



Financial
Intelligence Unit



Annual Report 2018

Financial Intelligence Unit

Annual Report 2018

Financial Intelligence Unit

Table of Contents

Preface	7
Overview of the FIU	9
Suspicious Transaction Reports (STRs)	11
Reporting Volume in the Reporting Year 2018	13
Total Number of STRs, Differentiated According to Groups of Reporting Entities	14
Result of the Assessment of the Suspicious Transaction Reports of 2018	17
Receipt of Procedural Documents from Public Prosecution Authorities	18
Temporary Freezing Orders	20
Transactions	20
Typologies and Trends	23
Sector-specific Findings	24
Real Estate	24
Trade in Valuable Goods	29
Risks to the Fight against Money Laundering and Terrorist Financing as a Result of New Technologies	33
FinTechs	34
Virtual Currencies	35
National Cooperation	37
Cooperation with Law Enforcement Agencies	39
Cooperation with Supervisory Authorities	39
Requests from Domestic Authorities	40
Cooperation with Reporting Entities	41
International Cooperation	43
Information Exchange with other FIUs	44
International Committee Work	47

Financing of Terrorism and other Crimes relevant to State Security	49
Total Number of STRs with Reference to Terrorist Financing or State Security	50
Dealing with STRs relating to Terrorist Financing or State Security	50
Strategic Evaluations of the Phenomenon of Terrorist Financing and State Security	51
Temporary Freezing Orders	54
Information Exchange in the Sector of Counter Terrorist Financing	55
Proliferation Financing	56
List of Figures	57
List of Tables	58
List of Abbreviations	59

**Dear Readers,**

Combatting money laundering and terrorist financing is gaining a cross-border, international significance in the context of the liberalisation and globalisation of the financial markets. High-volume proceeds from illegal activities are laundered world-wide and integrated in the legitimate economy. Therefore, the aim must be to prevent money laundering on the basis of international standards. The reorganisation of the Financial Intelligence Unit (FIU) in 2017 served this aim.

In 2018 the FIU continued its activities under the umbrella of the Customs Directorate General. During this time, the trend of a sharp increase in incoming suspicious transaction reports (STRs) continued with more than 77,000 STRs, which emphasises the relevance of the FIU's filter function. Once again, STRs from the non-financial sector were received only in low numbers, even with respect to highly-relevant issues, such as money laundering in the real estate sector. Nevertheless, valuable findings could be gained in this sector with the help of numerous STRs from the financial sector. To be able to identify trends at an early stage, for example with regard to virtual

currencies, the information received by the FIU is regularly subjected to evaluations independent of individual cases.

An important prerequisite for coping with large numbers of incoming STRs was established by successfully introducing an electronic reporting platform on 1 February 2018 for the first time. Furthermore, a strong increase of personnel and a further technical strengthening through consistent implementation of a multi-disciplinary approach for staff recruitment could be achieved in the course of the year. In future the FIU will also use modern, intelligent analysis tools ("artificial intelligence") to satisfy these quantitative and qualitative challenges. High priority was also given to the further optimisation and intensification of the cooperation with national and international partners.

The significance of the FIU is demonstrated in particular in the competence for systematic, strategic analysis of the total number of STRs and the findings gained on this basis, which are to serve all public and private agencies involved in the combatting of money laundering, for professional information. I may therefore direct special attention to the section "Typologies and Trends". Thus, I look optimistically into the future characterised by growth and challenges and wish you exciting reading of the Annual Report 2018.

Christof Schulte
Head of the FIU

Overview of the FIU

Overview of the FIU

The FIU, established as an independent, administrative central agency under the umbrella of the Customs Directorate General, is responsible for the receipt, collection and analysis of STRs which could be related to money laundering or terrorist financing.

As a real central agency, the FIU receives all STRs provided nationwide by reporting entities, directs these to a comprehensive analysis and evaluation and is therefore commensurate with international requirements, in particular as set out by the Financial Action Task Force (FATF). If this then yields suspicious facts about money laundering or terrorist financing, exclusively those STRs assessed as relevant are passed on to the law enforcement agencies (LEAs) and other responsible authorities (“filter function”). Since its reorganisation on 26 June 2017, the FIU sees itself as a central information hub which is upstream of criminal investigations and clearly separated from these. As an administrative authority, the FIU is not subject to the principle of legality, unlike LEAs. This constitutes an important prerequisite to be able to effectively exercise the newly gained “filter function”.

In addition to the evaluation of the STRs, the FIU is in constant contact with the reporting entities and the competent authorities at national level. With its central coordination function vis-à-vis the supervisory authorities of the Länder, the FIU is able to manage risk-based information and thus to support supervisory activities, particularly in the non-financial sector. Internationally, the FIU exchanges information and cooperates with the FIUs of other countries. By conducting a strategic analysis independent of individual cases, the FIU can identify new methods and trends in the area of

money laundering and terrorist financing, inform reporting entities and the competent authorities accordingly, and support the operational analysis of STRs which is based on a risk-based approach.

The FIU is a functional authority which is organizationally integrated into the Directorate General of Customs and which is technically independent within its tasks and powers. It is divided into two units (D.1 and D.2). On 1 October 2018, the new department “Risk Management / Compliance” was established with a direct reporting line to the head of the FIU. The working areas of Unit D.1 are responsible for general and cross-sectional affairs. The personnel focus of the FIU is on Unit D.2 (Operational Analysis), in which the electronically transmitted STRs are received, enriched, analysed and evaluated centrally. An adjustment of the existing structure will probably take place in 2019 as part of the further personnel reinforcement of the FIU.

Further technical information and the latest news can be found on the FIU’s website at www.fiu.bund.de.

Suspicious Transaction Reports (STRs)

Reporting Volume in the Reporting Year 2018

Total Number of STRs, Differentiated According to Groups of Reporting Entities

Result of the Assessment of the Suspicious Transaction Reports of 2018

Receipt of Procedural Documents from Public Prosecution Authorities

Temporary Freezing Orders

Transactions

Suspicious Transaction Reports (STRs)

The following chapter provides a detailed analysis of the STRs received by the FIU in 2018. All reports pursuant to Sections 43, 44 AMLA¹ and Section 31 b AO² submitted to the FIU are considered.³

Figure 1 first gives an overview of what happens to an STR after it has been received electronically by the FIU. For this purpose, the procedure of the operational analysis is presented in its individual steps.

From the Receipt of a STR to the Monitoring or Dissemination Decision

Once the FIU has received the electronic STR, it runs through an automated basic search, in the course of which the data created in the STR are compared with other databases. Hits generated in this way indicate, for example, whether a reported person has already appeared in connection with certain criminal offences. In the course of an initial evaluation, STRs are categorized in order to prioritize the processing of particularly urgent cases and to ensure that the STRs are directed to the FIU’s various working areas quickly and topic-related. After the information from different sources has been brought together and analysed, an assessment is made as to whether, from the FIU’s point of view, it can be established that an asset is related to money laundering, terrorist financing or other criminal offences, so that an analysis report can be handed over to the competent authority. Otherwise, the report remains for further observation in the so-called “monitoring” of the FIU’s central database until the facts can be enriched with new findings, as appropriate.

