports, constituting a slight increase in comparison to the previous year.

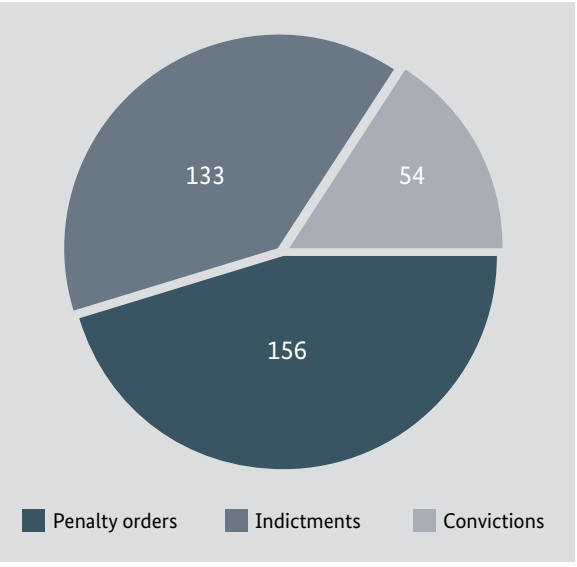


Figure 7:
Overview of the Convictions, Penalty Orders and Indictments Relating to Reports Received after 26 June 2017

At least 56 % of the convictions and penalty orders listed in the above figure were issued for financial intermediary activities.[8] Other clusters can be seen for various forms of fraud; convictions and penalty orders were also issued for so-called parcel agents. When fines were imposed as part of convictions, they amounted to approx. EUR 1,750 on average. When custodial sentences were imposed, they amounted to just under 12 months on average. For penalty orders, the average fine amounted to around EUR 2,200 and in three cases the penalty order was issued with a custodial sentence. In addition, cautions were issued in 21 cases in which fines were reserved during a probation period. In a total of 78 cases, illegally obtained assets were confiscated.

Parcel Agents
The parcel agent's (also termed a goods manager or postal provider) activity consists, in the main, of accepting, relabelling and forwarding parcels to the addresses stated by the principal. The agent is promised remuneration for this. The parcels to be forwarded, however, contain goods that have been ordered via fraud, e.g. with fake identities or using illegally obtained credit card information. The parcel agent becomes guilty of involvement with money laundering due to negligence and must, as the official recipient of the goods, also deal with the civil law claims from the companies suffering damages.

As in the previous year, orders for withdrawal of prosecution constitute an overwhelming majority of public prosecution feedback reports, amounting to approximately 97.8 %. Overall, however, it should be noted that the proportion of AML proceedings that lead to a conviction and/or a penalty order is not a sufficient tool for measuring the effectiveness of the reporting system. In just under 200 orders for withdrawal of prosecution, it was explicitly noted that the proceedings for money laundering alone had been stayed, but that separate investigations continued due to the predicate offence (e.g. fraud) and/or that the proceedings had been separated. A significant reason for this, according to the FIU's estimation, are the requirements pertaining to the facts of the case, which are particularly challenging for money laundering (Section 261, German Criminal Code, StGB). For a criminal conviction for money laundering in accordance with Section 261 of the StGB, not only the predicate offence but also the act of money laundering and a causal relationship between the predicate offence and the act of money laundering must be proven. On the other hand, proof of money laundering often does not contribute any "added value" in terms of criminal procedural law. In particular in cases in which the perpetrator of the predicate offence is also the perpetrator of the act of money laundering, the act of money laundering is generally not penalised in accordance with Section 261 (9) Sentence 2 StGB. In other cases, too, the sentence is frequently not significantly more severe as a result of the additional criminal conviction due to money laundering. Therefore, stayed AML proceedings do not necessarily mean that the STRs they are based on should be considered ineffective.

8 Insofar as the feedback reports were assessable.

Case Study – From STR to Conviction [9]

Initial STR

A business customer reported to the account-holding bank that a transfer of funds had been made illegally to another business account held at this bank. Due to this objection, the transfer amount was not credited to the recipient and the bank submitted a STR.

FIU Analysis and Dissemination

During the FIU's analyses, it was noted that Mr G, the CEO of the company, was intended to be the beneficiary of the transfer. He is a Spanish citizen and his permanent place of residence is also located in Spain. Furthermore, it was established that the account of the payment recipient was only opened two months before the alleged fraudulent transfer. The incident was immediately forwarded to the competent State Office of Criminal Investigation as the FIU recognised that it was a matter of particular urgency.

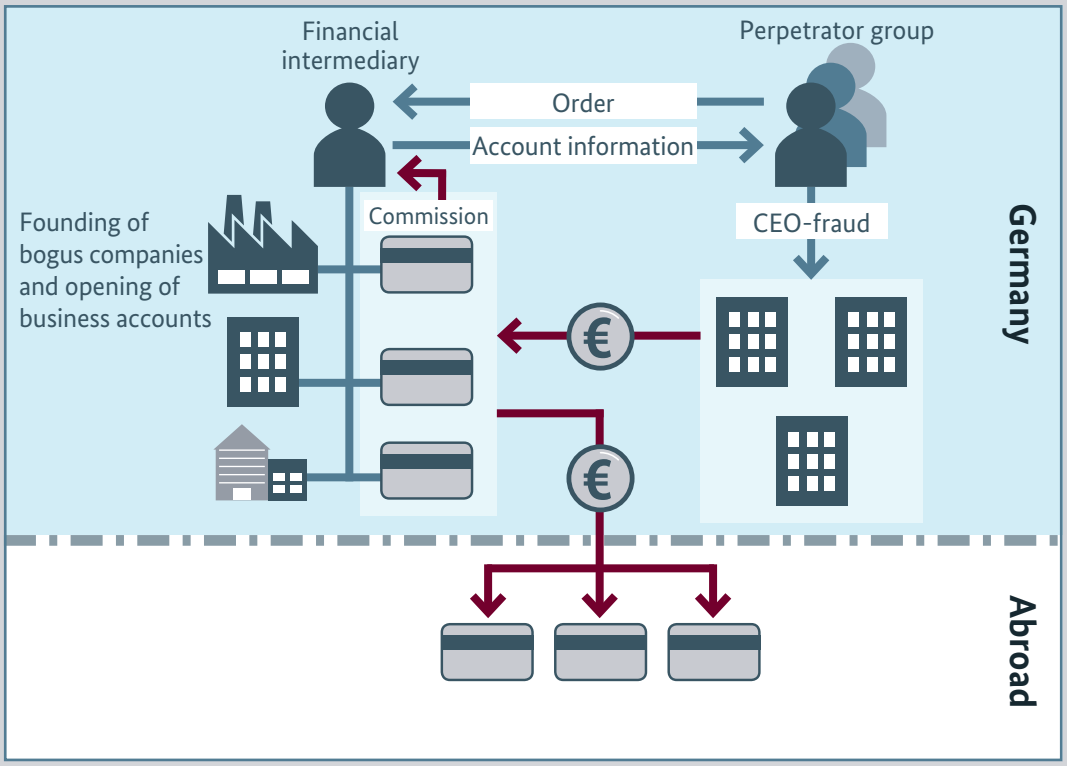


Figure 8: Case Study – From STR to Conviction

9 The present case study is a real case from the FIU's practice.

Investigations and Conviction

In the subsequent investigations, it was found that Mr G supported an international criminal association in committing CEO fraud[10] by acting as a financial intermediary for the perpetrators. Mr G and/or one of the companies that he had specifically founded for this purpose received money from illegal professional and gang-related fraudulent operations. Mr G was to transfer the funds paid into business accounts, which he had also newly set up, to other foreign accounts. In return, he received a commission in the amount of 3 % to 5 % of the transferred sum. The account data were passed on to the group of perpetrators.
Although Mr G could not speak German and could hardly speak English, with the help of a translator, he was able to appoint himself as CEO before a notary when he founded the companies with registered offices in Germany.
Once a European arrest warrant was ordered, Mr G was arrested in Spain and extradited to the Federal Republic of Germany. He was convicted of attempted money laundering and money laundering and was given a total custodial sentence of two years and nine months. In addition, a sum of money amounting to around half a million euro was recovered.

Temporary Freezing Orders

The FIU can prohibit a transaction from being executed if there is indications that the transaction is related to money laundering or serves to finance terrorism. This gives the FIU the opportunity to follow up on indications until the final assessment of the facts and to analyse the transaction without funds from criminal activities being removed from the sphere of state influence through cash withdrawals or transfers. The FIU has the option of issuing a temporary freezing order, which is an important and effective tool in preventing money laundering. Here, the necessity of executing a temporary freezing order is carefully weighed on a case-by-case basis. In the reporting year 2019, the FIU issued nineteen temporary freezing orders. This resulted in transactions with a total volume of around EUR 364 million being frozen for up to 30 days.[11] In five of these cases, a request from a foreign FIU was the trigger for executing the temporary freezing order.[12] In the case of the other fourteen temporary freezing orders, further analysis showed that eight orders exhibited probative facts that led to a dissemination to the competent authority.

10 In CEO fraud, the perpetrators contact company employees with decision-making power and impersonate the CEO of the company, for example. They try to manipulate the employees so that the latter arrange for a sum of money, which is usually high, to be transferred abroad in a short amount of time.
11 The majority of the total sum dates back to a temporary freezing order with an extraordinarily high volume.
12 For more information on temporary freezing orders due to requests from foreign FIUs, see the “International Cooperation” section.

Case Study – Funds from Merchandise Fraud [13]

Initial STR

The reporting bank noticed that there were several accounts which had received transfers of credit from third-party banks which had a payment recipient who was not the owner of the account. The intention was to subsequently transfer the funds to the benefit of another payment service provider. The recipient of the funds was already known to the bank internally in conjunction with commercial credit fraud.

FIU Analysis and Dissemination

When evaluating the accounts involved more closely, the FIU established that the account owners had transferred some funds among themselves or had converted funds into Bitcoin via virtual currency exchanges. Shortly after the first report was received, the FIU received other STRs that were linked to the initial STR.

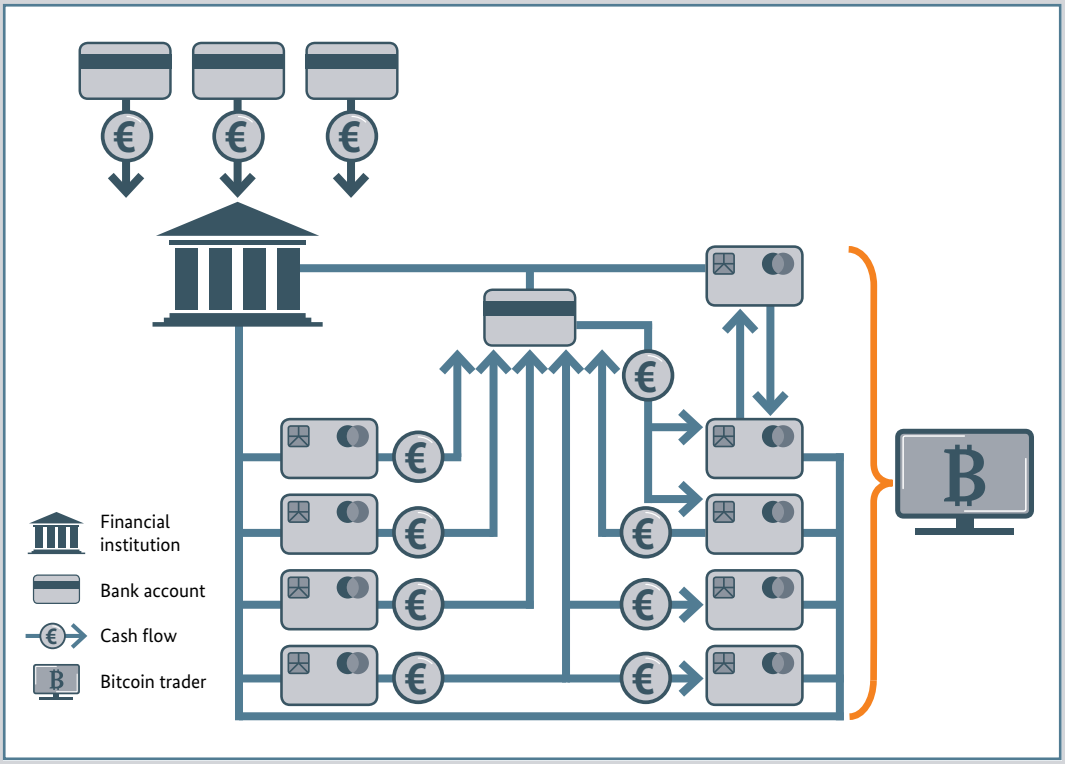


Figure 9: Case Study – Funds from Merchandise Fraud

13 The present case study is a real case from the FIU's practice.

In the subsequent analysis of the transactions, it was established that the accounts involved had numerous connections to each other. Thereafter, a temporary freezing order was decreed and the cash outflow of the accounts involved was thus prohibited.
In the course of further analysis, an examination of the bank statements for all accounts was carried out and it was noted that suspicious transactions were executed shortly after the accounts were opened and the incoming credit was transferred out on the same day. Overall, the transactions were executed with a view to concealing the origin of the money. The incident was sent to the competent State Office of Criminal Investigation (LKA) under the assumption that the account owners were either acting as financial intermediaries for unknown third parties or that the accounts were opened using identity theft without the knowledge of the account owners.

Transactions

Most of the STRs that are received by the FIU contain suspicious transactions which constitute an important component of detecting money laundering activity. In these transactions, transfers of assets are made between two parties, usually using a credit institution or a financial service institution. Examples of these are bank transfers, cash withdrawals from current accounts as well as cash transactions of all kinds or cashing in chips at casinos. Transferring virtual assets between digital wallets also constitutes a transaction.

In the reference period of 2019, the FIU received reports of around 355,000 suspicious transactions, around 13 % more than the previous year.[14] A suspicious report does not necessarily need to contain a transaction, but a single report can also contain a large number of transactions. The number of reported transactions therefore is not exactly equal to the number of STRs received.

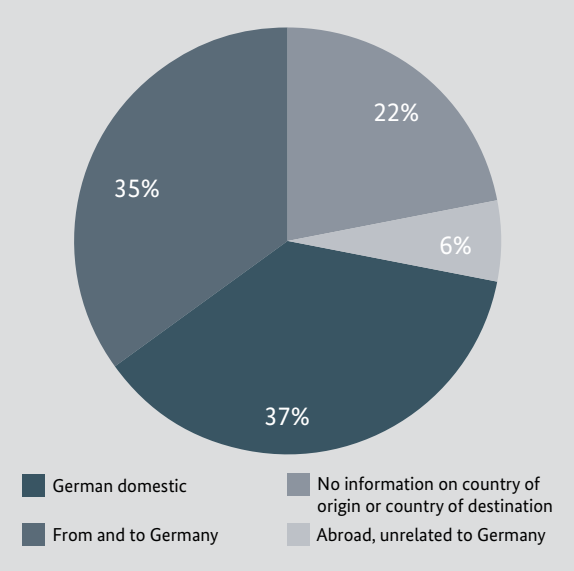


Figure 10: Foreign Involvement in Suspicious Transactions

The proportion of German domestic incidents rose to approx. 37 % (in the previous year, it was around 25 %). All further transactions are related to foreign countries (just under 41%), with Germany as the country of origin or destination for over a third of them (just under 35 %). Approx. 6 % of all transactions are purely international, as Germany is listed neither as the country of origin nor as the country of destination. This can, for example, be the case for correspondent banking activities in which the reporting credit institution is a reporting entity in Germany but acts exclusively as a service provider for settling cross-border transactions. In addition, a conspicuous number of transactions was reported in which France was both the country of origin and country of destination, as was the case in 2018. In these cases, a cluster of accounts opened at German internet banks with a view to committing fraud was also determined, where identification is possible without the account owner physically being present, for example by using a video identification procedure.

For a national analysis, transactions from and to Germany are particularly relevant. The following figures show the severity of the reported transactions that Germany was involved in as the country of origin or destination.

14 This number may increase after the preparation date of the annual report if further STRs containing transactions that were executed in 2019 are received in the course of 2020.

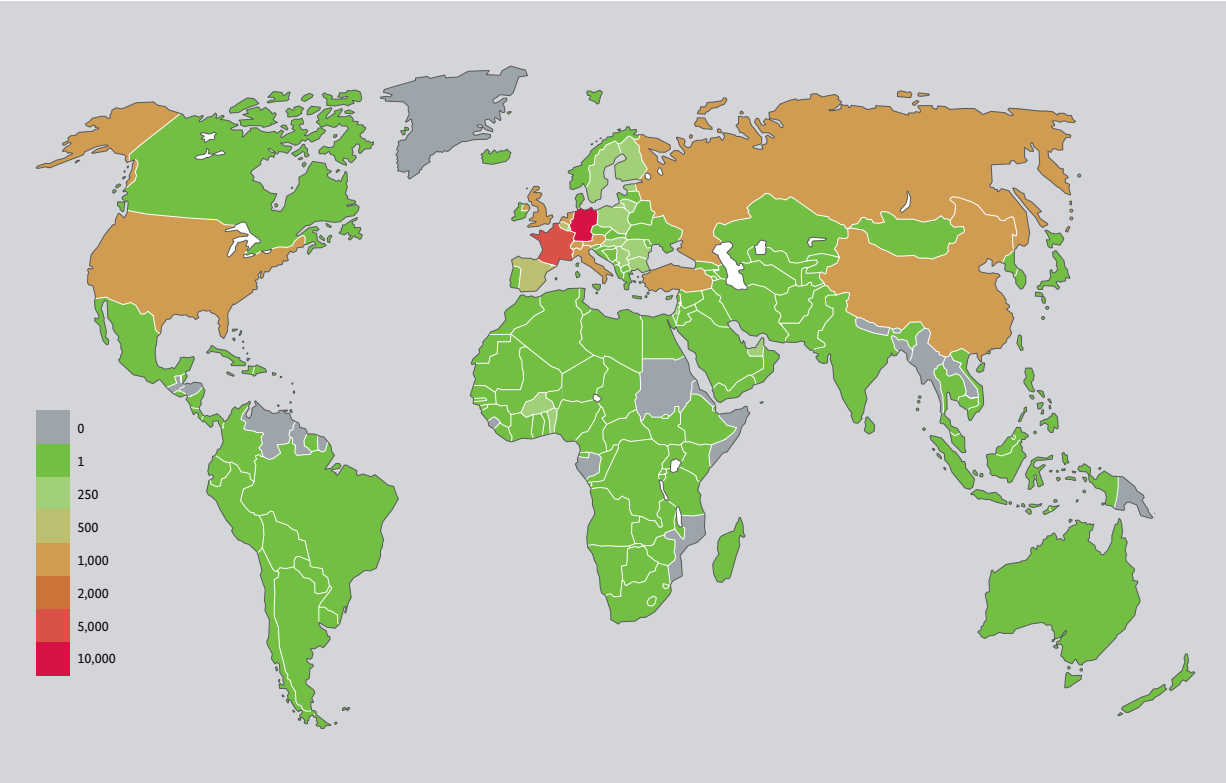


Figure 11: Number of Suspicious Transactions by Country of Origin

With regard to suspicious transactions from abroad that have Germany as their country of destination, the bulk are predominantly from West European countries, Turkey and the major national economies of Russia, the USA and China. France had by far the most suspicious transactions with Germany as the country of destination, amounting to around 3,600 transactions. Places two and three on this list went to the Netherlands and Switzerland, with over 1,700 transactions each. Taking the geographical proximity to Germany, the economic power of the respective countries and the proportion of people living in Germany with roots in the country of origin into account, the distribution of these transactions seems to be plausible. Far fewer transactions from Turkey were reported in comparison to the previous year. Turkey took second place in terms of the country of origin with the most suspicious transactions in 2018 but dropped to place 6 this year.