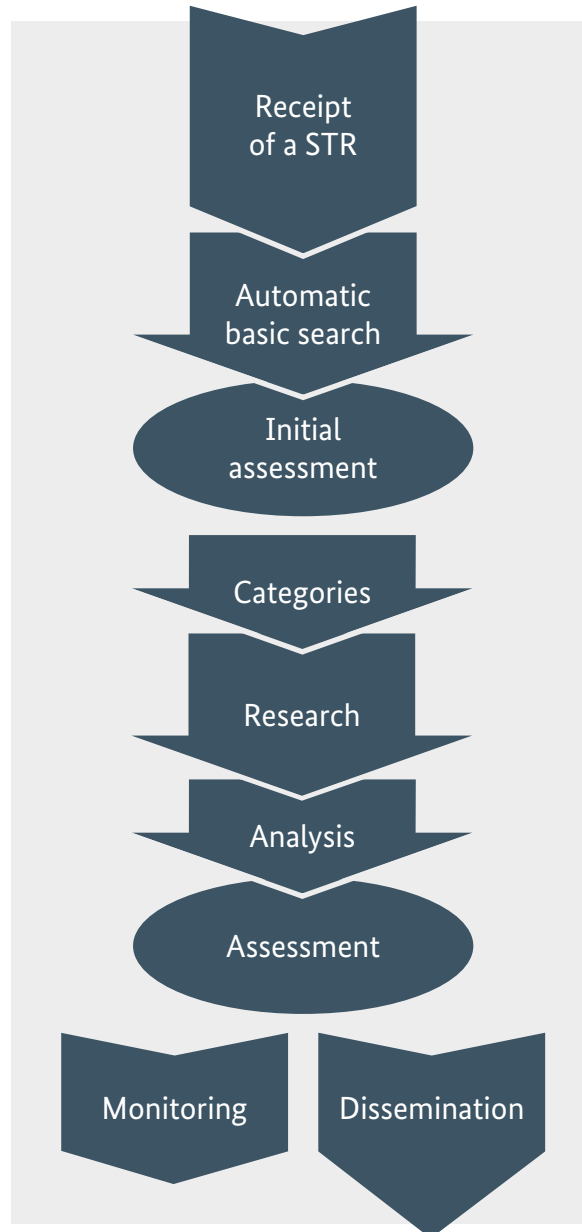


Figure 1 – Process Sequence of the Operational Analysis of STRs

1 Money Laundering Act (AMLA) of 23 June 2017.

2 Tax Code (AO) in the version of 1 October 2002; the receipt of STRs pursuant to Section 31b AO by the FIU is regulated in Section 30 AMLA.

3 All STRs and notifications are therefore listed, which are within the scope of Section 30 (1) No. 1-2 AMLA. Information submitted to the FIU pursuant to Section 30 (1) No. 3-4 AMLA are not considered as STRs from reporting entities for this purpose.

Reporting Volume in the Reporting Year 2018

The sharp increase in the number of STRs in recent years continues in 2018. With a total of 77,252 STRs received by the FIU in 2018, an increase of 29% can be observed compared to the previous year. In absolute terms, this is the strongest increase within one year with a total of about 17,500 STRs. Since 2008, the annual reporting volume in Germany has thus increased elevenfold, reflecting a trend towards ever-increasing awareness and automation among large banks and financial service providers.

Already in 2017, the increasing total number of STRs posed a major challenge for the FIU and the LEAs. The further increase in the number of STRs thus underlines the relevance of the FIU's filter function, leading to the dissemination of only valuable cases to the LEAs and other competent authorities. From the FIU's point of view, the

increase in the number of STRs shows that the regulatory goal of the Act on the Implementation of the 4th EU Anti-Money Laundering Directive, the implementation of the EU Money Transfer Regulation and the reorganisation of the FIU has been achieved.

As a result of the reorganisation of the FIU and the associated legal change from the obligation to file a criminal complaint to the obligation to submit a STR (under trade law), the threshold for reporting suspicious transactions has fallen significantly. Every STR represents an essential element for the FIU and in the overall view is an important source of information for the FIU as an intelligence authority. In this context, it is the task of the FIU to further raise awareness of the reporting entities with regard to the submission of relevant STRs.

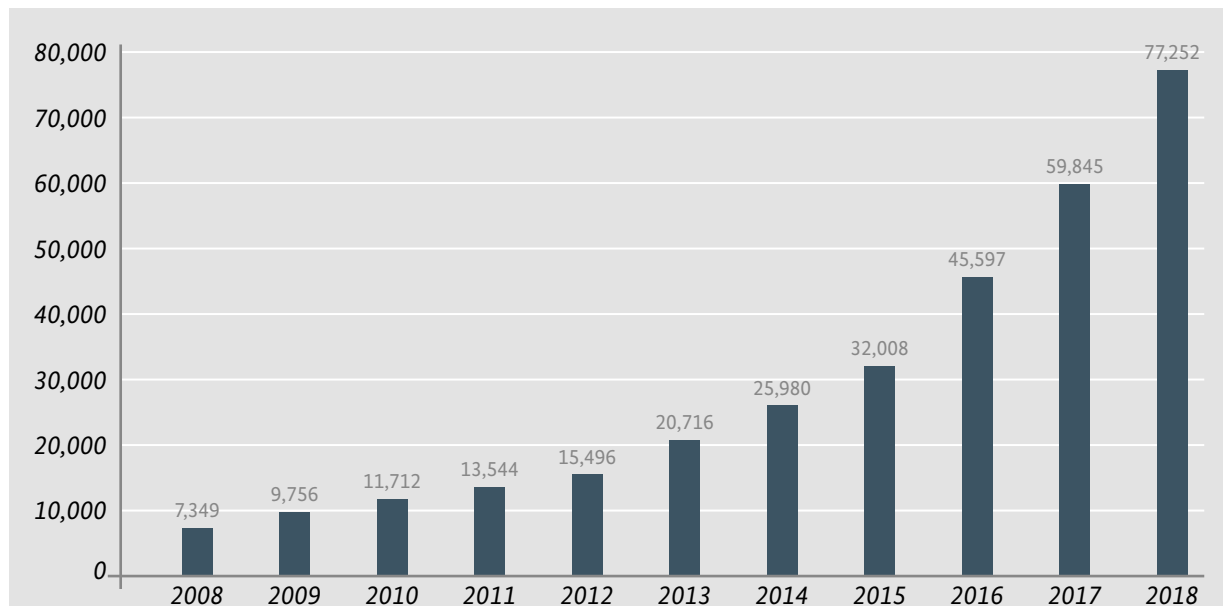


Figure 2 – Development of the Number of STRs under the AMLA (2008 - 2018)

Total Number of STRs, Differentiated According to Groups of Reporting Entities

The following table shows that the distribution of STRs among the respective subgroups of reporting entities has not changed significantly in 2018 either. Furthermore, over 98% of the STRs received

came from the financial sector, with credit institutions being the group with the highest number of those reports, accounting for 84% of all STRs.

	Reporting entities	2018	Comparison with last year
Financial sector	Credit institutions	65,132	↗
	Financial services institutions	10,552	↗
	Payment institutions and electronic money institutions	264	↗
	Agents	35	↗
	Independent business persons	0	→
	Insurance undertakings	137	↗
	Asset management companies	17	↗
	Total STRs financial sector	76,137	↗
Non-financial sector	Financial companies	7	–
	Insurance intermediaries	4	→
	Lawyers	22	→
	Legal advisors who are members of a bar association	0	→
	Patent attorneys	0	→
	Notaries	8	→
	Legal advisors	0	→
	Auditors and chartered accountants	2	→
	Tax advisors and authorised tax agents	4	→
	Trustees, service providers for trust companies	1	→
	Estate agents	31	↗
	Organisers and brokers of games of chance	150	↗
	Traders in goods	368	↗
		Total STRs non-financial sector	597
Others	Supervisory authorities	54	–
	Fiscal authorities	414	↗
	Other STRs ⁴	50	–
	Total	77,252	

Table 1 – Number of STRs by Group of Reporting Entities⁵

⁴ The decrease in other STRs is due to the allocation of all STRs to the categories listed above in 2018, which could not be done in the previous year because of the conversion of the reporting and IT system and, in particular, the STRs received by fax.

⁵ A comparison with the previous year is not possible for reports by financial companies, supervisory authorities and other STRs. In the course of data cleansing measures, some reporting entities in the category of financial companies were assigned to other categories, so that the number of STRs in this category decreased significantly. Notifications by supervisory authorities pursuant to Section 44 AMLA were not explicitly listed in the previous year. In 2018, the other STRs only contained STRs in the category “other reporting entities”.

With around 10,000 STRs, financial services institutions are the second strongest reporting group. The sharp rise in the number of STRs from this sector is almost exclusively attributable to the high activity of established financial services institutions.

Compared to the previous year, the number of STRs received from the non-financial sector has increased. Overall, however, the number of STRs from this sector still accounts for only slightly less than 1% of total receipts. As in previous years, there was an increase in incoming registrations from traders in goods, especially car dealers, as well as from organisers and brokers of games of chance. Here, in addition to casino operators, gambling operators such as betting offices have also increasingly submitted STRs. The number of STRs from the liberal professions and the real estate sector increased slightly.

Despite an increase in the total number of STRs from the non-financial sector, the number of STRs nevertheless remains at a low level in absolute terms. The observation already made in previous years that the FIU does not receive a sufficient number of STRs from the non-financial sector is again underlined in this year. The FIU plays an important role in raising the awareness of reporting entities of the non-financial sector and will further develop its coordinating role for supervisors.

STRs from public authorities and other reporting entities also account for slightly less than 1% of the total reporting volume. For the first time, reports by supervisory authorities⁶ which are also obliged under Section 44 AMLA to report to the FIU, if they become aware of facts indicating that an asset may be connected with money laundering or terrorist financing, are listed separately here. Likewise, financial authorities submit notifications to the FIU in accordance with Section 31 b AO.

The FIU is working intensively with the reporting entities to improve the reporting of suspicions and to raise awareness among the obligors regarding registration for the use of the electronic reporting channel. As a result of the measures taken by the FIU, the number of registered obligors rose from 1,998 in 2017 to 3,104 in 2018, which means that the quota of registered obligors increased by 55% in the year under review.

While Table 1 breaks down the number of STRs received by category of reporting entities, Table 2 below shows the number of reporting entities who submitted a STR in 2018 (active reporting entities).

Looking at both tables, it can be seen that in 2018 reporting entities from the financial sector submitted an average of just under 56 STRs, whereas in the non-financial sector only about three STRs per actively reporting entity were submitted to the FIU. The evaluation of the absolute reporting figures shows that the most active reporting entity in the financial sector submitted around 15,000 STRs and the most active reporting entity in the non-financial sector submitted around 50 STRs.

One explanation for this is that credit institutions in particular have comparatively highly developed, established monitoring systems whose effectiveness is subject to central supervision by BaFin. In addition, the structural structure of a typical company in the non-financial sector differs significantly from that of a company in the financial sector. While the handling of large volumes of transactions is a core activity of credit institutions and financial services institutions, the majority of non-financial sector reporting entities are often relatively small enterprises.

The number of active reporting entities in the financial and non-financial sectors rose from 1,220 in 2017 to 1,591 in 2018. In 2018 there were

⁶ See also page 39 for further details on cooperation with supervisory authorities.

also 58 active authorities who have submitted a STR to the FIU. As a result, the number of active reporting entities increased by 30% in the reporting year. A comparison of the two years shows, however, that in 2017 about 61% of the reporting entities were active reporting entities, whereas in 2018 only about 51% of the registered reporting entities submitted a STR to the FIU. One reason for

this is that the registration of the reporting entities is also used to gain access to the internal area of the FIU website and to view the information published by the FIU (e.g. typology papers). Thus, the registration of a reporting entity does not necessarily mean that there must have been a suspicion of money laundering or terrorist financing.

	Reporting entities	2018	Comparison with last year
Financial sector	Credit institutions	1,232	↗
	Financial services institutions	53	↗
	Payment institutions and electronic money institutions	22	↗
	Agents	9	↗
	Independent business persons	0	→
	Insurance undertakings	41	↗
	Asset management companies	14	↗
	Total STRs financial sector	1,371	↗
Non-financial sector	Financial companies	4	↘
	Insurance intermediaries	2	→
	Lawyers	13	↗
	Legal advisors who are members of a bar association	0	→
	Patent attorneys	0	→
	Notaries	5	↘
	Legal advisors	0	→
	Auditors and chartered accountants	2	→
	Tax advisors and authorised tax agents	3	↗
	Trustees, service providers for trust companies	1	↗
	Estate agents	20	↗
	Organisers and brokers of games of chance	24	↗
	Traders in goods	146	↗
	Total STRs non-financial sector	220	↗
	Total	1,591	

Table 2 – Number of active Reporting Entities

Result of the Assessment of the Suspicious Transaction Reports of 2018

In 58% of the STRs finalised by the FIU in 2018, indications of links with money laundering, terrorist financing or other criminal offences were found, so that they were disseminated, for example, to the competent State Office of Criminal Investigation (LKA). The intra-European comparison with other administratively oriented FIUs shows that this is a relatively high rate. It should also be noted that a given case may contain several related STRs.

In total, 42% of all STRs did not meet the requirements for dissemination to the competent authorities. These STRs were transferred to the FIU's monitoring system. This means that they were entered into the FIU's central database in order to continuously compare them with information from new STRs and, if necessary, to complement them so that they can be disseminated at a later point in time.

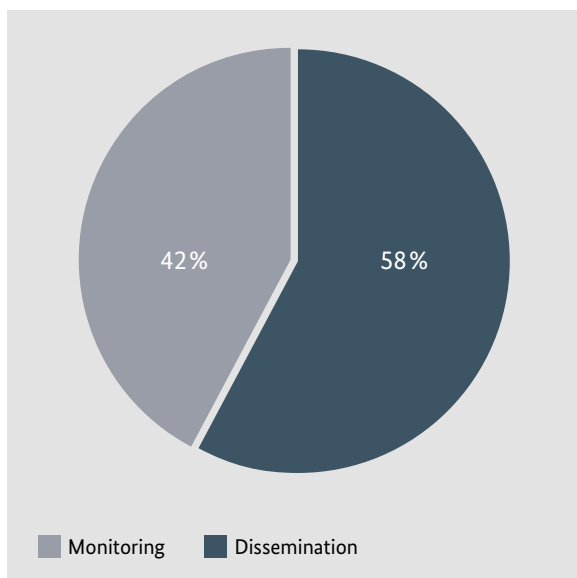


Figure 3 – Distribution of the STRs after Evaluation

The different recipients of the FIU's dissemination are shown in Figure 4.

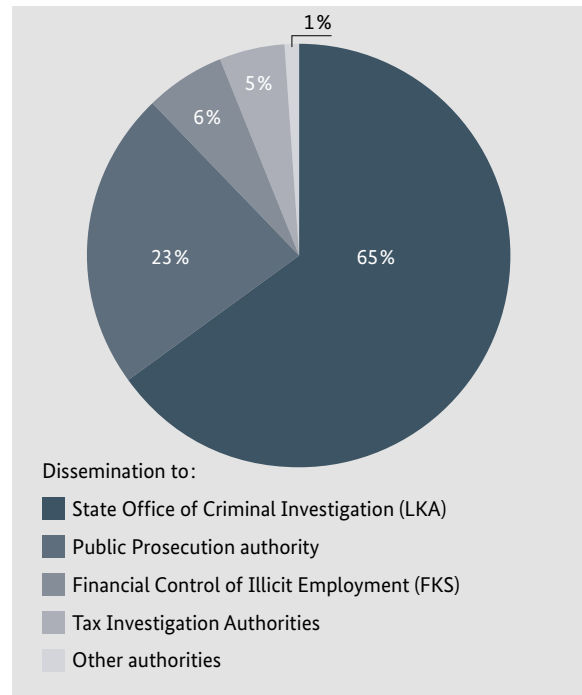


Figure 4 – Distribution of STRs according to Recipients

The most important recipients of the FIU's dissemination cases are the competent State Offices of Criminal Investigation (LKAs), which account for about two thirds of all cases. In two federal states, however, the cases are disseminated to the competent public prosecutor's office. Disseminations to the Financial Control of Illicit Employment (FKS) (6%) and to the Tax Investigation Office (5%) are also significant. These are carried out if the content of the assessed STRs contains only indications of illicit work and illegal employment or tax crimes. Other authorities to which the FIU disseminates cases are the intelligence services, the customs investigators and the federal police. However, these account for less than 1% of the total number of cases disseminated in 2018 respectively.