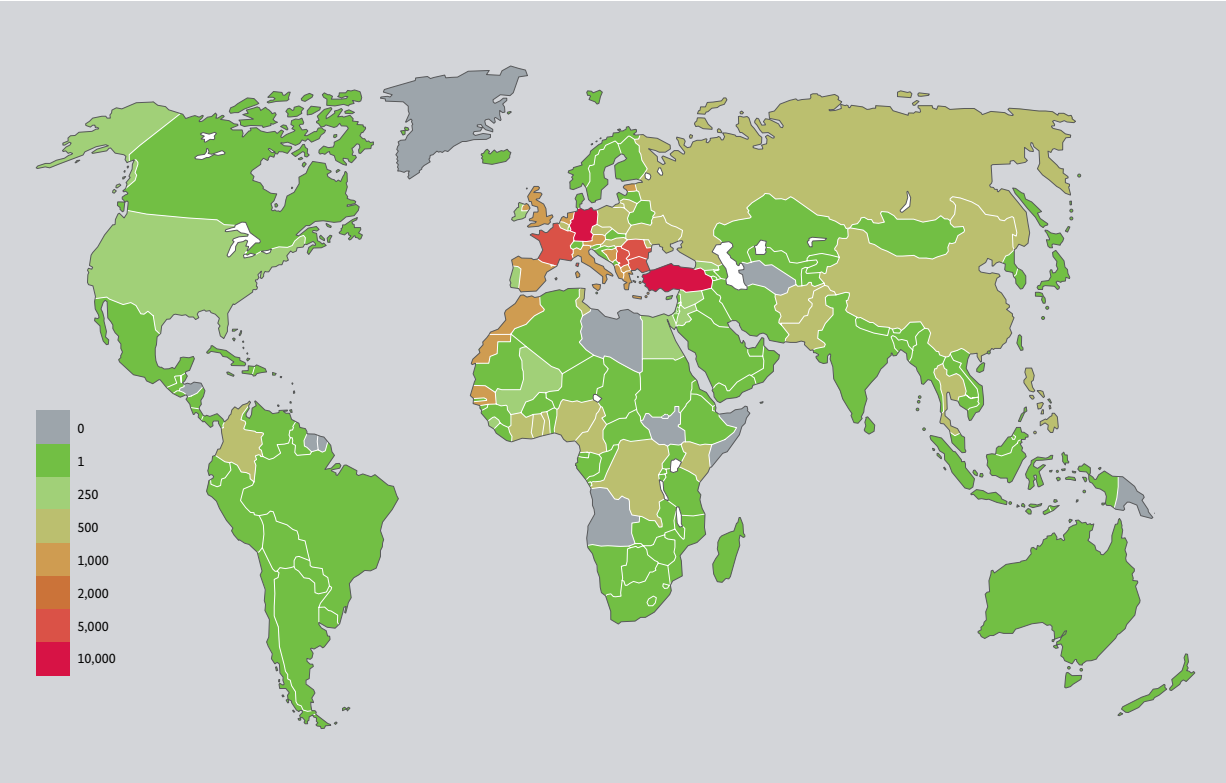


Figure 12: Number of Suspicious Transactions by Country of Destination

The number of outgoing transactions from Germany to other countries reported as suspicious in 2019 was significantly higher than the number of incoming suspicious transactions to Germany (around 92,000 vs. around 31,000), even though this number decreased slightly in comparison to the previous year. Over a quarter of the transactions had Turkey as the country of destination (approx. 25,000). While incoming transactions analysed by country of origin were heavily concentrated in West European countries, Southeast Europe plays a significantly larger role regarding the countries of destination. Thus, there are five Southeast European countries in the "top 10" list for the countries of destination receiving the most suspicious transactions: Bulgaria (approx. 6,500), Romania (approx. 5,500), Serbia (approx. 2,500), Kosovo (approx. 2,500) and Bosnia and Herzegovina (approx. 2,000). As in the previous year, the high number of suspicious transactions in East European countries could not be completely explained by geographical, economic or demographic factors.

In addition to the transactions listed here, separate STRs were received from multiple reporting entities concerning several thousand transactions in conjunction with so-called laundromats.[15] These were not included in the graphic due to the unusual situation in order to prevent distortion, e.g. regarding Denmark and Estonia.

15 See section "Total Number of STRs in Reporting Year 2019".

Typologies and Trends

Introduction of Key Risk Areas

Focus on Real Estate

Focus on Use of Cash (when procuring high-value goods), Here: Art and Antiques

Focus on Organised Crime in the Form of “Clan Crime”

Focus on Implementation of New Payment Methods, in this Instance: Virtual Assets

Typologies and Trends

Introduction of Key Risk Areas

The FIU further strengthened its risk-based orientation in the reporting year. To this end, a total of ten key risk areas that serve as steering and prioritisation instruments in operational analysis were identified with the participation of the law enforcement agencies.

During the development of the key risk areas, the findings of the National Risk Analysis (NRA) were taken into account along with the FATF's assessments. As it will be mandatory for reporting entities under the German Anti-Money Laundering Act to take the findings of the NRA into consideration when creating their own risk analyses in the future, the FIU was able to create an interlinkage that encompasses both partner authorities and reporting entities alike. The established key risk areas also enable the FIU to prioritise the incoming STRs and carry out appropriate risk-based processing.

The identified key risk areas take both industry-related and phenomenon-related risks into account and are continually reviewed. In essence, a distinction is drawn between the areas of money laundering and terrorist financing, although the implementation of new payment methods due to new technology has also been termed a mutual key risk areas.

Key Risk Areas Regarding Money Laundering

Real Estate

Real estate carries a high risk of money laundering. Sales generally involve large transaction volumes. In addition, there is a wide range of legal configuration options for potentially concealing the origins of the funds and the ownership structures (see section: "Property: The Role of the Beneficial Owner"), including the integration of national and foreign legal entities. As an invested asset that is independent of the economic situation, real estate is particularly stable in terms of its value, is tied to a specific location, can only be substituted under certain conditions and is thus considered the most significant investment property in Germany.

Use of Cash (when procuring high-value goods)

Trading valuable goods is characterised by the use of large sums of cash, which facilitates the anonymous transfer of larger sums of money. In addition, markets that are frequently obscure enable funds from criminal activities to be integrated into the legitimate economy. The acquisition of motor vehicles, art and antiques and other luxury goods are on focus here.

Trade-Based Money Laundering

Trade-based money laundering takes advantage of the complex nature of the flows of goods and money in international commerce. Over- or under-invoicing, charging for goods and services multiple times, fake commercial transactions, deliveries with contents which deviate from the description or incorrect descriptions, intermediation by third parties or using shell companies are typical scenarios here. Germany is a strong exporter and importer of goods and is thus considered particularly "attractive" for this typical method of money laundering.

Games of Chance/Betting

The gambling industry also offers methods for concealing the origins and further use of the funds used, also through its established diverse online market. A high circulation velocity and the use of cash below the legal identification limit of EUR 2,000 increase the gambling sector's susceptibility to money laundering.

Organised Crime in the Form of Clan Crime

Organised crime is on focus of crime control in Germany. Organised perpetrator structures and the resulting large-volume profits from illegal business must be laundered so that they can be integrated into the legitimate economy. Within this context, foreign extended families are the current particular focus of the law enforcement agencies' attention and of their police investigations.

Serious (Tax) Criminal Acts, e.g. Carousel Fraud

Trade across the borders between two EU Member States can result in the right to a tax refund due to the structure of VAT legislation. Carousel fraud often exploits this in large-scale, cross-border tax fraud operations. By the time the responsible tax auditor has become aware of the tax evasion, the companies involved often no longer exist.

Commercial Fraud and Identity Theft

Amongst others, the option of opening an account via a video identification procedure lulls consumers into divulging their personal data for opening bank accounts. The identity and legitimation checks are executed via video identification procedures and consist of simply showing identification papers to a camera and answering some questions. The perpetrators then use the accounts opened under the names of their victims for criminal purposes, which are generally related to commercial fraud (e.g. for running fake shops), or directly for money laundering.

Key Risk Area Regarding Terrorist Financing and Money Laundering

Use of New Payment Methods

The constant (technical) development of payment methods goes hand in hand with a significant acceleration in the speed of transactions, e.g. due to instant payments via apps and smartphones. Using virtual assets for making payments is also included within this subject area. For the relevant processing platforms and/or electronic payment systems, tracing transactions is difficult or even impossible due to the regularly applied encryption techniques and internet-based transmission paths. In light of this, they are susceptible to becoming vehicles for acts of money laundering and terrorist financing purposes.

Key Risk Areas Regarding Terrorist Financing

Misuse of NGOs/NPOs

Non-governmental organisations (NGOs) and non-profit organisations (NPOs) are held in high regard by society. They often act across country borders and have a large amount of financial resources, which makes them interesting to those seeking to finance terrorism. One method for committing misuse of an organisation consists of forwarding parts of the aid funds transmitted to it on to terrorist organisations. Fake aid organisations that are completely controlled by terrorist groups so that the funds can be used entirely for terrorist purposes are another possibility.

Misuse of Money and Value Transfer Services

The settlement of transactions via financial transfer service providers can also be abused with a view to financing terrorism. Specifically, cross-border transactions are subject to a higher level of risk if the country of destination is classified as a high-risk country. Here, the risk is that the sums of money will be transferred to conflict zones and will be used for terrorist purposes there.

In the following, the FIU's sector-specific findings for 2019 are presented according to selected key risk areas.

Focus on Real Estate

The FIU has identified the real estate sector and thus the STRs in conjunction with this sector as a key risk area. STRs relating to real estate transactions are thus always given high priority to enable the competent law enforcement agencies to carry out their investigations, particularly in consideration of the potential absorption of assets that this can entail.

The real estate sector in Germany is characterised by legal security, relative value retention and high individual transaction volumes. The purchase and sale of real estate is primarily used in the "integration phase" of money laundering, in which funds are continuously fed back into legitimate economic circulation. This means that "pre-laundered" money that was already in financial circulation is invested for the long-term in legal capital assets, and that the purchase thus appears completely legitimate. Real estate is an excellent vehicle for this due to the fact that it is generally priced very highly. The integration phase is also indispensable for the perpetrators in order to ensure that they remain protected from state intervention. Thus, in this phase, the objective is also to conceal the actual ownership structures for the real estate and/or the principals of the underlying real estate transactions.

The Role of the Beneficial Owner in Real Estate Business

Who is the factual decision-maker in a real estate transaction?
Who becomes the actual owner of the property?
Who is ultimately benefited by this without being publicly known?

On a national level, the legal due diligence when commencing a business relationship requires the beneficial owner to be identified, the control and ownership structure of legal entities to be established and the business relationship to be supervised accordingly. The documentation must be provided and revised on a regular basis to take risks into account. On an international level, the FATF also requires transparency and the availability of up-to-date and complete information.

The Beneficial Owner
The beneficial owner under the German Anti-Money Laundering Act (Section 3 AMLA) is the natural person that ultimately owns or controls the contracting party or the natural person at whose instruction a transaction is ultimately carried out or a business relationship is ultimately established.
A beneficial owner of a legal entity[16] is any natural person who, directly or indirectly, holds more than 25 % of the capital stock, controls more than 25 % of the voting rights or exercises control in a comparable manner.

16 Except incorporated foundations and other corporations that are not listed on a regulated market in accordance with Section 2 (11) of the German Securities Trading Act and that are not subject to any transparency requirements under European Community Law regarding voting shares or subject to any equivalent international standards.

As part of its analyses, the FIU regularly draws on various options for determining the beneficial owner. The FIU is able to obtain information on the beneficial owner using public registers, e.g. the company register (list of shareholders) and the transparency register. Furthermore, the FIU is entitled by the land offices to directly access the land title registers in order to identify actual real estate ownership structures. In addition to this, relevant information can also be obtained from the reporting entities, regardless of whether they have submitted an STR or not.
In the 2019 reporting year, determining the beneficial owner proved to be an important piece of information and provided added value in terms of information for the FIU's analyses. In conjunction with the real estate business, two kinds of typology that cropped up repeatedly were observed when processing the cases: These were the involvement of persons that acted on behalf of a third party and the financing of the purchase price via a complex network of companies. In addition to both of these phenomena, depositing cash of unknown origin and subsequent acquisition of a property was also a frequent reason for suspicion this year, just as it was last year.

Straw Man Transactions

The concealment of the beneficial owner was executed in conjunction with real estate transactions, also including the involvement of persons who were acting on behalf of third parties; these constitute so-called straw man transactions. In these cases, third parties externally represent themselves to the contractual parties without the latter being aware that the straw man is not acting on its own behalf. Frequently, this is either a family member of the actual beneficial owner or an unknown person acting as a favour or against payment similar to a commission who concludes business for third parties or takes on their roles, as these generally do not wish to, cannot or must not appear.

Case Study – Straw Man Transactions [17]

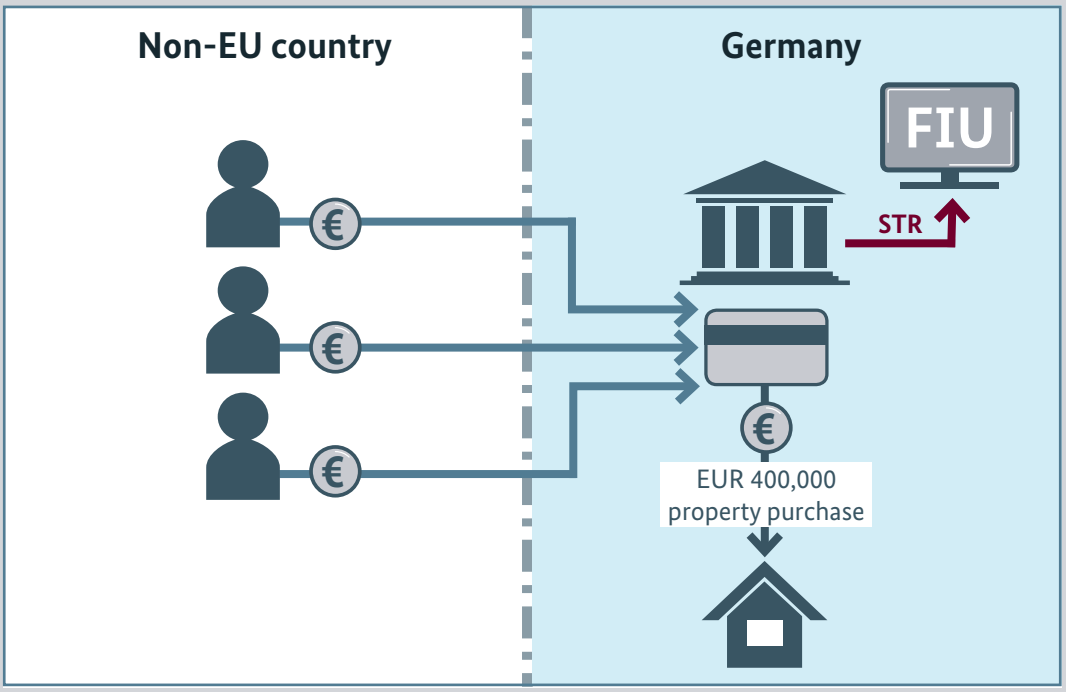


Figure 13: Case Study – Straw Man Transactions

Initial STR

A credit institution reported a private account that was held with it which had come to its attention due to a significant number of deposits from a non-EU country. The credits, in the amount of around EUR 400,000, were transferred from various private parties that did not appear to have any familial relationship with the account owner and thus did not appear plausible to the reporting entity.

FIU Analysis and Dissemination

In addition to the potential circumvention of the foreign exchange controls, the FIU analysis also showed that the amount of incoming payments did not match the financial situation of the bank customer. The FIU's internal research showed that, after receiving the incoming payments, which were apparently made by straw men, a property worth around EUR 400,000 was acquired. The connection between the originator of the payment and the actual owner could not ultimately be determined, meaning that the STR was transferred to the competent law enforcement agency.

17 The present case study is a real case from the FIU's practice.

Financing of the Purchase Price via a Complex Network of Companies

In Germany it is also the case that, when executing (luxury) real estate transactions, legal entities are often implemented as the owners of acquired properties without the natural person behind them being immediately apparent as the beneficial owner. As part of processing cases in 2019, legal forms with limited liability and limited disclosure obligations were identified inter alia, some of which did not have any recognisable business activities. These had come to the FIU's attention in conjunction with potentially suspicious real estate purchases. If no regular business activity is apparent, this can often be an indication of a dummy or shell company founded solely to manage finances. An attractive method of settling real estate transactions is thus to finance the purchase price by integrating these types of companies (generally foreign) in order to conceal the actual beneficial owner of the real estate transactions.

Case Study – Financing of the Purchase Price via a Complex Network of Companies [18]

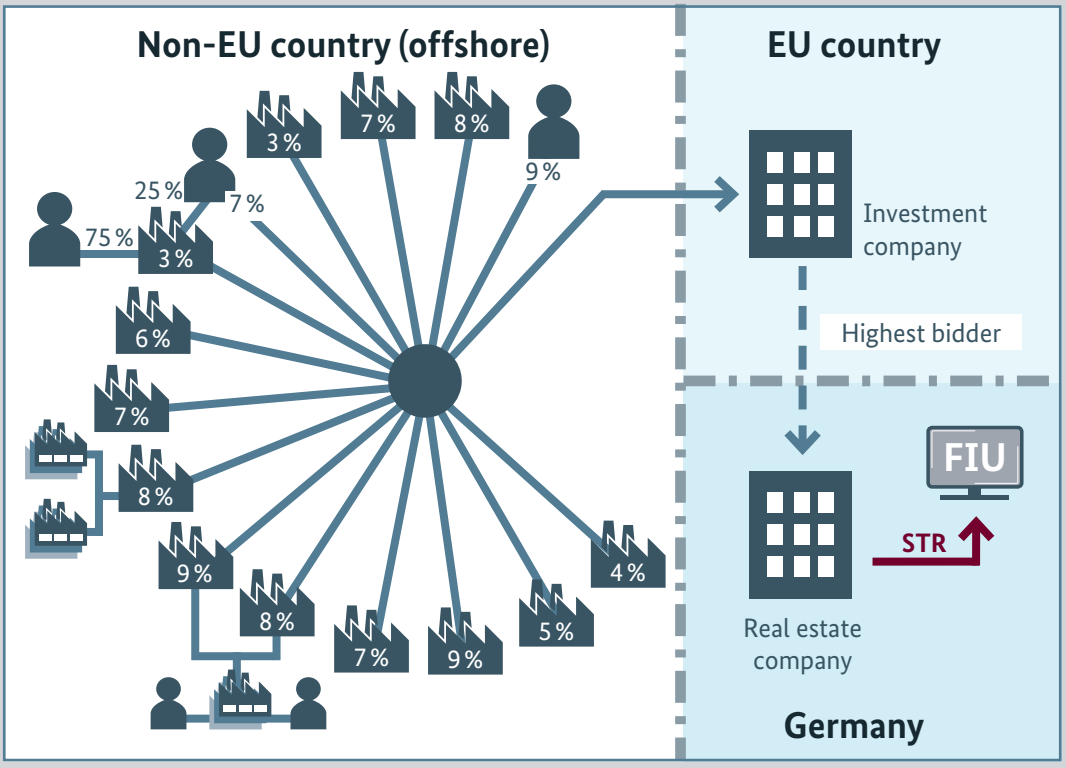


Figure 14: Case Study – Financing of the Purchase Price via a Complex Network of Companies

18 The present case study is a real case from the FIU's practice.

Initial STR

A reporting entity – a real estate company based in Germany – reported a planned sale of property amounting to around EUR 50 million due to abnormalities that had been detected in conjunction with the highest bidder for the upcoming deal. The aforementioned prospective buyer – an investment company based in an EU country – was distinctive due to its non-transparent holding structures, and consequently the actual beneficial owners could not ultimately be determined by the reporting entity.