Receipt of Procedural Documents from Public Prosecution Authorities

In accordance with the provisions of the AMLA, the competent public prosecution authority notifies the FIU of the commencement of the public charges and the outcome of the proceedings, including all dismissal decisions, in respect of criminal proceedings in the context of which the FIU has for-warded information. This is done by sending a copy of the indictment, a penalty order, a dismissal decision or a criminal conviction (“feedback”).

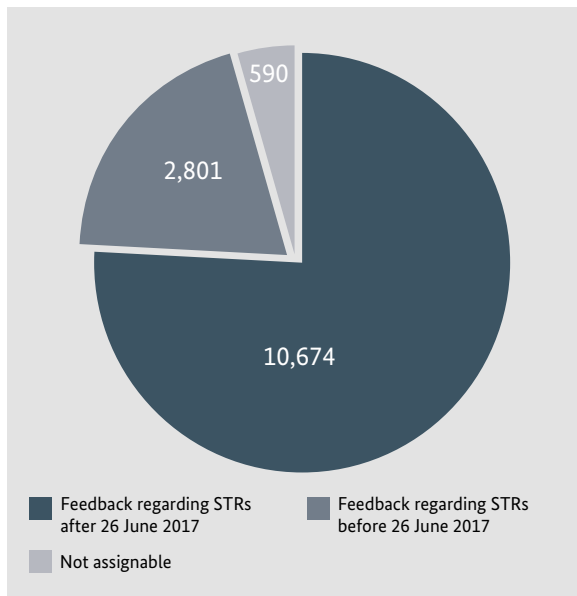


Figure 5 – Number of Feedbacks by Public Prosecution Authorities in 2018

In 2018, the FIU received a total of 14,065 feedbacks from the public prosecution authorities, of which 2,801 were received for STRs processed prior to the reorganisation of the FIU as of 26 June 2017. The significant decrease in the number of feedbacks compared to previous years is due to the fact, among other things, that since the reorganisation of the FIU, interrelated STRs have been pooled into a single case and are disseminated under a single case number. As a result, only one feedback per case number is to be expected regularly. This means that since 2018 a feedback can stand for several STRs and a direct comparison of the number of feedbacks with the previous years is not possible.

Furthermore, the filter function exercised since the reorganisation of the FIU ensures that not every STR received by the FIU triggers a procedure at a public prosecution authority, since irrelevant STRs remain in the FIU’s monitoring system.

A total of 275 of these feedbacks were feedbacks comprising convictions, penalty orders and indictments. As in the previous year, this corresponds to a share of approximately 2% of the feedbacks.

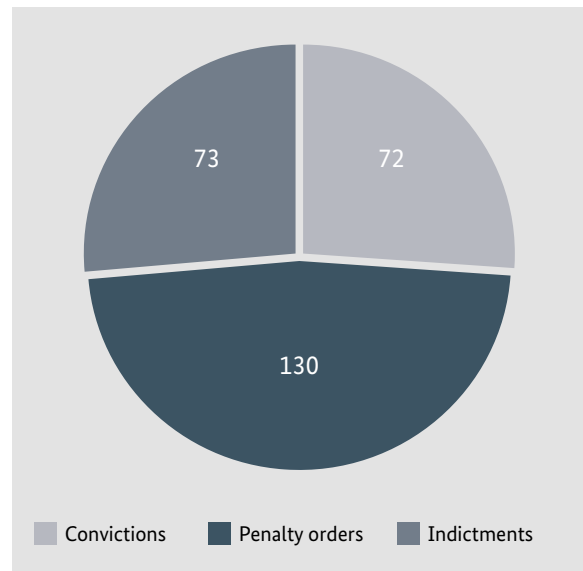


Figure 6 – Overview of the Convictions, Penalty Orders and Indictments

As in previous years, orders for withdrawal of prosecution continue to account for the majority of feedback by public prosecution authorities. Overall, however, it should be noted that the proportion of money laundering proceedings leading to a conviction or a penalty order is not sufficient to measure the effectiveness of the reporting system. Occasionally, orders for withdrawal of prosecution may state that the proceedings are to be discontinued solely for money laundering, but that they are to be further investigated separately for the predicate offence (e.g. fraud) or that the proceedings are to be separated. From the FIU’s point of view, one reason for this is, in particular, the difficulties in providing evidence with regard to the money laundering act itself. For a conviction for money

laundering according to Section 261 of the Criminal Code (StGB) not only the predicate offence but also the money laundering act, as well as a causal connection between predicate offence and money laundering must be proven. On the other hand, proof of money laundering often does not bring any “added value” in terms of criminal procedural law. In particular, in cases where the offender of the predicate offence is also the offender of the

money laundering, the money laundering offence is generally unpunished pursuant to Section 261 (9) sentence 2 StGB. In other cases as well, the sentence is often not significantly increased by the additional conviction for money laundering. Thus, a discontinued money laundering case does not necessarily mean that the underlying STRs are to be regarded as ineffective.

Case 1 – From the STR to the Conviction⁷

Initial STR

Mr. A receives a bank transfer of € 10,000 from a non-EU country and subsequently disposes of these in cash. The bank keeping the account reports this to the FIU.

Analysis by the FIU and dissemination

In the FIU's analyses a link can be established with other accounts held by Mr A with other banks which have recently been the subject of STRs due to unusual payments from the same country. An incoming report from the police establishes a link to another person with a similar profile, Mr B. The available information provides evidence that Mr A and Mr B are acting illegally as so-called “financial agents”.

Since sufficient relevant information can be gathered, an analysis report based on four STRs is sent to the competent State Office of Criminal Investigation (LKA).

Investigations and Conviction

In the subsequent investigations, it emerges that Messrs A and B support an international criminal organization by opening target accounts for incoming funds from computer fraud. Investigations are started against other persons who are active in the network.

Mr. A and Mr. B are each sentenced to almost two years suspended prison for deliberate money laundering in coincidence with the formation of a criminal organisation.

⁷ The described case study is a real case from FIU practice.

Temporary Freezing Orders

Pursuant to Section 40 AMLA, the FIU may prohibit the execution of a transaction if there are indications that a transaction is connected with money laundering or counter terrorist financing (CFT). This so-called “temporary freezing order” gives the FIU the opportunity to investigate the evidence and analyse the transaction without withdrawing incriminating funds from the state’s sphere of influence through cash withdrawals or transfers, until a final evaluation of the facts has been made.

The temporary freezing order is an important and effective instrument of the FIU to combat money laundering, whereby the need to implement a temporary freezing order is weighed up carefully on a case-by-case basis.

Transactions

Suspicious transactions are an important part of most STRs received by the FIU. Transactions are transfers of assets between two parties, often using a third party. Examples of transactions are bank transfers, cash withdrawals from current accounts, cash transactions of any kind, but also the re-deeming of chips in casinos.

Around 315,000 suspicious transactions were reported to the FIU in 2018.¹⁰ A STR does not necessarily have to contain a transaction, but a single STR can also contain a large number of transactions.