FIU Analysis and Dissemination

The FIU's analysis showed that the prospective buyer's complex network of companies had various multi-level and nested offshore limited partnerships, each structured in accordance with the statutory provisions in force in their respective countries. Here, shareholders generally held less than 10% of the company, resulting in the company being completely in free float. It was established that the purchasing company was founded just before the property purchase as part of the already existing (complete) company structure, which strengthened the suspicion that the founding of the company was potentially executed specifically in order to purchase the property.
Furthermore, the analysis established that the articles of association completely excluded natural persons from holding shares in the purchasing company, meaning that the investigation into the actual beneficial owners (natural persons) was only possible with a great deal of effort and/or was impossible due to insufficient transnational information. In addition, the personal liability of all CEOs designated by name, who were thus regarded as bogus beneficial owners within the entire complex, was completely excluded, so that the FIU was not able to determine sufficient information on the participants in the real estate transaction. Due to the extreme lack of transparency in the holding structures and not least due to the significant volume of the real estate transaction, the facts were disseminated to the competent law enforcement agency.

A total of 1,266 STRs were submitted to the FIU in conjunction with real estate transactions in the reporting year 2019. The reporting entities marked these with "Abnormalities in conjunction with the purchase/sale of real estate" as the reason for suspicion. Around 16 % of these reports came from the financial and supervisory authorities, around 79 % from credit institutions and the rest of the financial sector and around 5 % from the non-financial sector.

Although the number of STRs with the aforementioned reason for suspicion rose slightly overall, it can still be considered too low for the non-financial sector in view of the continuing significantly higher proportion of STRs from the financial sector. The number of STRs submitted to the FIU by estate agents increased: At 84 reports, this number was 2.5 times higher than in the previous year, which the FIU took as a sign of the increasing awareness in this subgroup of reporting entities. Notaries and lawyers sent in 38 STRs, so reports from these entities continued to be sporadic and in the low double-digit range. The majority of the STRs were still submitted regarding cash deposits or foreign incoming payments with funds of unknown origins. Furthermore, more STRs were received regarding cases where the identity of the beneficial owner was concealed.

Focus on Use of Cash (when procuring high-value goods), Here: Art and Antiques

In the area of money laundering, using cash when procuring high-value goods was identified as a further key risk area. Often, transactions for expensive goods such as art and antiques, motor vehicles and luxury goods such as watches and jewellery are executed in cash. Trading art and antiques is also characterised by a high level of anonymity and secrecy. Expensive objets d'art are often purchased discreetly in order to minimise the risk of a break-in or theft. In addition, obscure market conditions are also a complicating factor in some areas of the art trade sector. As art and antiques are often sold as individual items, it is frequently impossible to ensure that pricing is transparent. In combination with increasing diversification of asset portfolios, which include art and antiques as an additional investment element, this leads to high susceptibility to money laundering activity for the sector, e.g. via shell companies, concealment of actual ownership structures or use of cash of unknown origin.

The FIU only received 40 STRs that could be definitely assigned to the art sector in 2019.[19] Here, 5 % of the reports came from traders in goods, 7 % from fiscal authorities and 88 % from the financial sector. Credit institutions and financial service institutions thus submitted the overwhelming majority of the reports.

Suspicious transactions in the art and antiques trade often reach at least a five-figure sum. This illustrates the fact that high sums can be placed in this sector, which makes it attractive for money laundering. In most of the available facts of cases, the objets d'art or antiques served as the justification for suspicious transactions. Here, the incoming and outgoing bank transfers, some of which were made with involvement from abroad, and incoming and outgoing payments of cash were justified by stating that objets d'art or antiques had been sold or that equivalent items had been procured using these sums of money. It is often difficult to verify whether any physical sale of actual objects occurred.

STRs in conjunction with trade-based money laundering in the art market were apparent in this context. High-volume payments by third parties were reported that were arranged by a shell company based abroad with no connection to the final delivery location. This is done to create anonymity, facilitate money laundering activity and conceal the origin of the funds from criminal activities.

Discrepancies between the value of the goods as stated in the invoice and the appropriate market value, or regarding the transportation documents and shipping documents, were also frequent reasons for the submission of reports by reporting entities.

Smuggling or forgery of objets d'art generally plays a rather subordinate role in the present STRs, but individual reports were also received regarding these criminal activities over the course of the year.

Overall, it was established that despite the inherent susceptibility to risk, there were relatively few reports from the reporting entities in the art and antiques sector. The FIU therefore provided the reporting entities with a typologies paper in 2019 in order to give them specific support for the art and antiques sector. The paper contains information on typical patterns of behaviour and abnormalities in conjunction with money laundering and terrorist financing and thus facilitates the detection of potential crimes.

19 These STRs were either submitted directly by reporting entities in the arts sector or were marked with "Abnormalities in conjunction with the purchasing/sale of objets d'art and antiques" as the reason for suspicion by other reporting entities.

In addition, contacts were strengthened with the relevant associations and representatives from the art and antiques sector, and both sides aim to further expand relations in the coming years. Providing such information papers is intended to raise awareness among the reporting entities and encourage them to report more often in order to gradually increase the number of reports for the art and antiques sector.

The following account serves as an example to clarify how trade-based money laundering can be recognised in the art market.

Case Study – Payment by a Third Party[20]

A credit institution reported shareholder X of a large culinary establishment, who was also known to be a private collector. A large amount of money was paid into his business account by person A from non-EU country A. When asked, shareholder X stated that this amount was the proceeds from a sale of objets d'art to person B in non-EU country B. Shareholder X could not explain the link between person A and person B, nor why the payment did not come from the country of destination. Furthermore, there were discrepancies in the submitted invoice and the further explanations. An analysis by the FIU showed that another report had been made regarding the persons involved. According to this report, a loan agreement had been concluded between person A and person B. Looking at the big picture, these abnormalities could indicate the concealment of funds from criminal activities.

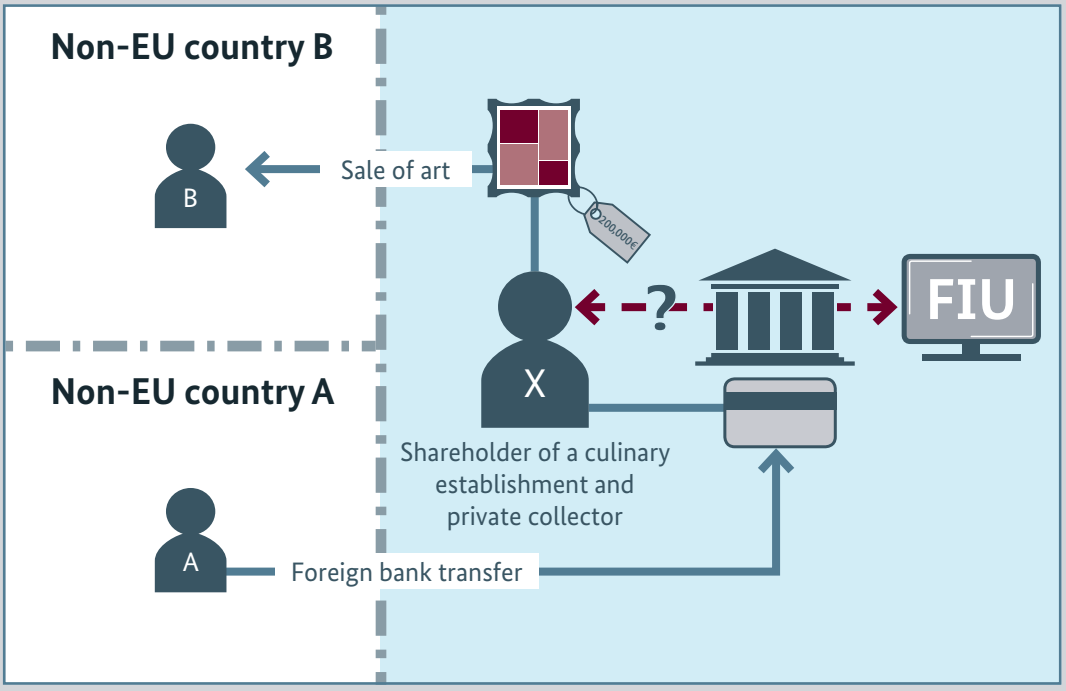


Figure 15: Case Study – Payment by a Third Party

20 The present case study is a real case from the FIU's practice which has been greatly simplified for better illustration.

As part of the adoption of the law on implementing the amending directive for the fourth EU Money Laundering Directive,[21] the previously applicable legal regulations for art trade were rendered more stringent. In the course of implementing the changes on the fourth EU Money Laundering Directive, the keepers of art storage facilities are also classified as reporting entities (as long as the storage is located in duty-free areas) along with traders in goods, i.e. every person that sells commercial goods, and art dealers (particularly art galleries and auction houses). In addition, after coming into force at the beginning of 2020, the law stipulates a general obligation to identify the customer for transactions with amounts exceeding EUR 10,000, regardless of whether payment is made in cash or not.

Focus on Organised Crime in the Form of "Clan Crime"

Organised crime is particularly characterised by the systematic committing of crimes where the ultimate goal is to create a large profit. This area, in its protean manifestations, has always been a top priority in the fight against crime. In addition to combating organised crime by Russian-Eurasian, Vietnamese and Italian groups, there is also a focus on crimes committed by members of extended families of Turkish and Arab heritage, also termed clan crime.

In this context, based on present information and findings, the FIU established this subject as a key risk area in the range of money laundering and terrorist financing.

FIU analyses on abnormalities in conjunction with extended families of Turkish and Arab heritage grouped findings from the FIU's database with information on criminal activity by clan members from the NRA[22] and findings available to the law enforcement agencies. Here, establishing that a person belongs to a family clan on the one hand and the necessary differentiation between criminal and non-criminal members of the extended family on the other pose a huge challenge in terms of data evaluation.

Thus, in many of the reports with a presumed connection to criminal extended families from a Turkish or Arab background, there are references to the use of straw men, some of whom have been deliberately recruited from another environment and have German-sounding surnames. Particularly in the context of clan crime, having the surname of a clan can be taken as an indication of belonging to that clan, so this procedure is excellent for diverting suspicions of potential relationships to a criminal extended family. Female family members are also frequently involved on the account management and business management side of operations, although male family members are more frequently known as criminal actors according to prosecuting information.

However, many STRs were identified which featured a suspected connection to a criminal extended family. Here, classification is carried out, inter alia, according to the findings of the prosecution and the FIU as well as using references from the reporting entities, who frequently are aware of the personal background of their customers. Further STRs could not be unambiguously assigned to this phenomenon, but in terms of content, they corresponded to the STRs that did have a clear connection.

21 Law on implementing the fourth EU Money Laundering Directive, on executing the EU Funds Transfers Regulation and on reorganising the central agency for financial transaction investigations of 23 June 2017 (German Federal Law Gazette [BGBl.] I, p. 1822); Law on implementing the amending directive for the fourth EU Money Laundering Directive of 12 December 2019 (BGBl. I, p. 2602).

22 See also the introduction in the "Typologies and Trends" section for information on the NRA's significance for the FIU.

The filtered STRs concerned numerous industries and were sent in from both the financial and non-financial sectors. Thus, the FIU observed STRs relating to retail, provision of services, gastronomy and also real estate, where various extended families were active.

In retail, the automotive trade (including lorries) was frequently named as the specific industry, along with gold, jewellery and antiques. STRs to this effect also appeared in the online trade sector and in trade with electronic devices. In some STRs, the food industry was also part of the facts presented.

Reports on the real estate industry concerned both private purchases and commercial purchasing processes. Here, the financial situation of the purchaser and the purchasing price for the property frequently diverge conspicuously. Reports also concerned completely missing financing, in conjunction with prior cash deposits into the account. In some STRs, clear interconnections between renters and landlords of properties can be seen. Here, suspected straw men were used to transfer the rent so that these interconnections would not become obvious.

Gastronomy was another industry which featured in the STRs. Here, business activity concerned not just shisha bars but also extended to pizzerias and steak houses, for example. Reports were also made concerning security services. Furthermore, individual STRs were received that related to the construction industry. Due to the lack of account activity, the FIU was often unable to discern any regular business activity in these cases.

In many STRs which showed closer links to criminal extended families of Turkish and Arab heritage, an active use of cash was established. Conspicuously high incoming or outgoing payments, returns and delivery versus payment for incoming and outgoing payments were the reasons for submitting an STR given by the reporting entities.

As the connection to clan crime, as stated above, is not easily detectable, this subject requires close cooperation between the FIU and the law enforcement agencies, which began in 2019. Further continuation and intensification of the information exchange is planned for 2020, as this subject continues to be a topical issue.

The following facts serve as an example to illustrate how attempts were made to funnel funds from criminal activities into the legitimate economy through various different channels.

Case Study – Concealment of the Origin of Funds [23]

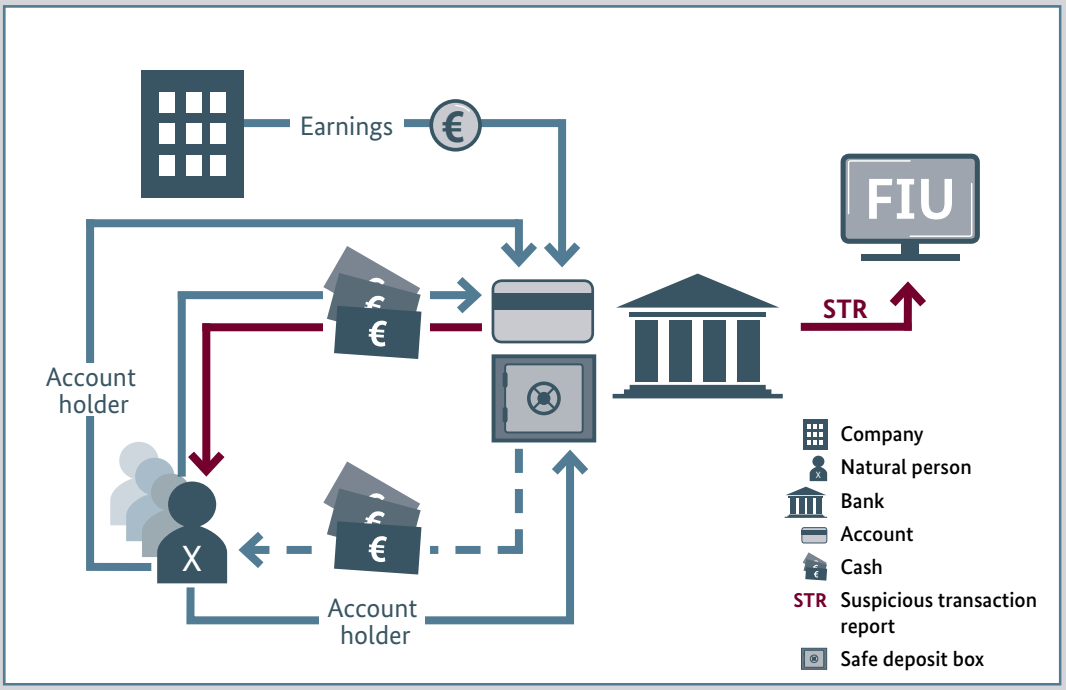


Figure 16: Case Study – Concealment of the Origin of Funds

Person x has a private account at a credit institution and draws income from employment. The credit institution noticed the account due to cash deposits made at short intervals, which totalled a high five-figure sum within one year. Withdrawals of smaller amounts of cash were also made. When the bank requested information on the origins of the funds, person x explained that the cash payments were money saved up for purchasing property which he had stored in a bank safe deposit box.

Due to the customer's wish to have the full account credit (a sum in the mid-five-figure range) paid out, the str was forwarded to the fiu as an urgent case.

The origin of the funds could not be verified during the FIU's analysis. Furthermore, there was reason to assume that person x was a member of a criminal family clan. The report was submitted to the competent law enforcement agency for further investigation. Here, it was determined that there was no temporal correlation between the dates on which the safety deposit box was accessed and the cash movements and that the statements that person x made to the bank were not true. Furthermore, the investigations confirmed that person x belonged to a criminal clan. The funds were confiscated by law enforcement as part of asset recovery.

23 The present case study is a real case from the FIU's practice.

Case Study – Concealment and Integration [24]

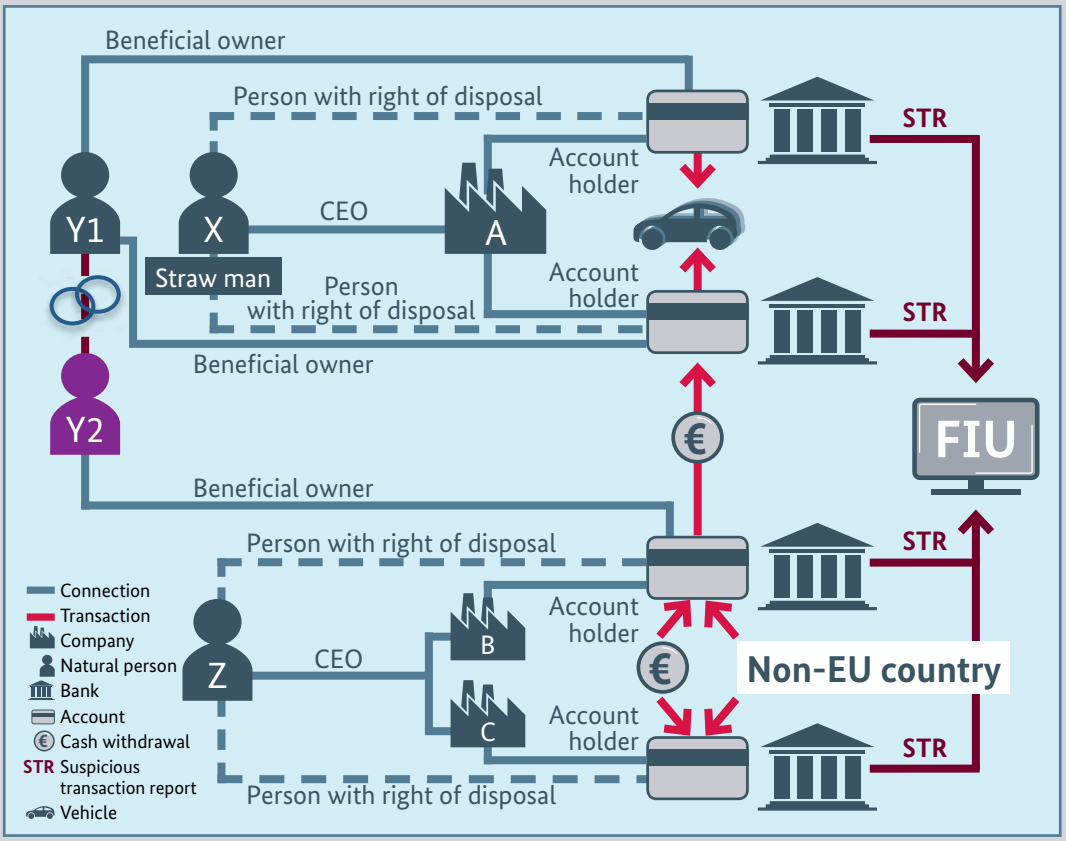


Figure 17: Case Study - Concealment and Integration

An STR concerning the business account of company A was sent to the FIU by a credit institution. The CEO and sole shareholder Mr X had previously admitted at the credit institution's counter to having acted as a straw man. In addition to Mr X having right of disposal, Mr Y 1 was also registered as the beneficial owner of the business account. At the counter, Mr X wished to end the business relationship with Mr Y 1 due to irregularities in the account and therefore wished for Mr Y 1 to be removed as the beneficial owner.
During the analysis, it was established that company A had another business account at another credit institution with the same rights of disposal. The second credit institution had also reported the account to the FIU as suspicious. Based on the consolidated account balances, it was ascertained that both accounts were mainly being supplied with payments from company B. Thereafter, the incoming funds were mainly invested in vehicles (purchase and leasing transactions).