In 2018, the FIU adopted a total of eighteen temporary freezing orders related to money laundering and terrorist financing. Transactions with a total volume of approximately € 504,500,000 were stopped for up to 30 days.⁸ In eight of these cases, a foreign request from another FIU was the trigger for implementing the temporary freezing order.⁹ For the remaining ten temporary freezing orders, the further analysis of eight measures revealed concrete facts which led to a dissemination of the facts to the competent authority.

Therefore, the number of transactions is not directly comparable to the number of STRs received. About a quarter of the reported transactions are intra-German transactions. In about 20% of the transactions, no information on the country of origin or country of destination is available. All other transactions are related to foreign countries, whereby transactions from and to Germany are particularly relevant for a national analysis. The following graphs show the intensity of reported transactions in which Germany was affected either as the country of origin or destination.

⁸ The largest part of the total amount is attributable to a temporary freezing order with an unusually high volume.

⁹ See page 44 for more information.

¹⁰ After the preparation date of the annual report, this number may increase if suspicious transactions involving transactions carried out in 2018 are reported later in 2019.

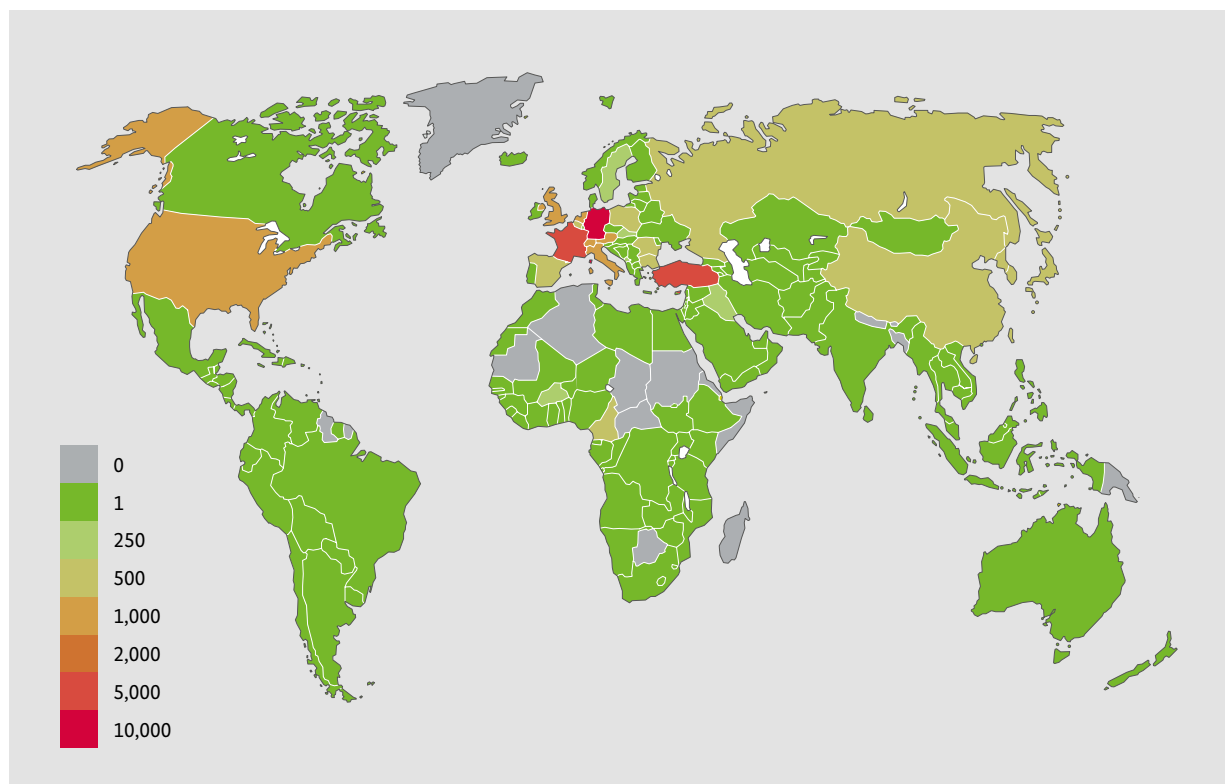


Figure 7 – Number of Suspicious Transactions According to Country of Origin

Looking at the countries of origin (cf. Figure 7), it can be seen that European countries, the USA and the large Asian countries are the focus areas. France and Turkey stand out as countries of origin for around 3,400 and 2,400 transactions respectively. The USA is the only non-European country from which more than 1,000 suspicious

transactions reached Germany. Taking into account the geographical proximity to Germany, the economic strength of the respective states and the proportion of people living in Germany with roots in their country of origin, the distribution of transactions seems plausible.

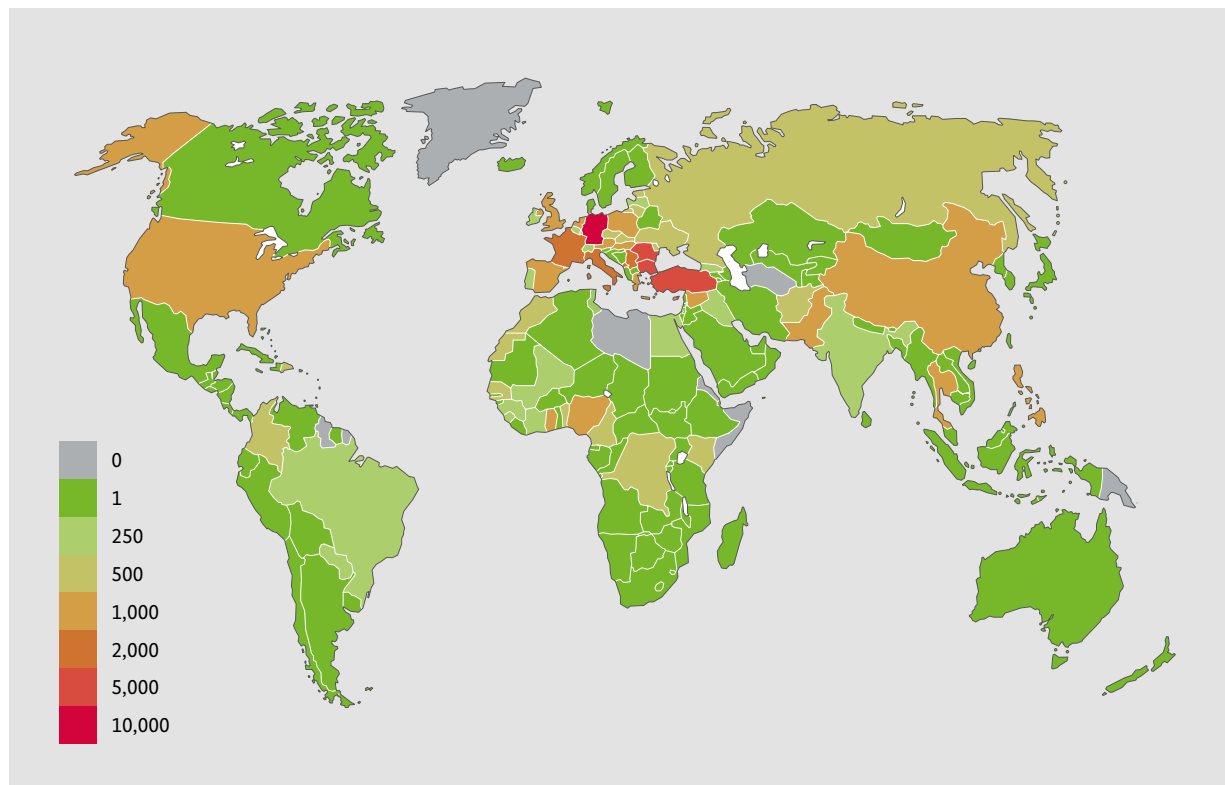


Figure 8 – Number of Suspicious Transactions according to Country of Destination

The transactions originating from Germany show a different picture (cf. Figure 8). On the one hand, there is an overall higher number of outgoing transactions than of incoming transactions reported to Germany (113,000 compared to 31,000). On the other hand, differences can be seen in the regional distribution. Nevertheless, the European countries also dominate here. Besides Turkey (27,000) and France (24,000), Bulgaria (9,800), Romania (8,000) and Kosovo (4,100) have the highest transaction figures. Overall, the high number of suspicious transactions in Eastern European countries does not seem to be fully explainable by geographical, economic or demographic circumstances. In addition, there are a larger number of non-European countries that have been the destination countries for more than 1,000 transactions originating in Germany. These include Ghana and Nigeria in Africa; Pakistan, China, Thailand and the Philippines in Asia; Syria and Lebanon in the Middle East; and the United States.