24 The present case study is a real case from the FIU's practice.

An STR on company B's account was also received by the FIU. The account attracted attention due to a high number of credit payments from abroad, which were followed by subsequent transferral of these deposits (to company A, among others) or cash withdrawals. The CEO and sole shareholder of company B was Mr Z. He also held rights of disposal to the business account. In addition to Mr Z, Ms Y 2 was a beneficial owner of the account. Ms Y 2 was the wife of the aforementioned Mr Y 1, meaning that a further connection was established between the STRs.
Furthermore, it was determined that Mr Z was the CEO and sole shareholder of company C. The business account of company C was also reported through an STR. The account had a similar transaction scheme to the account of company B. Furthermore, various pieces of evidence supported the assumption that Mr Y 1 could be a member of a criminal family clan. The STRs were disseminated to the competent law enforcement agency.

Focus on Implementation of New Payment Methods, in this Instance: Virtual Assets

An in-depth examination of the topic of virtual assets and/or virtual currencies was already carried out in the 2018 annual report. In the meantime, the FIU has adopted this subject as an essential part of the key risk area "Implementation of New Payment Methods". Despite their high volatility and large fluctuations in their market value, virtual assets are now established as an instrument that can also be used to transfer large financial assets. Due to the speed and anonymity that they provide, there is a significant risk that virtual assets can be used to transform illegal funds into legal funds. The FATF published its updated "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" in June 2019.[25] Due to the law on implementing the amending directive for the fourth EU Money Laundering Directive, the legislator created regulatory provisions in accordance with the FATF guidelines for the sector, according to which the providers of virtual asset services become reporting entities, as they are financial service institutions, and are thus subject to the supervision of the BaFin. These changes came into force at the beginning of 2020.

In 2019, the FIU again received numerous reports in relation to virtual assets. Over the course of the year, the number of STRs in which reporting entities stated that the reason for suspicion was "Abnormalities in conjunction with virtual currencies" developed in a slight upward trend (see the linear curve in Figure 16). In total, around 760 STRs had this reason for suspicion. The increase compared to the approximately 570 reports in 2018 is smaller than the increase in the total number of STRs received. However, analyses determined that a large number of STRs did actually have a connection to virtual assets and/or currencies, but were not marked with the according reason for suspicion by the reporting entities.

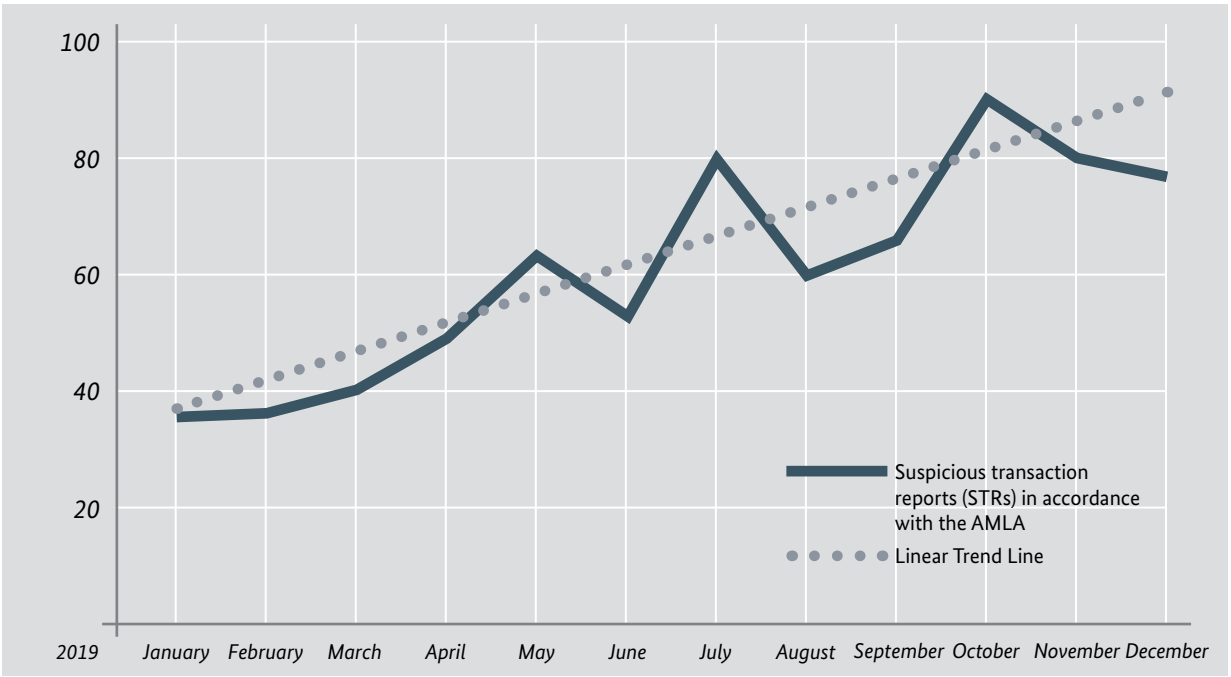


Figure 18: STRs with the Indicator "Abnormalities in Conjunction with Virtual Currencies"

25 Cf. FATF (2019): Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers; https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

A special evaluation showed that over half of the reports with connections to virtual currencies also related to money laundering activities which followed from fraud. Here, merchandise fraud stands out in particular, followed by phishing activity. The transmission of the illegally obtained funds to trade platforms abroad in order to convert the funds into virtual currency and then transfer them on is a typical method here. The goods and products allegedly obtained from the victims are frequently offered for sale via so-called fake shops, classified ads or hacked user accounts on large auction platforms. Details for bank accounts that the perpetrator has direct or indirect access to are given to the buyer for payment of the purchase price. Frequently, the accounts belong to financial intermediaries who, for example, responded to employment ads by fraudulent companies and in whose name new accounts were opened or who use their own existing accounts to process payments for their role as a financial intermediary. Often, these can also be accounts that have been opened using stolen identity data which are controlled by criminals with central access to them. After the payment has been received, it is either immediately converted into virtual assets or the funds are forwarded to trading platforms for virtual assets first, which are generally based abroad.

Reports in conjunction with fraudulent forms of investment and investment opportunities are another focal point. Here, the purported investments in virtual assets are simply used as a front. In actuality, defrauding the investors is the main aim of the game. In addition, a large number of STRs are also made in conjunction with unauthorised money or value transfer services. Here, the brokering of capital assets and shares relating to virtual currencies is offered without permission of the financial supervisory authority.

Based on the subject focus of the STRs considered here, it is clear that virtual assets can be used as a digital means of value for money laundering activity, particularly for forwarding illegally obtained funds quickly and concealing their illegal origins. This is supported by the fact that the traceability of virtual transactions still poses a challenge. Firstly, the amount of data is frequently insufficient to link transaction data with persons and secondly, in the virtual arena, assets can quickly be moved across geographical country borders and be transferred to foreign trade platforms, which makes tracing these transactions more difficult.

Almost all STRs in conjunction with virtual assets were reported to the FIU by credit institutions. In the main, the reports deal with traditional financial transfers, e.g. by way of bank transfers that indicate underlying transactions with virtual assets. To date, references to explicit transactions with virtual assets within the virtual arena have been relatively rare and have mainly come from law enforcement agencies and foreign partner FIUs. This highlights the importance of including providers of virtual asset services in the reporting entities group.

Case Study – Concealment with the Aid of Virtual Assets [26]

The unknown suspect opened five accounts with different credit institutions within a short period of time, using a fake identity. Four accounts received payments from victims of fraud over a period of several days. These sums were soon transferred to trade platforms for virtual assets. Some of the funds collected from two accounts were paid out in cash, in one case after they had been transferred to a credit card. The fifth account was blocked immediately after it had been opened as the credit institution had detected that a counterfeit foreign identity card was being used. All of the account-holding banks submitted STRs, mostly because the transfers had been cancelled by the victims and because of investigation queries.
Two of the three trading platforms for virtual assets that were used are based abroad. The forwarded funds were converted into Ethereum and Bitcoin on the third platform, which was German. After this, the virtual assets were forwarded via a network of various wallets. Some of these wallets also had funds paid into them from foreign trading platforms. It is likely that this was also money from victims of fraud. After multiple transfers of the virtual assets, the path that the funds had taken could be partly traced back to a trading platform on which the virtual assets were presumably converted back into euro.

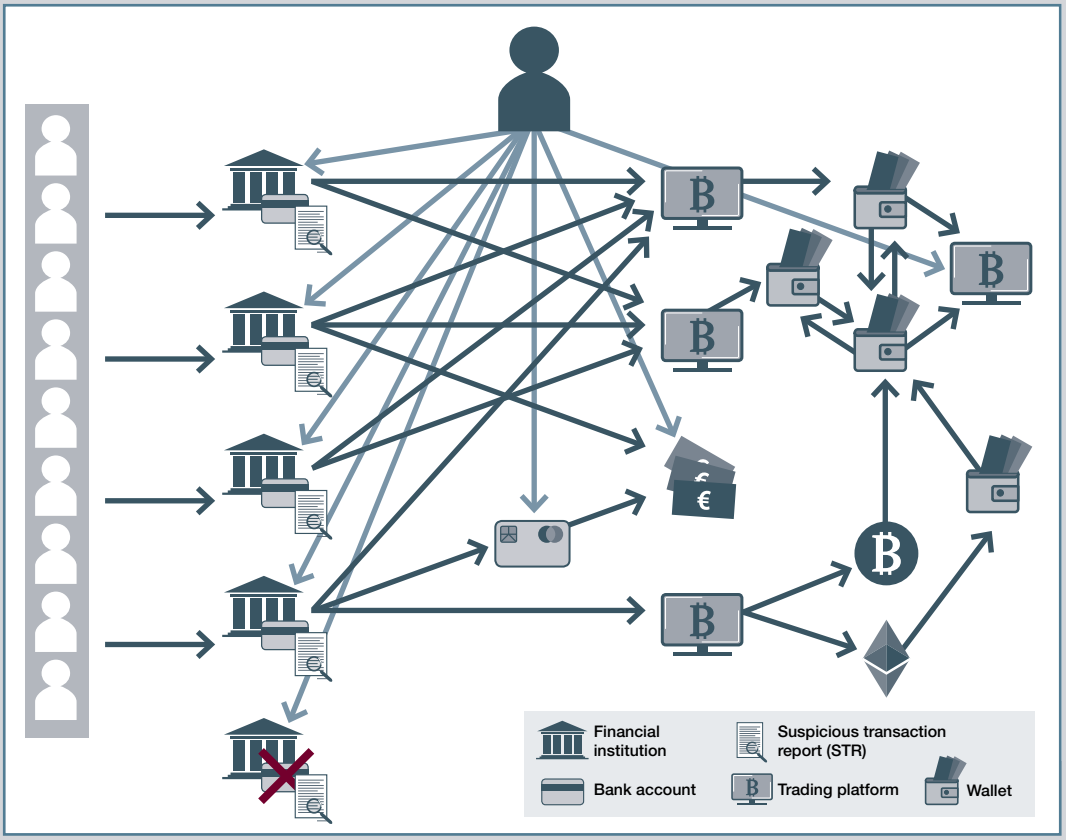


Figure 19: Case Study – Concealment with the Aid of Virtual Assets

26 The present case study is based on real STRs. To improve comprehension, various analytical complexes have been summarised, and transaction processes that are not clarified completely are shown as examples.

National Cooperation

Cooperation with Law Enforcement Agencies

Cooperation with Supervisory Authorities

Requests from Domestic Authorities

Cooperation with Reporting Entities under AMLA

National Cooperation

Figure 20: An Overview of National Cooperation

In order to enable the FIU to fulfil its legal duties, particularly the collection and analysis of information in conjunction with money laundering and terrorist financing, the close and sustained cooperation of all national authorities within the network is crucial. The FIU's national partner authorities include:

- the competent law enforcement agencies and judicial authorities (federal police and police of the Länder [German states], public prosecution authorities, the Financial Control of Illicit Employment, the Customs Investigation Service, tax investigation authorities),
- the competent supervisory authorities (including the German Federal Financial Supervisory Authority, various supervisory authorities of the Länder in the non-financial sector),
- the authorities of the fiscal administration (the Federal Central Tax Office, the fiscal authorities of the Länder), and
- the Federal Office for the Protection of the Constitution (BfV), the Federal Intelligence Service (BND) and the Military Counter-Intelligence Service (MAD).

In addition to cooperation with the national partner authorities, an active exchange with the reporting entities in accordance with Section 2 (1) AMLA is indispensable. The FIU came into contact with a diverse range of subgroups of reporting entities in 2019, particularly those from the non-financial sector, thanks to a wide variety of measures.

Cooperation with Law Enforcement Agencies

As in previous years, an active exchange with national law enforcement agencies was maintained in 2019. For example, the FIU's management completed its inaugural visits to the heads of all State Offices of Criminal Investigation and the Federal Criminal Police Office in spring 2019. This was followed by bilateral discussions at management level with public prosecution authorities.

The FIU organises conferences on an ongoing basis with the aim of promoting mutual understanding and intensifying cooperation. The bi-annual conference with the law enforcement agencies should be mentioned in particular, specifically with representatives of national police authorities (State Offices of Criminal Investigation and the Federal Criminal Police Office), representatives of the financial investigative bodies of the Länder, as well as representatives of public prosecution authorities of North Rhine-Westphalia, Schleswig-Holstein, the Central Organised Crime and Corruption Office of Celle and the Central Organisation Office for Asset Recovery of North Rhine-Westphalia. In addition to specialist discussions, these events covered diverse subjects such as the participation of the law enforcement agencies in identifying and assessing the key risk areas.

Work Shadowing
Mutual work shadowing between law enforcement agencies and the FIU are an important step towards expanding their trust-based cooperation. Through work shadowing, the guests were able to acquaint themselves with the working methods and to exchange information directly with other professionals.

In addition, the FIU furthered the awareness of cases that involve risks of money laundering or terrorist financing through several presentations on its work in the past year. Examples among the fiscal authorities include the conference of tax investigators, the professional conference for the audit service and the nationwide exchange of experience of the Financial Control of Illicit Employment on the subject of asset recovery. In addition, various police training events were held on the subject of money laundering.

Liaison Officers

In 2019, an important link in the cooperation was created with the pilot scheme involving the posting of liaison officers from the FIU (FIU LOs) to the State Offices of Criminal Investigation (LKAs). The FIU LOs promote a direct and trust-based exchange of information between the LKAs and the FIU.

The FIU LOs are the FIU's initial direct contacts for operational cooperation issues for the respective law enforcement agencies (police, customs, tax investigation authorities, public prosecution authorities) and other FIU cooperation partners in the Länder. In addition, they support the further process optimisation in the FIU's cooperation with, in particular, police authorities and public prosecution authorities. Their task is also to support the targeted communication of location-specific findings in line with quality optimisation and any required realignment when setting key risk areas within the FIU.

Within the framework of the pilot project, a total of six FIU LOs were initially sent to various LKAs (Berlin, Baden-Württemberg, Hamburg, Lower Saxony, Saxony, Mecklenburg-Western Pomerania and Hesse). The LKA Mecklenburg-Western Pomerania was supported by the FIU LO of the LKA Hamburg. The posting of liaison officers proved to be an effective means of achieving the above-mentioned goals, so that a posting of FIU LOs to all Länder is planned for 2020.

Cooperation with Supervisory Authorities

Strengthening cooperation with the supervisory authorities, especially in the non-financial sector, remained a key issue for the FIU in 2019.

In the course of 2019, the FIU organised a number of conferences for supervisory authorities where specialist topics were discussed and supervisory authorities had the opportunity to exchange information. For example, the FIU facilitated an inter-agency exchange with the two-day workshop "Combating money laundering in the real estate sector", which gave not only supervisory authorities but also law enforcement agencies and fiscal authorities the opportunity for joint discussions and, in the course of the workshop, involved associations and reporting entities in the real estate sector. This event illustrates how the FIU fulfils its coordinating function to ensure a comprehensive exchange of information between all participants on methods of money laundering and terrorist financing. In addition, the FIU participated in events organised by various supervisory authorities in order to support them by means of specialist presentations on money laundering typologies and to introduce the FIU's working methods.

In 2019, the FIU started its work shadowing programme at the supervisory authorities. The aim here is to gain a better understanding of supervisory activities and of the specific characteristics regarding the different groups of reporting entities in order to develop new support concepts for supervisory authorities.

First Concerted Campaign against Money Laundering in the Automotive Industry

In 2019, the FIU coordinated a concerted campaign by the supervisory authorities of the Länder with regard to the key risk area "use of cash (when procuring high-value goods)" identified by the FIU, specifically in the automotive industry. The aim was to carry out audits of reporting entities in the automotive industry within a specified period of time on the basis of pooled information in order to verify their implementation of obligations under anti-money laundering law. In preparation for the campaign, the FIU provided the respective supervisory authorities with relevant information on supervisory issues.

The campaign showed that there is a need for further awareness-raising among reporting vehicle dealers. It highlights the need for supervisory audits and underlines the effectiveness of the concerted campaign coordinated by the FIU.

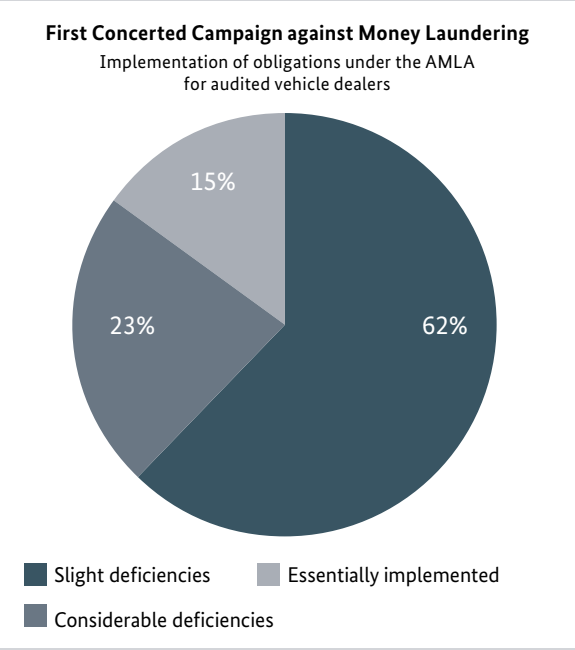


Figure 21: First Concerted Campaign against Money Laundering in the Automotive Industry

The good cooperation with the BaFin was successfully continued in 2019. The BaFin implemented its first work shadowing placements at the FIU. Joint meetings are held at regular intervals to ensure a continuous exchange of information between the two authorities in a spirit of mutual trust. The BaFin and the FIU have agreed on "principles of cooperation" in the area of prevention of money laundering and terrorist financing. These principles serve to structure and further intensify the cooperation and came into force in autumn 2019.

Requests from Domestic Authorities

If it appears to be necessary for the investigation of money laundering and terrorist financing or for the prevention of other risks, domestic authorities, such as law enforcement agencies and intelligence services in particular, are entitled to request personal data from the FIU under certain conditions. This is done by means of a request. In 2019, 3,260 such requests were submitted to the FIU.

The domestic requests increased by approximately 70% compared to the previous year. Police authorities and public prosecution authorities are increasingly availing themselves of the possibility to efficiently and promptly augment their investigations with information available at the FIU. This regularly involves requests as to whether reports of suspected money laundering have been submitted to the FIU for a suspect in a preliminary investigation conducted by the police and prosecutors. There has also been an increase in the number of requests from other bodies such as fiscal and supervisory authorities.

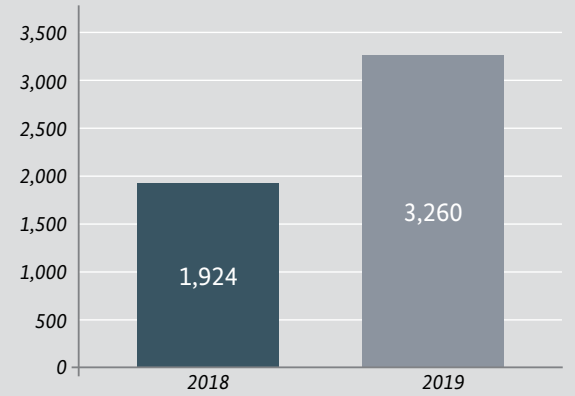


Figure 22: National Requests

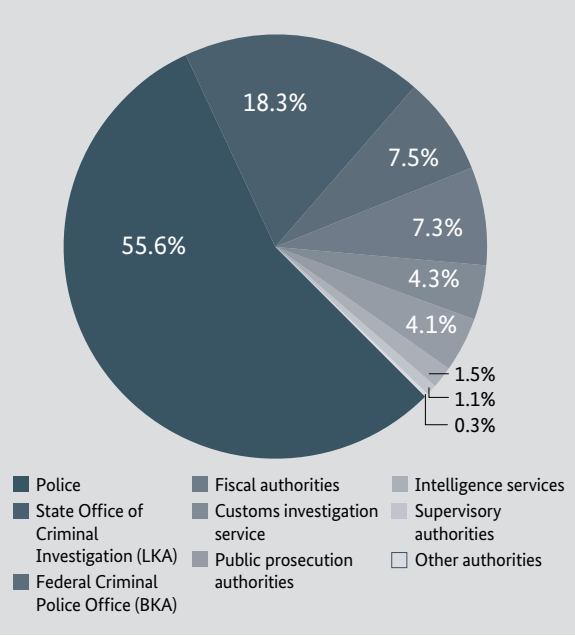


Figure 23: Breakdown of Domestic Requests by Sender

Case Study – Cooperation with the Federal Criminal Police Office [27]

The Federal Criminal Police Office (BKA) is conducting investigations on behalf of the Frankfurt am Main public prosecution authority against three persons suspected of involvement in acts of corruption pursuant to Section 108 e of the German Criminal Code (StGB) or Art. 2 (2) of the Act on Combating International Bribery (IntBestG). The suspects are a former member of the German Federal Parliament (MdB), an active MdB and another person. The suspects are allegedly involved in the receipt and redistribution of sums in the six to seven-digit euro range from a non-EU state, both through accounts held by the companies they manage and through their private accounts. In its request, the BKA asked the FIU to provide information on the persons, companies and organisations involved.

As a matter of fact, the FIU had information at its disposal that was related to the persons and companies in question. STRs involving the aforementioned persons were classified as reports on politically exposed persons due to their function as active or former German politicians. Various other STRs and requests from other authorities concerning these persons and the companies involved in the suspicious transactions were identified in the database.

For example, one credit institution reported abnormalities in a business account held with it. Since the opening of the account, credits totalling approximately EUR 3.4 million had been received from several alleged shell companies. Some of these companies were linked to organised money laundering operations. The credits were transferred to a German company of the former MdB and the other suspect and from there were partially transferred to a company account of the other suspect, who runs his own law firm. Both recipient accounts in turn showed large cash outflows to foreign accounts. The bank's assumption that the originators of the foreign payments to the German company of the two suspects could be shell companies was largely confirmed by FIU research.

Furthermore, the FIU obtained information from foreign partner authorities about companies and private individuals who were allegedly involved in organised money laundering operations and who could be connected to the BKA's investigative complex. Money had been transferred by various companies to individuals and companies generally involved in lobbying work. One recipient of these funds should be another German politician. In this way, the FIU was able to link several independently received STRs and information from partner authorities. The collected findings were then made available to the BKA, which provided valuable new insights for the BKA's investigative complex.

27 The present case study is a real case from the FIU's practice.

Case Study – SWIFT Hacking [28]

The FIU received a national request from a law enforcement agency. The request was based on a procedure described as "SWIFT hacking".
The law enforcement agency approached the FIU with the request to forward all STRs in the context of SWIFT hacking to it and to collect further information on the procedure described. The first step was to generate a query profile for the type of crime committed and use this to search for the relevant money laundering STRs of the reporting entities. As a result, a total of ten reports was clearly assigned to the topic "SWIFT hacking". The information they contained was prepared and sent to the law enforcement agencies for further processing.

SWIFT Hacking
"SWIFT hacking" refers to an attack against a bank or financial service institution. The attackers focus on the participants of the SWIFT network. With the help of malicious software that has been planted at the bank in advance, attackers can generate fake SWIFT messages within the SWIFT system (bank system for transmitting information and payment notifications for financial transactions) and place them in the SWIFT network. In this way, unauthorised payments to the attackers are triggered. Furthermore, applications are manipulated in such a way that order details are not displayed or hidden. This delays the detection of the fraud by the bank. It enables the attackers to spread the funds and get them "out of harm's way".

28 The present case study is a real case from the FIU's practice.

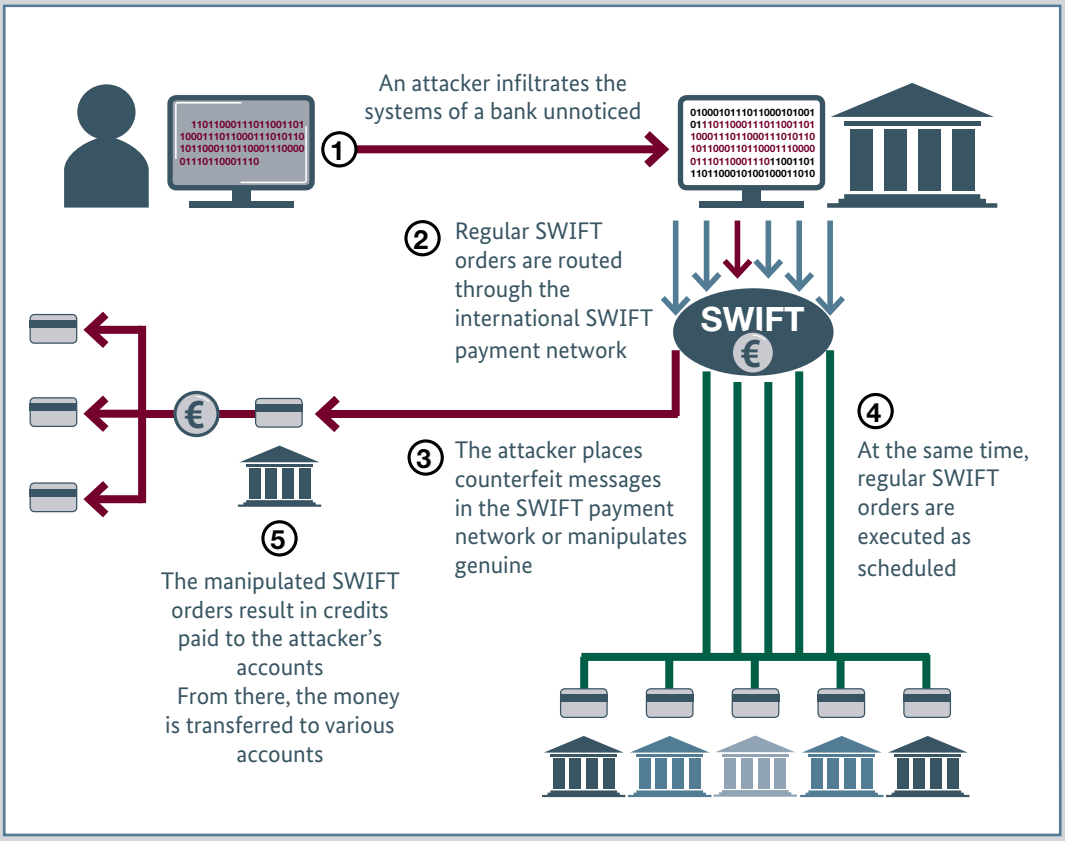


Figure 24: Schematic Representation of a SWIFT Hacking

Cooperation with Reporting Entities under AMLA

In addition to the existing formats used for the financial sector, cooperation with the non-financial sector in particular was intensified in 2019. In October 2019, the FIU's annual Money Laundering Conference with reporting entities and associations of the non-financial sector took place. Particularly associations from the areas of jewellery, gemstones and precious metals as well as art and antiques trading participated actively in this year. The event was characterised by expert lectures and discussions on relevant topics covered by the key risk areas, such as money laundering in the real estate sector, the gambling sector and issues in connection with trading valuable goods. The associations and reporting entities also participated actively by giving their own presentations, for example on the subject of money laundering in the real estate sector. One of the FIU presentations focused on the particular relevance of determining the beneficial owner in business relationships.[29]

The FIU intensified its cooperation with the reporting entities through various technical presentations at events, for example at conferences of the German Federation for Motor Trades and Repairs in Cologne and at the Institute for Notarial Law at the Friedrich Schiller University Jena.

Participation in Trade Fairs
A special form of information exchange took place in 2019 through the FIU's participation in trade fairs. The FIU was represented with an information booth
– at the AdvoTec trade fair and
– at DKM, the leading fair for the finance and insurance industry.
Visitors to the booth at both trade fairs were able to obtain comprehensive information, asked specialist questions and discussed the existing legal situation.

29 For further information on the beneficial owner, see the "Typologies and Trends" section.

Public Private Partnership – Anti Financial Crime Alliance

The prevention and combating of money laundering and countering of terrorist financing are central elements in protecting the economic cycle in Germany, the state and the economic operators from misuse of the financial systems, including in the non-financial sector, as well as from financial crime. To prevent, detect and punish money laundering and terrorist financing, the interaction of the FIU with supervisory authorities, law enforcement agencies and private sector institutions, both financial and non-financial, is crucial. In order to intensify cooperation between the authorities and private sector institutions involved in preventing and combating money laundering, a "public private partnership" (PPP) was founded in September 2019 under the umbrella of the FIU.

To date, this national form of cooperation is unique in the field of financial crime in Germany. The plan is to facilitate an intensive and lasting exchange of information from the public and private sectors with the aim of jointly identifying new trends and developments and developing optimisation potential for the reporting of suspected money laundering. Both sides can contribute their respective strengths and specific know-how to the new alliance and also benefit from the skills of the other side in a long-term cooperation. The alliance is establishing a long-term strategic cooperation in the field of money laundering and terrorist financing and strengthening the cooperation as joint partners. This partnership is called the "Anti Financial Crime Alliance" (AFCA for short).

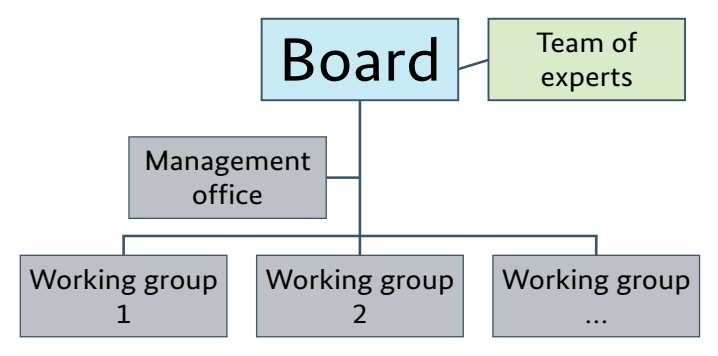


Figure 25: Structure of the AFCA

Structure of the AFCA

The Board is composed of an equal number of public sector representatives and private sector reporting entities. It is responsible for the strategic orientation of the AFCA and is advised by a team of experts. The Management Office incorporated in the FIU is the main interface between the various participants and users and the Board of the AFCA. The operational core is formed by the working groups, which meet regularly, have clear time limits and are demarcated regarding their subject matter. When the AFCA was founded, two working groups were set up: Working group 1, "Principles of cooperation" deals with issues relating to the further development of rules and methods of cooperation within the AFCA, such as the further development of the founding documents or the elaboration of operational processes for shaping cooperation between the working bodies or the preparation of statements on issues relating to the functioning of the AFCA. In working group 2, "Risks and trends in the area of money laundering and terrorist financing in the financial sector", participants exchange views on facts regarding specific phenomena and topics of common interest relevant to suspicious transaction reporting. The establishment of further working groups is planned. The structure of the AFCA follows a partnership-based approach with equal input from all participants, thus allowing for strategic exchanges related to problems and phenomena between government institutions and the private sector.

International Cooperation

Information Exchange with other FIUs

International Committee Work

International Cooperation

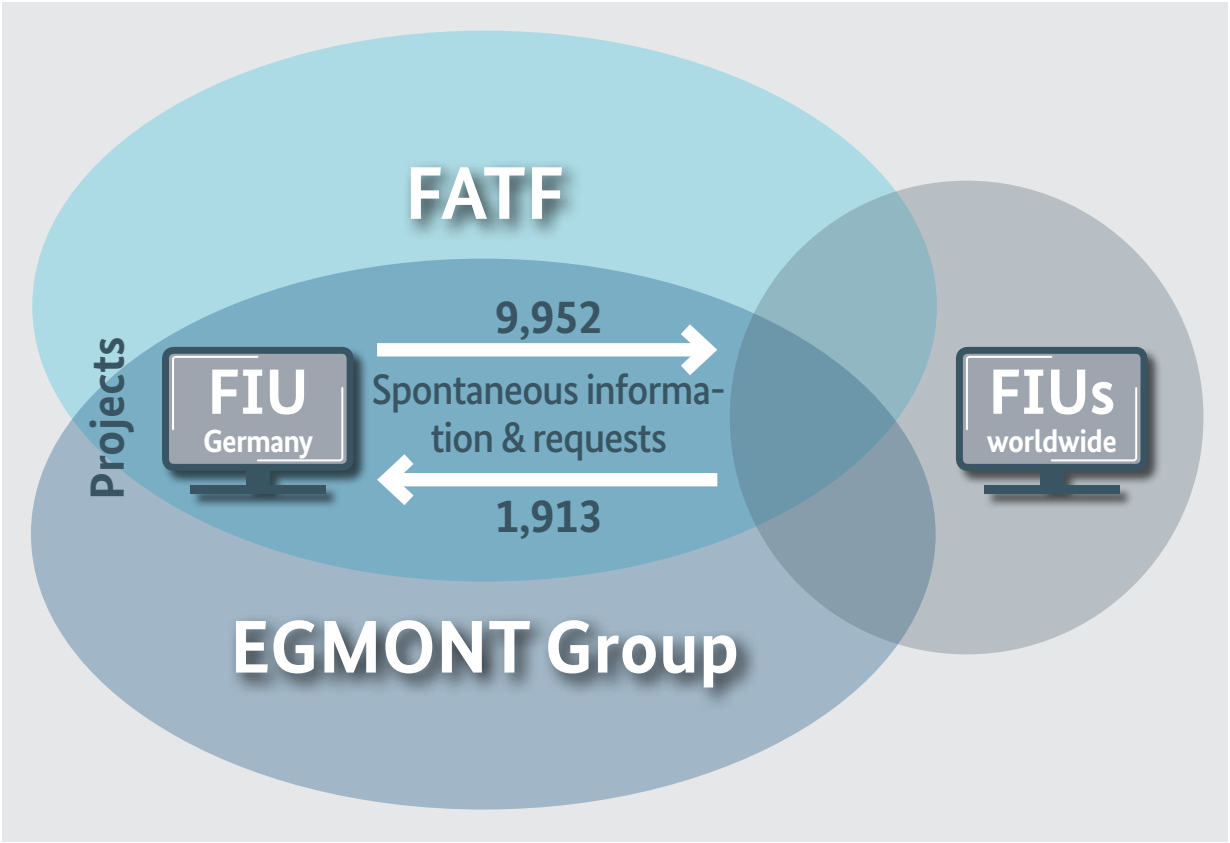


Figure 26: An Overview of International Cooperation

In order to effectively prevent and combat money laundering and counter terrorist financing, international cooperation is indispensable in addition to sustained cooperation with all national authorities within the network. In 2019, the FIU Germany further expanded both the information exchange with other FIUs and its international committee and project work.

Information Exchange with other FIUs

In this exchange, relevant information is continually and proactively passed on to the international partner FIUs or made available upon request. This ensures that cross-border structures and cases can also be comprehensively investigated. International cooperation with other FIUs is carried out at the operational and strategic level, always in strict compliance with the Egmont Group's guidelines. The exchange of information between the FIU and its European and international partner authorities always takes place via Egmont-Secure-Web or FIU.net.

In 2019, the FIU exchanged information in this way with a total of 149 countries. The cooperation with EU countries such as France, Italy, Great Britain, Luxembourg, the Netherlands, Malta and Finland was particularly close.

Incoming and Outgoing Information and International Requests

In 2019, the total number of international cooperation cases rose to 11,865 (2018: 6,355).

This figure included 2,327 requests (2018: 2,101) and 9,538 incidents of spontaneous information[30] (2018: 4,254). This increase shows that the FIU Germany does justice to its responsibility as an actor in the international association of FIUs worldwide and has successfully established itself in this area.