Suspicious transactions not directly related to Germany are often correspondent banking transactions involving German banks. An exception is the high number of reported transactions stating France as both the country of origin and the country of destination, but which were settled via a German account. Here an accumulation of fraudulently opened accounts with German Internet banks can be observed, where identification of the account holder is possible without physical presence, e.g. via a Video-Ident procedure.

Typologies and Trends

Sector-specific Findings

Real Estate

Trade in Valuable Goods

Risks to the Fight against Money Laundering and Terrorist Financing
as a Result of New Technologies

FinTechs

Virtual Currencies

Typologies and Trends

Sector-specific Findings

Real Estate

The real estate sector is a sector with high risk for money laundering activities. One reason for this is that real estate is a very high-priced, value-stable commodity and therefore very large amounts of money can be moved in individual transactions without attracting much attention. At the same time, there are opportunities to limit the transparency of the origin of funds and ownership.¹¹ For example, financing models involving offshore locations can make it more difficult to trace the origin of funds. Due to a multitude of legal options for domestic and foreign legal entities, which permit the use of complex ownership structures, ownership relationships can also be difficult to understand in certain cases. A money laundering risk is also seen in this area in the international context.¹² For example, the acquisition of luxury real estate by shell companies is seen as an attractive way to launder money anonymously. This is particularly true in the case of direct payment of the purchase price without financing, where no services have to be provided by credit institutions and the probability of triggering a STR is thus significantly reduced.¹³

A **shell company** is a properly registered company that has a postal address (a letter-box) but no regular business activity. Several shell companies often share one postal address and it is not uncommon for one person to preside over a number of shell companies, but merely provides their name and does not make any business decisions.

In many ways, real estate is a special commodity. They are large-volume, durable, location-bound and can only be substituted to a limited extent. With gross fixed assets of around € 13.9 trillion (80.3% of total gross fixed assets) in 2016, real estate is the most important asset class in Germany,¹⁴ according to an expert opinion by the German Association for Housing, Town Planning and Regional Planning (Deutscher Verband für Wohnungswesen, Städtebau und Raumordnung e.V.). For the same year, a gross value added of € 302.9 billion is attributed to the real estate industry,¹⁵ which corresponds to 10.9% of the total economy of the Federal Republic of Germany.¹⁶ Due to the economic and social importance of the real estate sector and the high risk of money laundering activities, special attention is paid to STRs from this sector.

11 Cf. BKA 2012 (Federal Criminal Police Office), Special study - Money laundering in the real estate sector in Germany.

12 See FATF 2008, RBA Guidance for Estate Agents.

13 FinCEN Advisory 2017, Advisory to Financial Institutions and Real Estate Firms and Professionals, FIN-2017-A003

14 See Economic Factor Real Estate 2017, Just, Voigtländer et. al., Expert Opinion for the German Association for Housing, Urban Development and Regional Planning and the Society for Research in the Real Estate Sector, Scientific Editing by the Institute of the German Economy Cologne and the International Real Estate Business School, University of Regensburg.

15 Real estate management in the narrower sense (real estate trading, letting, leasing, brokerage, administration).

16 Cf. economic factor real estate 2017 (see above).

In 2018, the FIU received 31 STRs directly from estate agents. In addition to these, however, other entities obliged under the AMLA also have insights into real estate transactions. For example, in 2018 the FIU received more than 750 STRs explicitly stating that the reason for reporting were “unusual activities in connection with the purchase or sale of real estate”. A total of around 3,800 STRs could be linked to the real estate sector, which accounts for almost 5% of the total reporting volume. The vast majority of these STRs were submitted by credit institutions, with tax authorities representing the second largest group of reporting entities. Very small numbers of STRs relating to the real estate sector were received from notaries, lawyers and asset management companies.

A frequently cited reason for submitting STRs to the FIU is the settlement of real estate transactions with cash. Cash deposits and payments are usually justified by customers with real estate sales or purchases abroad. In such cases, the origin or use of the funds often cannot be traced or can only be traced with considerable effort.

Another risk factor in connection with real estate transactions as a vehicle for money laundering is the overvaluation or undervaluation of real estate. Here, too, there are numerous STRs from reporting entities describing transactions in which inexplicable changes in the value of the same property were detected. This is particularly frequently reported in connection with the rapid resale of properties and constellations in which buyers and sellers are directly or indirectly connected to each other.

The involvement of foreign companies, where the ownership structure is often more difficult to understand, is also frequently reported in connection with real estate transactions. Especially when offshore companies are involved in transactions, credit institutions submit STRs because the beneficial owners often cannot be identified.

The evidence available to the FIU underlines the need to get more STRs from entities of the non-financial sector involved in real estate transactions. In 2018, the FIU prepared a special reference and typology paper for the real estate sector in order to support reporting entities in submitting STRs in connection with the purchase or sale of real estate, which is addressed to the various relevant reporting entities for this sector.

Case 2 – Conspicuous Sale of Real Estate¹⁷

Initial STR

As the managing director of company A, Mr V acquired a property for € 250,000. Two years later, he informed his bank about the sale of the property. The sale and transfer agreement had already been notarised, so that Mr V announced the payment of the purchase price of € 750,000 by buyer K. However, the sale was cancelled at short notice. The following year the property was sold to Company B for € 1.9 million.

FIU Analysis and Dissemination

Shareholder of both Company A and Company B is Company C. Mr V, is also the managing director of Company C. The use of different credit institutions on the buyer and seller side made it difficult to identify the business connections. Connections to a further STR on the parties involved could be established.

The implausible increase in value of the property and the conspicuous corporate structures provide sufficient indications for dissemination to the competent authority. In addition, there are further indications from the second STR concerning the parties involved, including undetermined sources of funds from abroad. The case was disseminated to the competent State Office of Criminal Investigation (LKA).