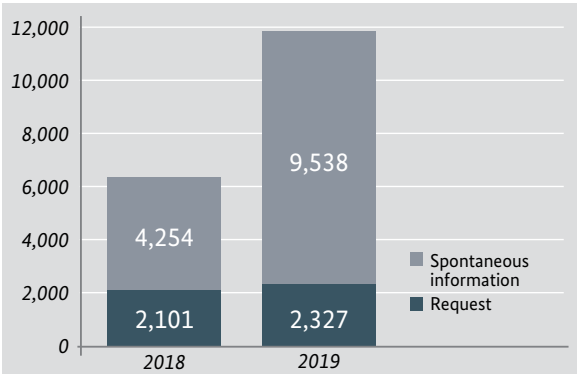


Figure 27: Cases of International Cooperation in a Year-On-Year Comparison

30 Spontaneous information is the proactive communication of an issue that may be relevant to a partner FIU without being linked to a request sent by the partner authority.

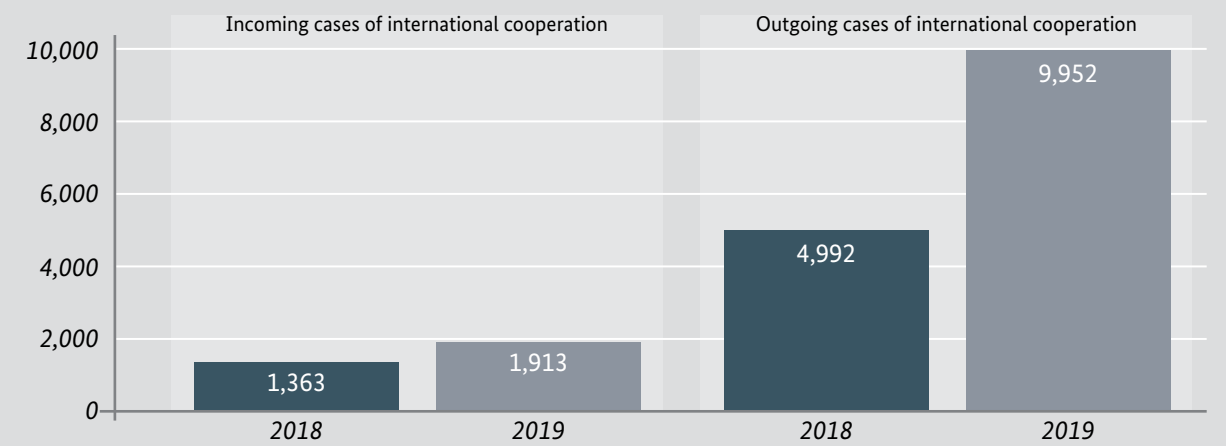


Figure 28: Incoming and Outgoing Cases of International Cooperation

The intensive exchange with the FIUs international partners is especially demonstrated by the pronounced increase in cases, particularly for outgoing cases, that totalled 9,952 (2018: 4,992). In total, the FIU sent outgoing information to partner FIUs in 141 countries.

While the number of outgoing international requests remained almost identical at 1,218 (2018: 1,255), the 8,734 incidents of outgoing spontaneous information were more than double the previous year's figure (2018: 3,737). With 78 %, the majority of this spontaneous information was addressed to EU FIUs, and the cooperation with France and Italy was of particular note.

In addition, FIU Germany received a total of 1,913 cases from over 100 different FIUs worldwide. Of these cases, 1,109 (2018: 846) were incoming international requests and 804 (2018: 517) were incoming spontaneous information. Of the total of 1,913 incoming cases, 1,411 originated from FIUs from a total of 27 EU countries. This represents a significant increase compared to 2018. However, as in the previous year, the majority of the cases received were international requests at 58 %.

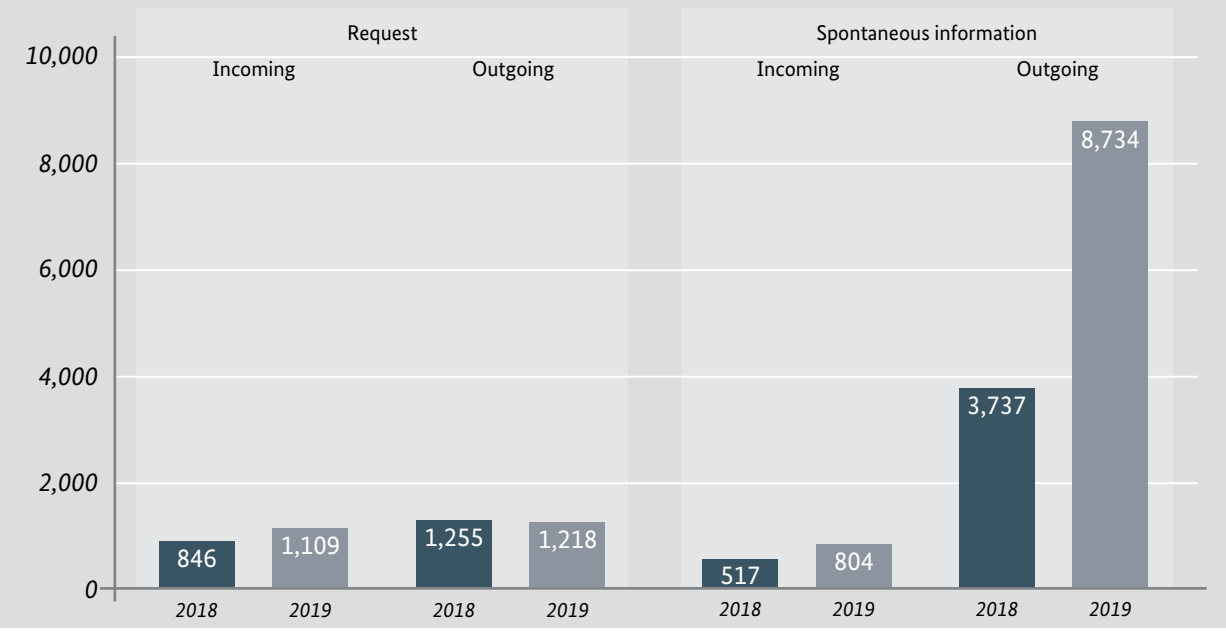


Figure 29: International Requests and Spontaneous Information in a Year-on-Year Comparison

As shown in the following diagram, the international cooperation cases (requests and spontaneous information) received by the FIU Germany in the reporting year 2019 mainly originated in the neighbouring EU countries as well as Malta and Finland. With regard to FIUs from non-EU countries, the cooperation with the FIUs in the USA and Russia was a key issue.

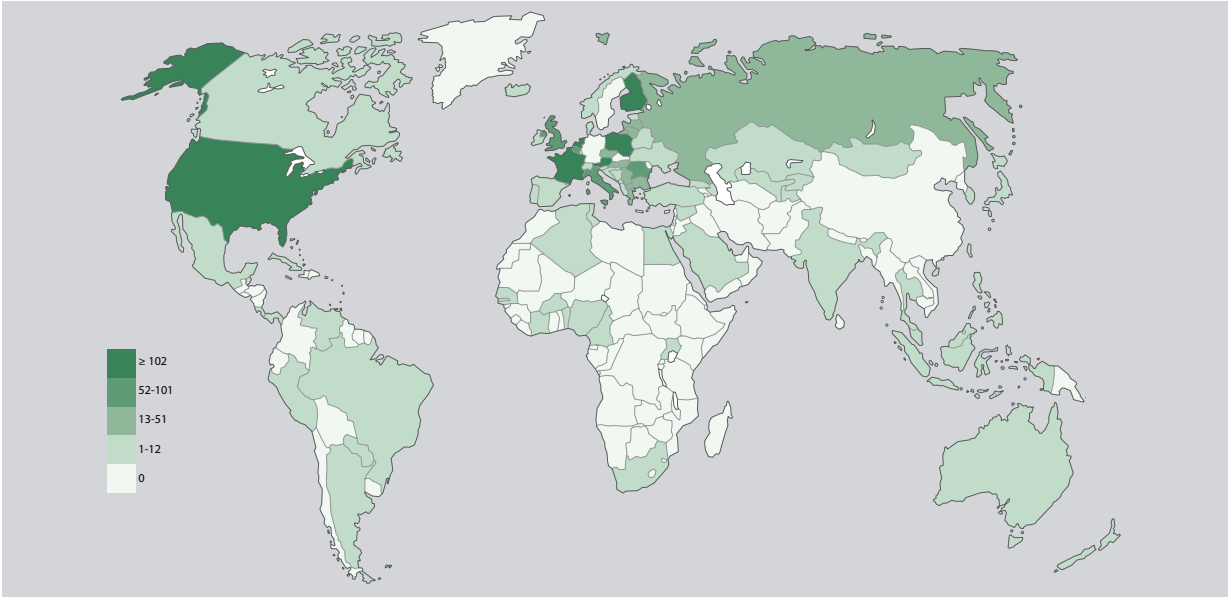


Figure 30: Incoming Cases of International Cooperation by Country of Origin

Neighbouring and non-bordering EU states also played an important role regarding requests and spontaneous information disseminated by the FIU Germany. A large proportion of outgoing requests and spontaneous information concerned France, Italy, Great Britain, Spain, the Netherlands and Austria. With regard to FIUs from non-EU countries, there was an intensive exchange with Argentina, Switzerland and the British Virgin Islands.

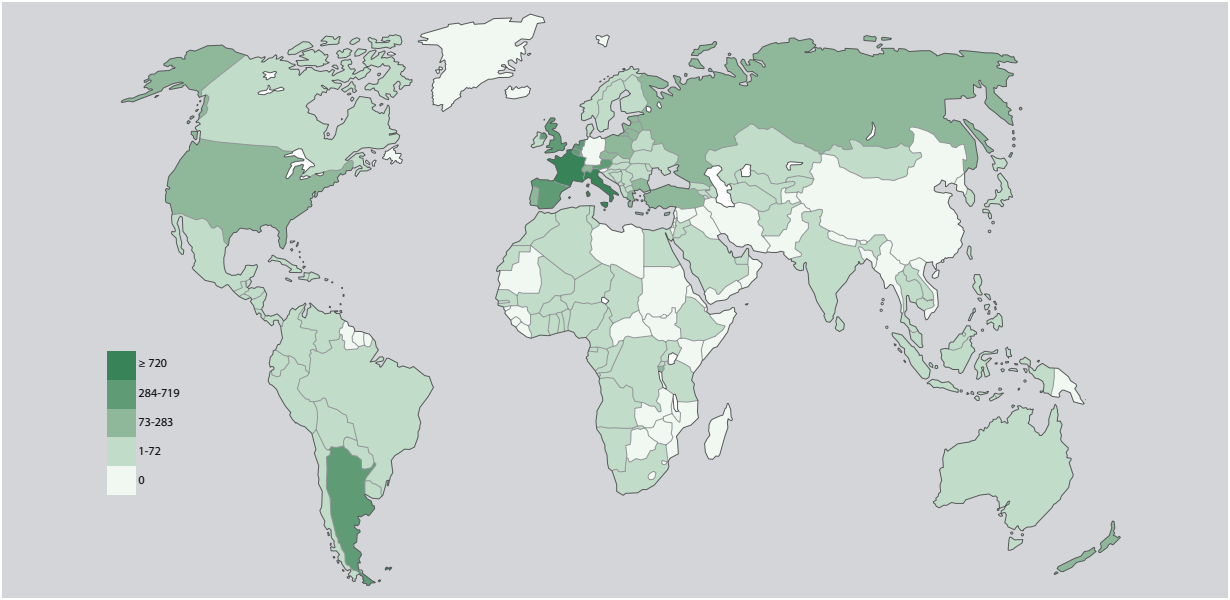


Figure 31: Outgoing Cases of International Cooperation by Country of Destination

The following tables illustrate the main addressees and senders of incoming and outgoing international requests and spontaneous information in the reporting year. Through a direct comparison of the respective top 10, the close cooperation with the neighbouring EU countries France, Luxembourg and the Netherlands becomes particularly apparent. In addition, particularly regular exchanges took place with Italy, Spain and Great Britain.

Country	Incoming international requests
France	148
The Netherlands	73
Luxembourg	65
Malta	52
Italy	46
Finland	43
Austria	40
Belgium	36
Great Britain	35
USA	34
Other FIUs	537
Total	**1,109**

Country	Outgoing international requests
Luxembourg	163
Great Britain	94
Lithuania	72
The Netherlands	71
Spain	65
France	50
Ireland	47
Austria	46
Switzerland	44
Poland	43
Other FIUs	523
Total	**1,218**

Country	Incoming spontaneous information
Luxembourg	190
Malta	141
Austria	62
USA	52
Poland	47
Finland	41
Gibraltar	30
Slovakia	20
Jersey	20
Great Britain	17
Other FIUs	184
Total	**804**

Country	Outgoing spontaneous information
France	3,260
Italy	692
Spain	386
Great Britain	360
Argentina	355
The Netherlands	327
Belgium	263
Austria	260
Cyprus	179
Switzerland	155
Other FIUs	2,497
Total	**8,734**

Table 3 a-d: Number of Incoming and Outgoing Spontaneous Information and International Requests by Country

Temporary Freezing Orders

A further instrument for effectively combating money laundering is the securing of funds from allegedly criminal activities on request via a temporary freezing order.

A total of five temporary freezing orders were implemented as a result of incoming requests from other FIUs. In three cases, an account was temporarily blocked completely, in the other two, transactions were temporarily halted. The temporary freezing orders involved a total volume of over EUR 4 million.

Case Study – International Temporary Freezing Order for Carousel Fraud [31]

The FIU of an EU Member State asked the FIU Germany for further information against the background of investigations into VAT fraud and the illegal use of petroleum products as fuel which were being conducted there. In this process, raw materials were shifted between EU Member States as part of an intra-community supply chain, their freight and delivery documents were falsified and the original goods were re-declared as fuel. The request gave indications that accounts held in Germany might be involved.
The FIU Germany transmitted related personal and company data to the requesting FIU and immediately issued two temporary freezing orders, as a result of which account balances totalling around EUR 3 million were temporarily frozen. The FIU also noted that the companies and persons involved had already been found to have acted in connection with violations of the provisions of the Energy Tax Act. Based on past experience, the FIU identified the logistics chains as a typical approach in (petroleum) tax offences. Based on the analysed account activity of the companies concerned, the suspicion was further substantiated.

Carousel Fraud
A "carousel fraud" is a common form of tax evasion in the EU involving a large number of companies. It involves exploiting legal regulation of a VAT-exempt delivery between companies within the EU to sell tax-exempt goods to Germany. The VAT which is incurred when the goods are resold several times within Germany is then added to the value of the goods by the seller, but is not paid to the tax office. When "reselling" the goods across the border, the last seller can have the VAT refunded by the tax office, even though the latter has not collected the corresponding VAT.

31 The present case study is a real case from the FIU's practice.

In this case, the successful cooperation with the foreign FIU supported further criminal prosecution there. This led to the arrest of persons, the seizure of assets and the assertion of claims for compensation from the material benefits gained. The facts of the case were forwarded to a domestic law enforcement agency for possible further investigations and in order to maintain the asset protection measures.

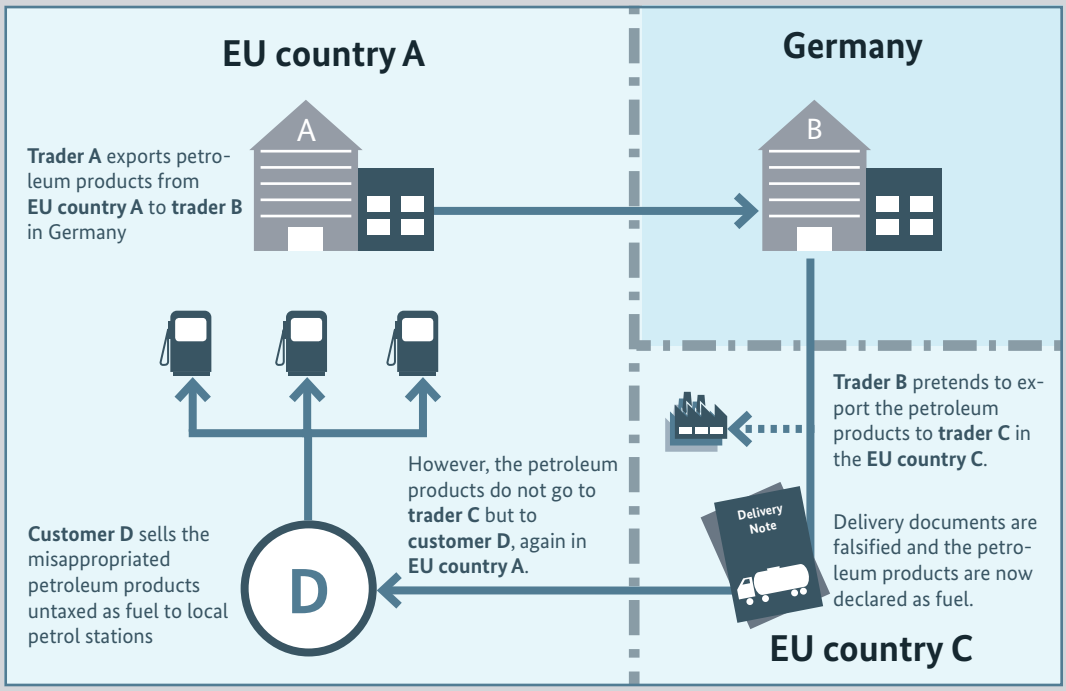


Figure 32: Case Study – Carousel Fraud

International Committee Work

An elementary component of the FIU's strategic objective is to intensify and optimise international relations through active participation in international committees and organisations and participation in international workshops dealing with the topics of money laundering and terrorist financing. The FIU's aim is to integrate with these structures so that it can exchange and apply new findings, approaches and analysis products profitably in its daily work.

This strategic cooperation can be bilateral or multilateral. In the 2019 reporting year, representatives of the FIUs of the Czech Republic, the Netherlands, North Macedonia and Belgium visited the FIU Germany. In addition, the FIU Germany visited the Chinese and British FIUs abroad. The aim of these meetings is to exchange views on cooperation with reporting entities, law enforcement agencies, supervisory authorities and international partners and to gain an overview of the methods used in operational and strategic analysis, including the IT used for each.

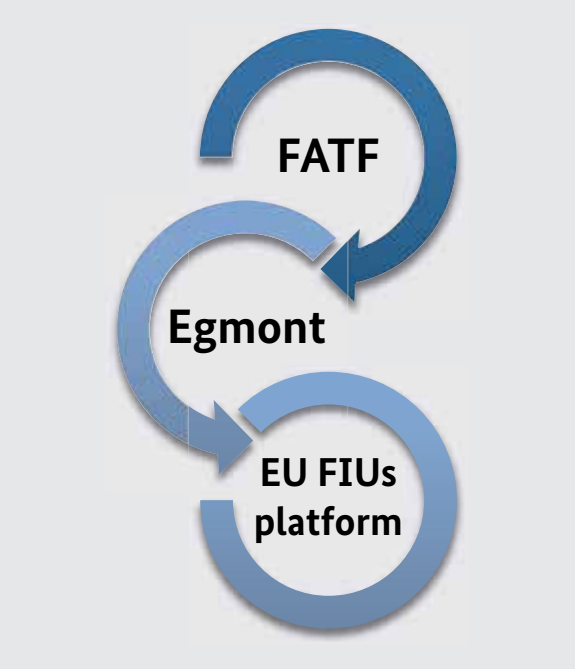


Figure 33: International Committees

In addition to the bilateral meetings, the FIU also takes part in the regular multilateral cooperation meetings of all German-speaking FIUs (Austria, Liechtenstein, Luxembourg, Switzerland).