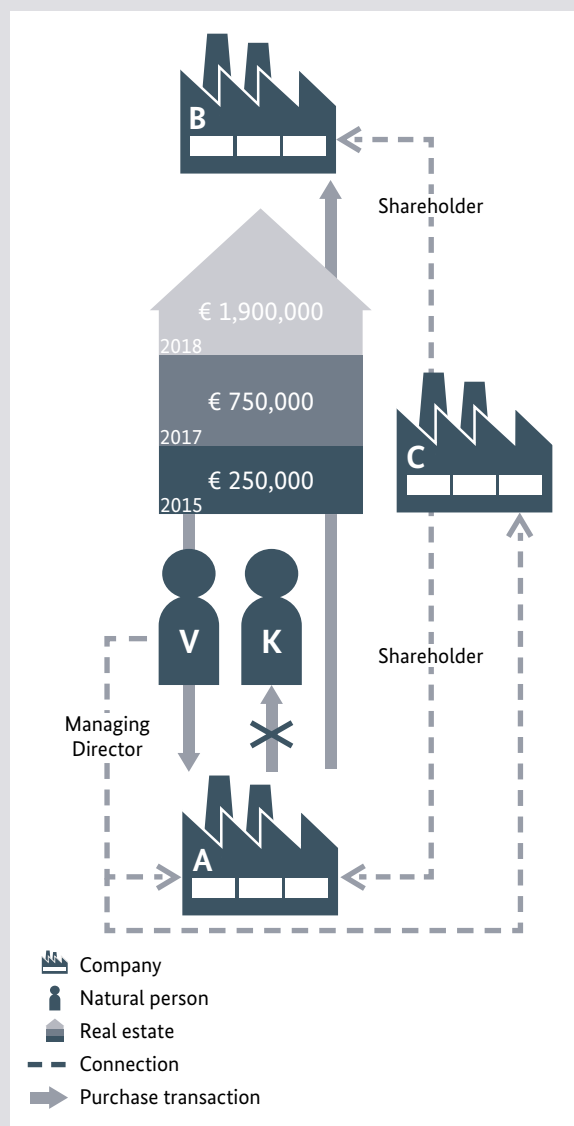


Figure 9 – Conspicuous Sale of Real Estate

17 The described case study is a real case from FIU practice.

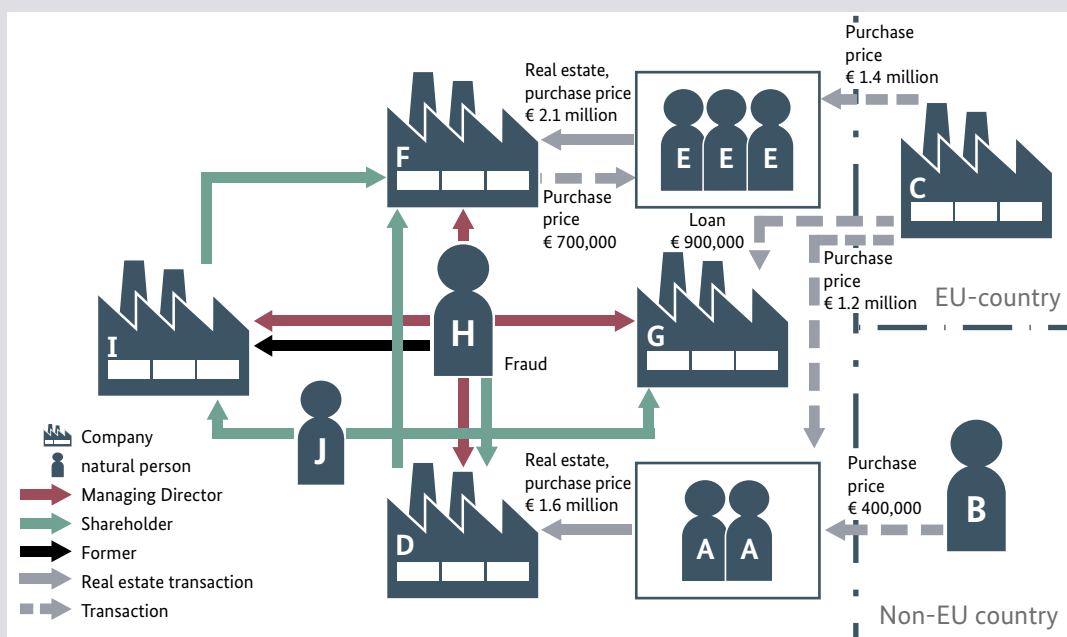


Figure 10 – Funds from Abroad

Case 3 – Funds from Abroad¹⁸

Initial STRs

The joint account of siblings A received € 400,000 from Mr B from a non-EU country for the purchase of a property. A second payment of € 1.2 million to purchase the same property was made by company C from an EU country. The actual buyer of the property is company D. The allocation of the purchase price seemed unusual to the reporting bank. In addition, the purchase price seemed to be clearly too high for the location and condition of the property.

FIU Analysis and Dissemination

Links have been established to two other STRs involving company C. One STR concerned a sale of real estate by owners E to company F with similar characteristics as described above, another STR concerned a conspicuous payment by company C to company G. Through shareholder and managing director constructions, Mr H, a central person of the construct, could be associated with companies D, F, G and another company I. Mr H already has a criminal record for fraud.

Sufficient clues and relevant information have been gathered which suggest a connection to money laundering. The case was disseminated to the competent State Office of Criminal Investigation (LKA).

18 The described case study is a real case from FIU practice.

Case 4 – No Direct Contact with Estate Agent¹⁹

Initial STR

Mr A contacted a real estate agent by telephone with the intention of selling a property as managing director of an asset management company. Research on Mr A led to asset management company X, which initially appeared to be inconspicuous. There was no personal contact. When the estate agent called the telephone number provided by Mr A, an employee of an unknown company E answered. The estate agent’s searches connected company E with criminal activities via a press article. The persons mentioned in the article are also in connection with asset management company X.

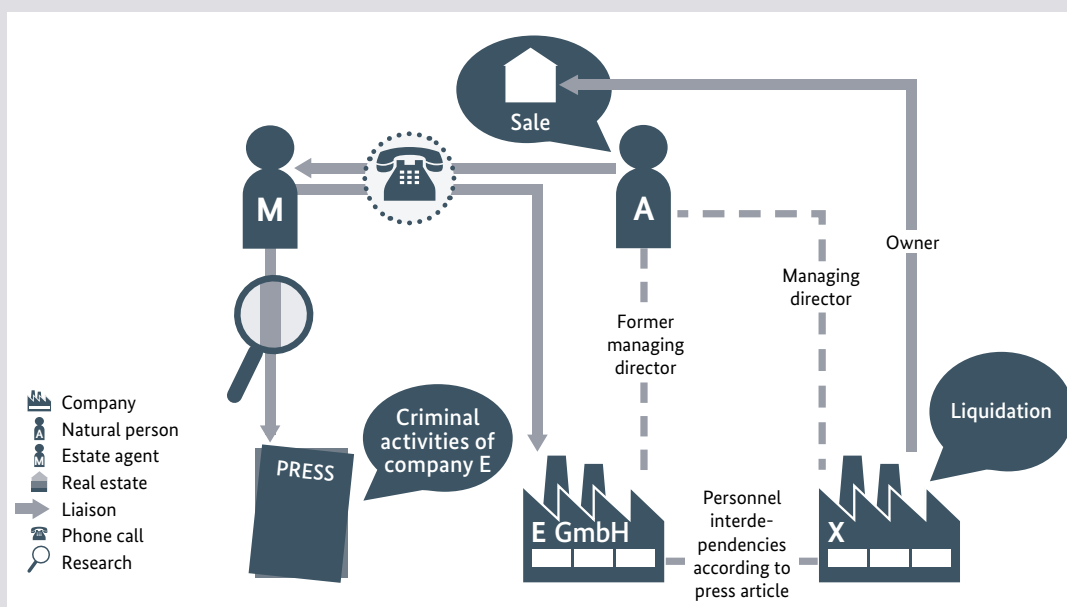


Figure 11 – No Direct Contact with Estate Agent

FIU Analysis and Dissemination

A further STR by a credit institution regarding asset management company X had already been received. In addition, it turned out that Mr A had already been investigated for breach of trust.

It was possible to gather sufficient relevant information to justify dissemination to the competent LEAs. The findings from the STRs, which came from both the financial and non-financial sectors, were compiled into an analysis report and disseminated to the competent State Office of Criminal Investigation (LKA).