Financial Action Task Force (FATF)

The FATF is the main international committee for preventing and combating money laundering and countering terrorist financing. It sees itself as an intergovernmental working group with the aim of preventing and combating money laundering at the international and national level and enabling the detection of assets of illegal origin. To this end, it makes recommendations and regularly reviews its members for compliance and effective implementation. To date, the FATF includes 37 states, the EU Commission and the Gulf Cooperation Council.

In 2019, the FIU Germany was part of the German delegation led by the Federal Ministry of Finance (BMF) at the three annual FATF plenary sessions. In this context, the specialist involvement of the FIU has grown steadily. The FATF plenary sessions were preceded by forums of the heads of FIUs. The German FIU was actively involved in preparing and implementing those forums.

Egmont Group of FIUs (Egmont Group)

The Egmont Group is a network of currently 164 FIUs with the objective of promoting cooperation and the exchange of expert knowledge and financial information between the individual FIUs. For the joint prevention and combating of money laundering and countering of terrorist financing, the five working groups of the Egmont Group regularly define various focal points in order to discuss specialist issues and develop new approaches.

The FIU Germany regularly takes part in the plenary and working group meetings held during the year and is an active member of working groups in several projects of the Egmont Group. In addition to its involvement in the Membership, Support and Compliance Working Group (MSCWG), the FIU Germany primarily supports the MSCWG Pool of Experts. The Pool of Experts is responsible for reviewing country reports and interpreting the FATF standards and the additional standards set by the Egmont Group. Many new approaches, also from a strategic point of view, were realised in the Information Exchange Working Group (IEWG). The working group, chaired by the deputy head of the FIU Germany, was for example able to refine the future orientation of the IEWG and to implement a new business plan for the years 2019 – 2020. The aim of the IEWG is to deliver tangible results that support the FIUs in their day-to-day work and benefit the Egmont Group as a whole.

In this context, several projects were launched with the participation of the FIU Germany, which include the following focal points:

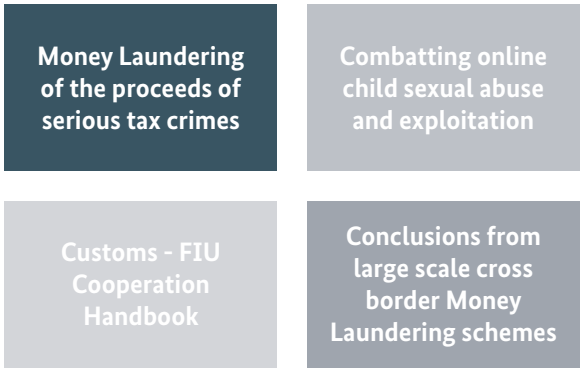


Figure 34: Egmont Projects

International Cooperation Project
"Conclusions from large-scale cross-border Money Laundering schemes"
The strategic evaluation project started in the summer of 2019 and is implemented within the Egmont IEWG under the direction of the FIU Germany together with eleven other FIUs. The central question for the international FIUs is what lessons can be learned from the analysis of so-called laundromats[32] and how the knowledge gained can be used to create added value for the future, especially regarding the early detection of conspicuous financial flows and the generation of up-to-date operational findings.

EU FIUs Platform

The EU FIUs platform is an expert group established in 2006 by the European Commission. The focus is on strengthening cooperation and professional exchange between European FIUs. In addition, the Commission supports its members and is advised by them on specialist issues.

In this context, the FIU Germany is consistently and strongly committed at the European level. In addition to its thematic cooperation, the FIU regularly participates in several EU projects, which focus primarily on optimising collaboration with European FIUs in the operational area.

32 Cf. the explanation in the section "Suspicious Transaction Reports (STRs)".

Terrorist Financing and other Crimes Relevant to State Security

Total Number of STRs Related to Terrorist Financing or State Security

Temporary Freezing Orders

Proliferation Financing

Strategic Evaluations of the Phenomenon of Terrorist Financing and State Security

Information Exchange in the Area of Terrorist Financing and State Security

Terrorist Financing and other Crimes Relevant to State Security

Total Number of STRs Related to Terrorist Financing or State Security

Between 1 January and 31 December 2019, a total of 6,253 of STRs were received by the FIU that contained initial indications of relations to terrorist financing or state security.

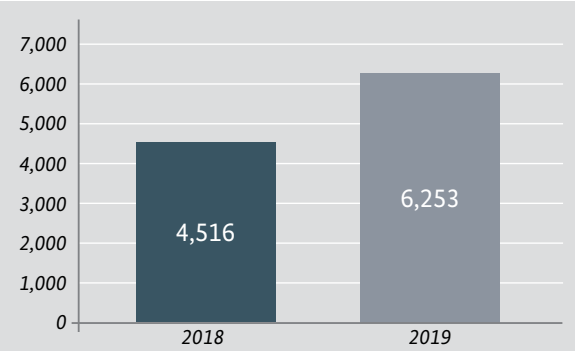


Figure 35: STRs Related to Terrorist Financing or State Security

In 2019, the number of STRs related to terrorist financing or state security thus rose compared to the 2018 reporting year. In relation to the total number of STRs, the proportion of STRs related to terrorist financing or state security is around 5 %.

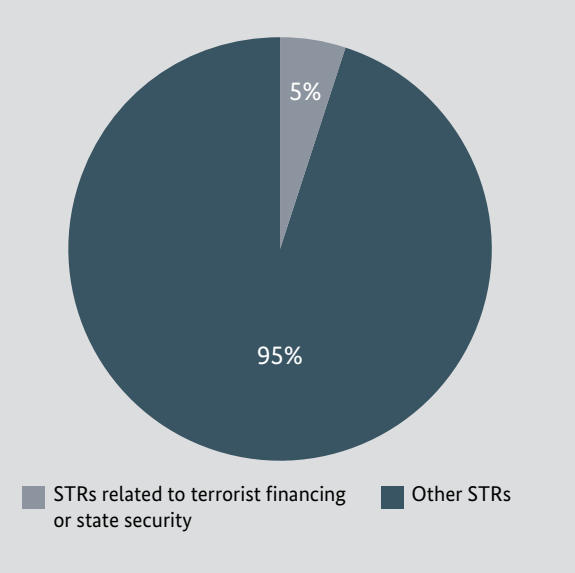


Figure 36: Relative Proportion of STRs Related to Terrorist Financing or State Security

Proposals to increase the total number of STRs and improve the quality of reporting were stepped up in the reporting period and, in this context, were regularly directed towards the reporting entities by the responsible unit. In addition to these FIU-specific measures, the reporting behaviour of the reporting entities themselves is also influenced by media events, global and regional political developments and supervisory measures. Against this background, an increase in the total number of STRs can also be expected in future.

Temporary Freezing Orders

In the reporting year 2019, there were two cases where the operational analysis regarding temporary freezing orders revealed the need to further examine whether a transaction was related to terrorist financing or other offences relevant to state security. Accordingly, two temporary freezing orders pursuant to Section 40 AMLA were issued with a total volume of approximately EUR 21,000, in the course of which transactions were stopped in order to shed more light on the facts of the case.

One of these temporary freezing orders was issued in the context of an STR containing indications of a possible affiliation with the Salafi scene and the associated illegal fundraising activities allegedly used to finance terrorism. The case was handed over to the competent law enforcement agency after completion of the FIU analyses.

Facts Relevant to State Security
Facts relevant to state security are those cases which have as their object a serious act of violence endangering the state or the preparation of such an act, including cases where measures must be taken to protect the internal and external security of the state, its institutions and symbols. In addition to counter-espionage and the observation of anti-constitutional developments, this also includes processes that serve to avert danger and prosecute politically motivated crimes.

Case Study – International Temporary Freezing Order for Possible Affiliation with the Salafi Scene; Illegal Fundraising [33]

Initial STR

An individual personally notified a bank of the receipt of payment for a five-digit amount, reportedly from a car sale, which was to be withdrawn in cash. In this context, the customer support employee noticed a change in the customer's external appearance, which prompted him to submit an STR. According to internal research by the reporting entity, the account turnover also revealed a possible connection of the customer to an Islamic community. The matter was reported as urgent, since the customer had already announced a prompt cash withdrawal at the time the funds were credited.

FIU Analysis and Dissemination

In the course of the FIU analysis, it was initially established that the individual did not have a vehicle registered to them, which made the customer's statement that the incoming payment came from a car sale seem implausible. In addition, numerous accounts in Germany and abroad could be assigned to the individual. For further analyses and research, in particular to obtain further information from foreign partner FIUs, the FIU prohibited the announced cash withdrawal of the amount received in accordance with Section 40 AMLA before it could take place.
Requests for information were immediately sent to foreign partner FIUs for further analysis. An FIU located in an EU Member State subsequently provided the information that there were numerous accounts held with a payment service provider in that country where various payments declared as donations had been received. The transfer references included allusions to excerpts from Islamic prayers and to the Zakat, the religious duty to share wealth in Islam. The subsequent analysis of the account turnover showed that the amounts from several originators, flowing together in only one user account held with the payment service provider, corresponded exactly to the amount subsequently received by the customer's account in Germany. A transfer of the pooled donations to Germany was thus traced by the FIU. The analysis report with the research results presented above was subsequently disseminated to the competent LKA. The procedure described above corresponds to a typical modus operandi of terrorist financing, in which payments are made by various originators with no discernible plausible connection between the parties involved in the transaction ("many-to-one").

33 The present case study is a real case from the FIU's practice.

Proliferation Financing

Proliferation refers to the spread of weapons of mass destruction, in particular nuclear, biological, chemical and radiological weapons, which includes their launcher systems, technologies, know-how and the materials or components needed to manufacture them. Strict legislation and effective export controls are indispensable in Germany, since various high-risk states continue to be dependent on the world market for research and production of weapons and launcher systems in spite of their own, sometimes considerable, technical progress.

Indications of proliferation financing come not only from incoming STRs but also from communications from intelligence services and reports by foreign authorities. When processing individual cases, the FIU is in close contact with the Customs Investigation Service, in particular the Customs Criminological Office.

There are international standards for combating and preventing proliferation financing with the aim of detecting or preventing the distribution or spread of the aforementioned goods, technologies and know-how. Despite its strict export controls, Germany can be the target of procurement efforts by high-risk countries. In particular, the settling of transactions and the associated disguised transaction paths are diverse and subject to constant change in order to circumvent export control procedures. In addition to existing export control procedures, the analysis of STRs and in particular the respective financial flows serve to identify proliferation-promoting activities at an early stage.

Some possible circumventions of legal export regulations are the inclusion of companies, persons or state institutions (e.g. universities) that are free from suspicion as addressees of a delivery or the processing of transactions via unsuspicious third countries.

A total of 26 STRs related to the risk countries Iran and North Korea that contained possible links to proliferation financing were submitted to the FIU. In the reporting period, fewer STRs were received compared to the previous year, as the reporting entities had conducted specified and project-based searches for these countries in 2018 and did not do so in the reporting period.

Strategic Evaluations of the Phenomenon of Terrorist Financing and State Security

Key Risk Area: Misuse of NGOs/NPOs

The introduction of the key risk area "Misuse of NGOs/NPOs" was carried out together with the other key risk areas defined on 16 July 2019 and is a result of the FIU's risk-based approach. The fight against terrorism is a top priority for Germany. Because of its role as a central agency, the FIU is an important player here, bringing together incoming information in a targeted manner and processing it based on risk.

The terrorist threat situation in Germany is currently characterised predominantly by Salafi movements and globally oriented jihadi groups that do not have own organisational structures in Germany.[34] Likewise, numerous foreign terrorist groups have significant circles of supporters in Germany. In this context, a possible approach to supporting terrorist financing activities is the targeted use of fake charitable organisations (NGOs/NPOs) which are under the complete control of terrorist organisations or the misuse of legitimate aid organisations.

Non-governmental Organisation (NGO)
Non-governmental organisations are private or public organisations that represent political interests, but are not subordinate to the state or government and do not operate for the purpose of making a profit. In principle, this includes all associations or groups that represent common interests (e.g. in the fields of environmental protection, animal welfare, human rights, health care and development work). These include, for example, trade unions, religious communities and citizens' initiatives, as well as foundations or associations.

Nonprofit Organisation (NPO)
Nonprofit organisations do not operate for the purpose of making a profit and are established for social (such as religious, cultural, educational, social and family) purposes. They can either be established in private form, for example as an association, federation or foundation, or as public NPOs, e.g. as a public enterprise or administration. Unlike NGOs, however, they do not generally address political issues and also generate their own financial resources, meaning that they are not funded exclusively by membership fees.

34 Cf. National Risk Analysis 2018/2019, Federal Ministry of Finance, p. 44 (see footnote 1).

Risk Relevance of NGOs/NPOs

NGOs and NPOs are particularly vulnerable to misuse for terrorist financing purposes. Due to their purpose and social orientation, these forms of organisation enjoy a high level of social prestige and trust. NGOs/NPOs regularly act across country borders and have a large amount of financial resources, which makes them attractive for terrorist purposes. Numerous disbandment proceedings regarding NGOs/NPOs in recent years have shown that these forms of organisation are being misused for the purpose of terrorist financing.

The core risks of NGOs/NPOs are either of organisational or sectoral origin, thus exposing the organisations to the partial or complete misappropriation of assets:

- NGOs/NPOs can be misused or misappropriated by internal actors – e.g. the staff of an aid organisation – or external actors – e.g. payees operating in a crisis region – for the purpose of illegal or terrorist activities. These are risks inherent in the form of the organisation, which mostly occur in lawfully established NGOs/NPOs (organisational risk).
- NGOs/NPOs can use their defined objectives and purposes to cover up a misuse of all the available assets for illegal or terrorist purposes. This is a fundamental sectoral risk, which occurs in particular in connection with sham organisations which falsely present themselves as nonprofits but which in fact have close ties to terrorist or extremist organisations and completely misappropriate the assets (sectoral risk).

Figure 37: Possibilities for Misuse of NGOs/NPOs

In the view of the FATF, the NGOs/NPOs involved in service activities – especially in the field of humanitarian aid – and thus operating in crisis regions are particularly exposed to risk. In addition, the FATF focuses on NGOs/NPOs which generally operate regionally, but whose supporters are inclined towards terrorist or extremist organisations ("Terrorists think globally, act locally"). Hence, the FIU pays special attention to organisations that operate in crisis regions and war zones. The FIU also focuses on risk factors directly related to natural and legal persons. Concrete actors and the cooperation of several organisations can be conspicuous flags for a connection with terrorist financing. At the same time, there is increasing evidence in Germany that individual organisations are particularly vulnerable to terrorist financing and are being misused.

Characteristics of Terrorist Financing

The involvement of the NGO/NPO sector in connection with terrorist financing can, in principle, be classified as all three characteristics of the internationally recognised triad: "raising", "moving" and "using" of funds. Since the assets in question are usually raised outside crisis regions, are moved into crisis regions with the involvement of NGOs/NPOs and are used there for terrorist purposes, all activities related to these assets can be gateways for terrorist financing.

Raising:
With respect to donations, in particular when raising funds, both knowing and unknowing supporters can become originators of risky transactions. The FIU's finding that the transactions in question could serve to finance terrorism is therefore primarily related to persons. In the context of identifying such transactions, the FIU regularly recognises abnormalities regarding persons under observation of the Federal Office for the Protection of the Constitution (BfV) or the State Offices for the Protection of the Constitution (LfV) or the sanctions list returns relevant search hits. It is also an observable fact that calls for donations previously made on social media serve as a trigger for the subsequent donation payments.

The transitions between the characteristics of terrorist financing are fluid. Reported facts can therefore always concern several characteristics, as the following example illustrates:

One-to-many
STRs through which incoming payments can be identified that are subsequently transferred to numerous recipients (mostly other private accounts or association accounts) with no discernible plausible connection between the parties involved in the transaction.

Many-to-one
STRs through which incoming payments can be identified that are borne by different originators (usually other private accounts or association accounts) with no discernible plausible connection between the parties involved in the transaction.

Moving:
The transferring of financial resources, e.g. because they have to be temporarily stored or because the movement of the funds is to be concealed, is also possible with the involvement of NGOs/NPOs. Underlying FIU analyses show that, in particular, extremist associations, their sympathisers or trusted third parties are involved in the settling of transactions, as payments declared as donations are made via their private accounts and are then usually withdrawn as cash. The use of alternative transaction channels often results because of previous cancellations of the association accounts concerned by the account-holding institutions.

Using:
The FIU's findings show that STRs are increasingly being submitted regarding funds that are withdrawn (mostly in cash) in crisis regions, the actual use of which cannot – after leaving the paper trail – be traced on the basis of transaction data, and that consequently, a connection with terrorist financing cannot be excluded.

Cash Withdrawal in the Region on the Border with Syria
An STR was submitted regarding two cash withdrawals of six-digit amounts which were previously transferred to the account by way of numerous small donations by various private individuals.

Total Number of STRs for Reporting Year 2019

Since the introduction of the key risk area "Misuse of NGOs/NPOs" on 16 July 2019, the FIU assigned a total of 133 STRs to this indicator, which were subjected to an in-depth analysis. Among other things, the activities of the NGOs/NPOs already under observation by the BfV or LfV were analysed, as well as the activities of organisations which were previously the subject of relevant negative media coverage. The recipients of the transactions concerned are often the organisations under observation; the reporting entity will then submit an STR in the event of "donations" made to crisis regions. Generally, the payments or facts in question therefore have a background which is potentially relevant to terrorist financing, but they may also have other backgrounds or explanations. Consequently, the STRs assigned to the risk indicator are not exclusively cases where misuse of NGOs/NPOs has been detected or confirmed, but are initially cases where an in-depth FIU analysis must be carried out to shed light on the background of the payment. Therefore, the STRs concerned only contain indications of a possible existing risk in connection with terrorist financing.

After immediately forwarding the report to the BfV, the FIU analyses the transactions or facts reported as suspicious and then forwards them to the competent law enforcement agency if there are actual indications that the transaction could serve to finance terrorism. The STRs concerned contain relevant, forwardable information – both in the report itself and as a result of the analysis. Such indications may be based on the transactions' frequency, volume or lack of plausibility, but also on relevant database hits or other available information from partner authorities, which includes information on previously conducted proceedings, possible indications of links with terrorist groups and other intelligence which is obtained mainly through national or international requests. Through its role as a central agency, the FIU is also in a position to establish links between the various types of information it receives and to bring together similar information submitted by different reporting entities, in order to process it according to an intelligence-led approach and transmit it to law enforcement agencies.

The assignment of STRs to key risk areas is carried out exclusively by the FIU after a corresponding assessment; there is no possibility for the reporting entities to mark them in advance, as is the case with topical reasons for suspicion. In its case-by-case analysis work, the FIU carries out an assessment of the facts in question, and this is therefore independent of the assessment of the reporting entity.

The FIU was able to identify individuals at a nationwide organisation who collected pooled donations for the organisation and then withdrew cash from the account to be used for unlawful purposes. Through law enforcement, the movement of funds could be reconstructed all the way to a war zone. In this case, the FIU disseminated a total of 58 STRs to law enforcement. The findings gained in this manner are the subject of several criminal proceedings as well as proceedings to ban an association.

Key Risk Area: Misuse of Money or Value Transfer Services

Money or Value Transfer Service
A money or value transfer service is a payment service under the German Payment Services Supervision Act (ZAG). This involves the transfer of funds without the need for an account-based relationship between the parties to the transaction or between these and the payment service provider. The transmission of funds (i.e. the financial transfer) is thus carried out without the use of accounts in the name of the payer or payee held by the service provider (payment accounts). For the provision of money transfer transactions, it is not important whether the sum of money is received in cash, by bank transfer or by offsetting. The receipt of the sum exclusively for forwarding to a third person or their representative is the decisive factor.

Risk Relevance of Money or Value Transfer Services

According to the NRA, the money or value transfer service is at increased risk, in particular due to the high frequency of cash, the payments outside of business relationships and regular foreign involvement. A particular emphasis is on transactions that involve so-called high-risk countries as the country of destination. Here, there may be the danger that sums of money will be paid out in conflict regions to be used for terrorist purposes. The simple structure and the high speed of business transactions render the danger of misuse more likely and increase the susceptibility to risk. The global availability makes it difficult to distinguish normal support payments from payments intended to be used for terrorist purposes. A case in point is the use of forged identity documents to transfer cash abroad. The fact that the agents are not obliged to collect further information – beyond identification – in line with the know-your-customer principle, and are therefore unable to provide information on the background of the payments or the economic circumstances of the payment service users, means that such information is usually only taken into account to a limited extent in the FIU analysis.

Know-your-customer (KYC)
"Know-your-customer" is a legitimation check of new and existing customers for the purposes of money laundering prevention which must be carried out as part of due diligence under the AMLA.

Misuse of Money or Value Transfer Services for Terrorist Purposes

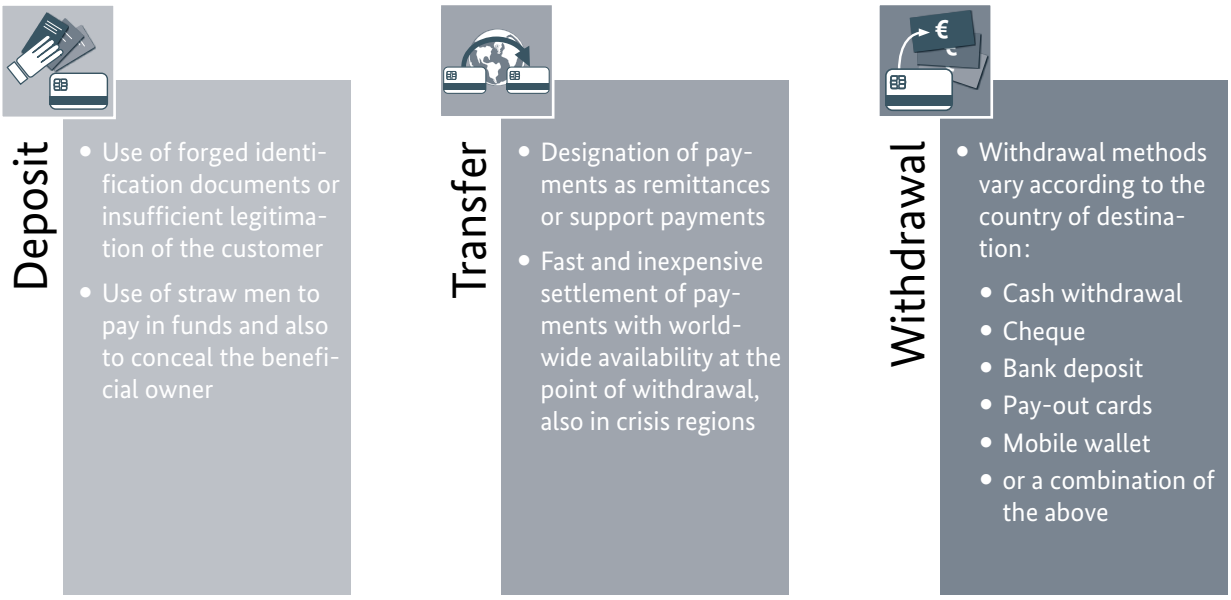


Figure 38: Money or Value Transfer Services

The following case study illustrates the points of contact between the money and value transfer services and all three characteristics of terrorist financing.

Case Study – Money or Value Transfer Services [35]

A suspicious transaction report received by the FIU showed a total of four same-day transactions to two different recipients, which were subsequently withdrawn in the (war) region on the border with Syria. The transfer reference included an allusion to "family assistance", whereupon the reporting entity contacted the customer by telephone, as it wondered about the alleged family relations of the originator of the payment. The customer stated that he did not know the recipients of the money himself, but acted as a "messenger" for the originators of the payments, as, lacking own identification documents, they were unable to initiate transactions themselves.

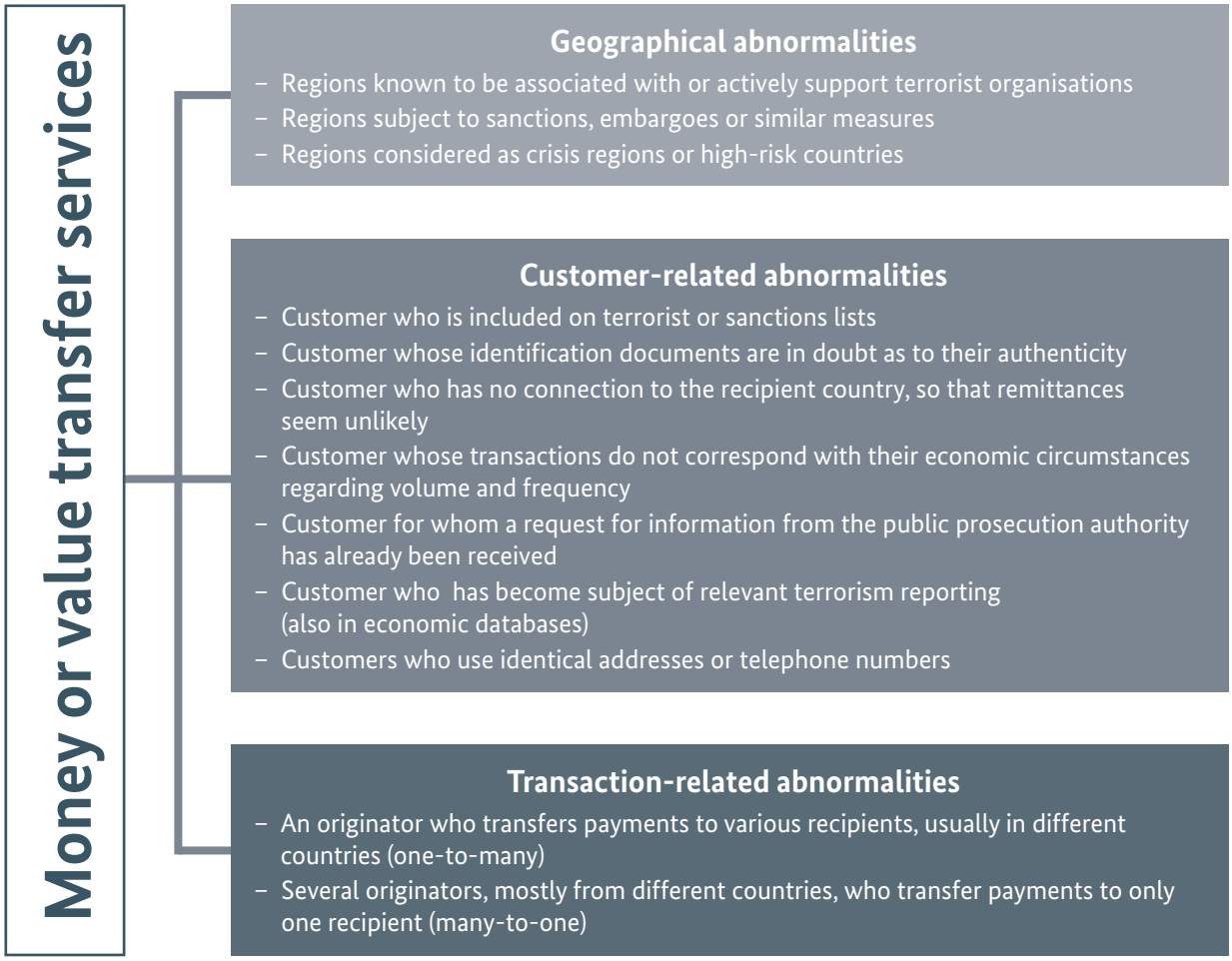
35 The present case study is a real case from the FIU's practice.

Total Number of STRs for Reporting Year 2019

The money or value transfer services in Germany is mainly occupied by three large foreign payment service providers. After credit institutions, these are the second largest group of reporting entities in terms of the total number of STRs to the FIU. In 2019, this group of reporting entities submitted a total of 7,528 STRs to the FIU. A total of 145 STRs were assigned to the key risk area "Misuse of Money or Value Transfer Services".[36]

An overall analysis of the reporting behaviour of the reporting entities shows that the STRs submitted can be divided into three different categories according to the reason for suspicion: geographical, customer-related and transaction-related abnormalities.

STRs were submitted to the FIU during the reporting year primarily against the background of payments made to crisis regions. These concerned outgoing payments from Germany. In addition, STRs were submitted on the basis of customer-related abnormalities, i.e. abnormalities justified in the person of the payment originator. In most cases, facts were reported in which the frequency or amount of the transactions carried out was conspicuous, as no family or economic background was evident to the reporting entity which could have been considered a plausible reason for



36 Only STRs received after the key risk area was introduced on 16 July 2019 are considered.

carrying out the transactions. The vast majority of the payments reported as abnormal were made to high-risk countries or crisis regions; the FIU has no information on the further movement of the funds after they were withdrawn at an agent based there.

The subsequent FIU analysis revealed the use of numerous forged identity documents, the authenticity of which is not checked during the identification process, in contrast to opening a bank account. It also became apparent that, due to the intrinsic risk associated with segmentation of business and the resulting divergent data quality, there are regularly cases of multiple registrations of persons in the databases of financial transfer service providers.

Among the transactions reported as relevant to terrorist financing, there were only a few cases where, upon closer examination, the FIU found evidence that they were actually related to terrorist financing. Transferring funds via the money or value transfer service is usually cheaper and quicker – in the context of remittances – than using the formal banking system; thus, this payment method can also be chosen for legitimate economic reasons without the intention of using it for terrorist purposes. However, the simple structure and the high speed of business transactions always entail risks with regard to terrorist financing and are attractive to persons with a terrorist background. For this reason, monitoring the money or value transfer service is a relevant instrument in the fight against terrorist financing, despite the rather low proportion of detected indications of misuse.

In about half of all cases where the FIU was able to identify indications of connections with terrorist financing or events relevant to state security, an Islamist involvement was found. Other reasons for dissemination were, for example, indications of xenophobic extremism, right-wing extremism or other criminal offences. In addition, regarding some STRs from financial service institutions, the FIU had received information that investigations and criminal proceedings were already pending, for example due to terrorist financing.

Information Exchange in the Area of Terrorist Financing and State Security

There is an ongoing exchange of information regarding the prevention of terrorist financing, in particular between the FIU's department specialising in terrorist financing and the Federal Office for the Protection of the Constitution (BfV), the Federal Intelligence Service (BND) and the Military Counter-Intelligence Service (MAD). The FIU also collaborates closely with the state security departments of the federal police authorities and those of the Länder. In this connection, the FIU received numerous national requests, mainly in the context of investigations, preliminary investigations or in situations of immanent risk. In 2019, the FIU received a total of 290 national requests related to terrorist financing or state security.

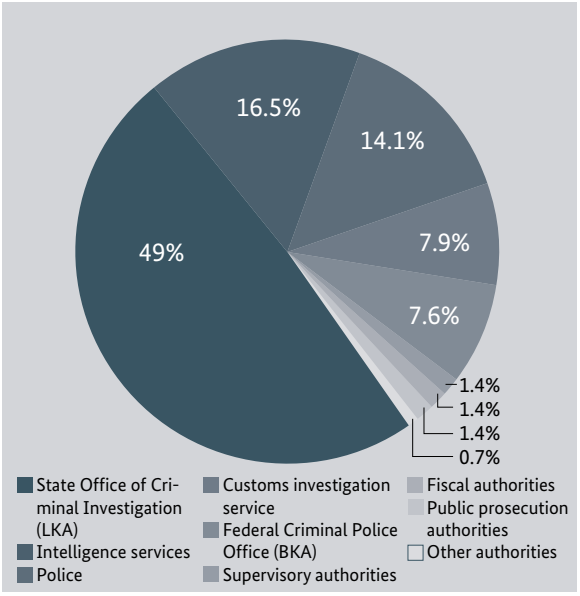


Figure 39: Breakdown of Domestic Requests Related to Terrorist Financing or State Security by Sender

While only a very small proportion of all incoming national requests received by the FIU were submitted by intelligence services, they account for the second largest share of requests related to terrorist financing or state security (almost 17 %).

The FIU maintains a continuous and trust-based exchange of information with the national state security services and national intelligence services at various levels. Various exchange formats were established, such as a "round table", as well as mutual work shadowing placements. In 2019, the FIU hosted the first FIU federal and Länder state security conference, which served to introduce the working methods and promote a common understanding of the risks involved in terrorist financing or state security matters. In addition to exchange formats designed to promote the identification of development trends, regular meetings are held at the working level to discuss specific events.

Alongside its national cooperation in the area of terrorist financing, the FIU also regularly exchanges information with partner FIUs from other countries. In this context, the FIU received regular requests and spontaneous information from its foreign partner authorities. In the reporting year, the FIU received and analysed a total of 221 international requests (97) and instances of spontaneous information (124) from abroad. These were sent to the FIU by 16 EU Member States and 20 other countries.

The FIU also sent a total of 60 requests and 13 pieces of spontaneous information related to the prevention of terrorist financing to foreign FIUs worldwide. In this context, information was sent to 15 EU Member States and eight other countries. As n the previous year, cooperation was particularly strong with Luxembourg, the USA and France.

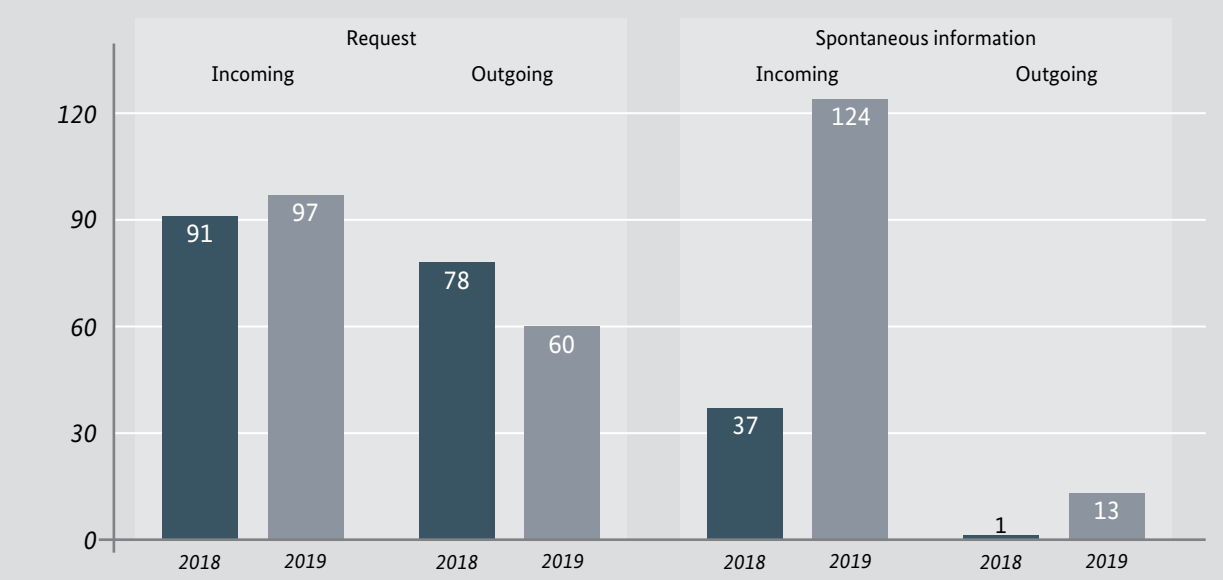


Figure 40: Cross-border Exchange of Information Related to Terrorist Financing or State Security

Country	Incoming international requests
France	30
USA	9
Belgium	7
Luxembourg	6
The Netherlands	4
Tajikistan	3
Cyprus	3
Finland	3
Italy	3
Other FIUs	29
Total	**97**

Country	Outgoing international requests
Luxembourg	24
The Netherlands	5
Belgium	4
Austria	4
France	3
Turkey	3
Great Britain	3
USA	2
Italy	2
Other FIUs	10
Total	**60**

Country	Incoming spontaneous information
Luxembourg	53
USA	51
Great Britain	6
Argentina	3
The Netherlands	2
Other FIUs	9
Total	**124**

Country	Outgoing spontaneous information
France	3
Turkey	2
Other FIUs	8
Total	**13**

Table 4 a-d: Number of Incoming and Outgoing Spontaneous Information and International Requests Concerning Terrorist Financing by Country

Case Study – State Security[37]

Initial STR

Via an investigation team created for this purpose, the competent LKA sent requests to the FIU to clarify the facts of the case. These requests aimed to obtain information available at the FIU regarding accounts held in Germany by the persons under suspicion.

FIU Analysis and Dissemination

An account access procedure carried out as part of the operational analysis was answered by the Federal Central Tax Office (BZSt) within about 50 minutes. The result was then immediately communicated to the investigating LKA. In the following, more in-depth analysis, two requests for information were made to domestic banks, as well as a request to an FIU located in an EU Member State, as relevant links were identified via a consolidation of accounts.
The relevant information was disseminated to the competent authorities within a few days so that it could be taken into account in the ongoing investigations.

37 The present case study is a real case from the FIU's practice.

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Explanation
AFCA	Anti Financial Crime Alliance
AMLA	Anti-Money Laundering Act, act on tracing profits from serious criminal activities (Geldwäschegesetz, GwG) in the version dated 23 June 2017, as last amended by Article 1 of this Act on 12 December 2019.
AO	German Tax Code, valid in the version dated 1 October 2002, as last amended by Article 1 of this Act on 21 December 2019.
BaFin	Federal Financial Supervisory Authority
BfV	Federal Office for the Protection of the Constitution
BKA	Federal Criminal Police Office
BND	Federal Intelligence Service
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FIU LOs	FIU liaison officers
FKS	Financial Control of Illicit Employment
GZD	Central Customs Authority
IEWG	Information Exchange Working Group
KYC	Know-your-customer
LfV	State Office for the Protection of the Constitution
LKA/LKAs	State Office(s) of Criminal Investigation
MAD	Military Counter-Intelligence Service
MdB	Member of the German Federal Parliament
MSCWG	Membership, Support and Compliance Working Group
NGO	Non-governmental organisation
NPO	Nonprofit organisation
NRA	National Risk Analysis
PPP	Public-private partnership
STR	Suspicious transaction report

LEGAL NOTICE:

Published by:
Central Customs Authority
Financial Intelligence Unit (FIU)
P.O. Box 85 05 55
D-51030 Cologne

Edited by:
Central Customs Authority

Design and creation:
Central Customs Authority, Training and Science Centre of the Federal Revenue Administration

Registration number:
90 SAB 272

www.zoll.de

Cologne, June 2020

www.fiu.bund.de