19 The described case study is a real case from FIU practice.

Trade in Valuable Goods

Pursuant to Section 2 (1) No. 16 AMLA, traders in goods belong to the group of reporting entities that submit STRs to the FIU. According to Section 1 (9) AMLA, the term “traders in goods” includes “any person who disposes of goods on a commercial basis, regardless of in whose name or on whose behalf he is acting”. The following figure shows the most important subgroups of the 146 reporting traders in goods who have submitted at least one STR in 2018. Among the other reporting entities are, inter alia, retailers of the most varied orientation, wholesalers, furniture stores, basic suppliers and the distribution divisions of large enterprises from the manufacturing industry.

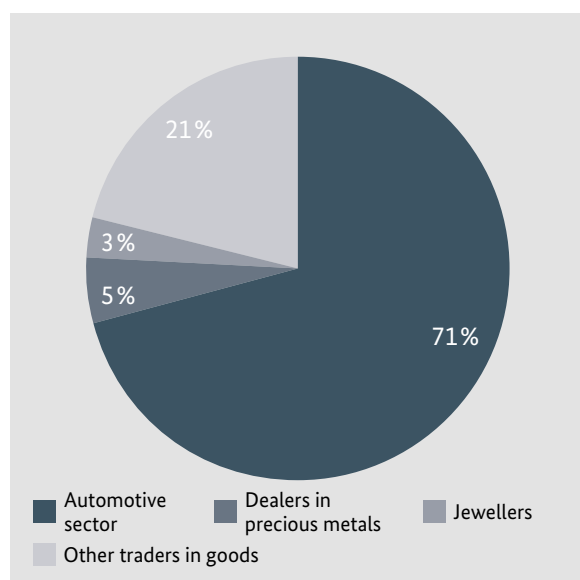


Figure 12 – Subcategories within the Group of Traders in Goods

The fact that a wide variety of goods are suitable as investment goods for incriminated funds is shown, among other things, by the facts that became known at the end of 2018 in connection with the Danske Bank. It became known that several major German corporations from different sectors purchased goods with incriminated funds from abroad and subsequently exported these. From the very large and heterogeneous group of reporting entities of traders, however, individual sectors can be identified whose goods are particularly suitable for money laundering. The success of Europol’s investigation, which became known as Operation “Cedar”, provides a further reason for taking a closer look at the trade in goods.

There it was discovered that a professional money laundering organisation in Germany, for example, acquired used cars, watches and other luxury goods with incriminated funds, then exported them and resold them abroad in order to conceal the source of the incriminated funds used. At peak times, an estimated € 1 million per week were laundered throughout Europe.²⁰ In addition to car dealers, individual jewellers based in Germany were also targeted by the investigators, as large sums of incriminated money were placed without triggering STRs.

20 Comp. e.g. Europol (2017): From Suspicion to Action: Converting financial intelligence into greater operational impact, pg. 16.

Automotive Sector

Motor vehicles (cars) are, like real estate, generally suitable for money laundering activities, as they are high-priced goods which hold their value. They are also highly portable and can even be used as transport vehicles for other valuables. The automotive retail sector is very cash intensive, especially in the used car segment, which further increases the risk of money laundering. In the luxury car segment, vehicles are therefore particularly suitable as investment goods for the integration of incriminated funds. According to the Federal Statistical Office, companies in the automotive retail sector generated sales of just under € 182 billion in 2016.²¹

Within the group of traders in goods, car dealers are the largest and strongest reporting subgroup of reporting entities, accounting for 71% of all active reporting parties and over 60% of STRs.

However, when looking collectively at the STRs submitted by car dealers in 2018 and the STRs explicitly stating “unusual activities in connection with the purchase or sale of motor vehicles”, only 30% of these STRs came from car dealers. At 65%, most STRs come from credit institutions, but leasing companies, supervisory authorities, tax authorities and financial services institutions also submitted STRs in connection with the purchase or sale of motor vehicles.

The different groups of reporting entities have very different insights into the business processes, which is why it is essential for the best possible detection of money laundering activities to combine information from different perspectives. Car dealers often have direct contact with the buyer and can therefore identify unusual activities on a personal level. Frequent reporting reasons here are, for example, the involvement of third parties in sales negotiations, payment or collection of the vehicle. Difficulties in identifying the buyer are also reported, whereby the targeted avoidance of personal contact is also often a reason for reporting. Banks, on the other hand, have detailed knowledge of their customers' accounts and the possibility of applying precisely defined filters to large amounts of data. They report, for example, on the allocation of the purchase price to several transfers (often from different accounts, sometimes from suspicious foreign accounts) or on higher cash payments for the purchase of a motor vehicle.

In 2018 the FIU developed a special typology paper to support reporting entities in reporting suspicions in connection with the purchase or sale of motor vehicles and made it available to the reporting entities in the internal area of the FIU website, which deals specifically with the specifics of the motor vehicle trade.

21 Statistical Yearbook 2018, Chap. 24. Domestic Trade.

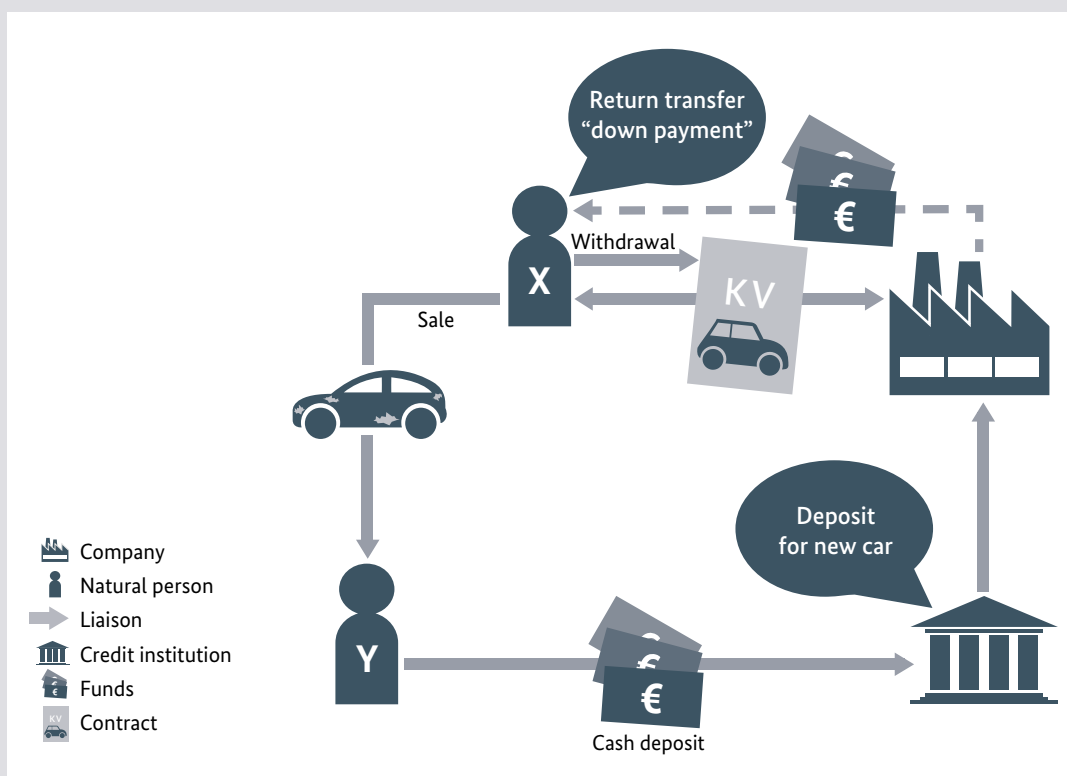


Figure 13 – Cash to Book Money

Case 5 – Cash to Book Money²²

Initial STR

Mr X ordered a new vehicle from a car dealer. He sold his old car privately to Mr Y for around € 20,000. He convinced Mr Y to pay the purchase price for his old vehicle directly in cash to the car dealer’s credit institution which assumed that Mr Y had been authorised by the car dealer, whereas the car dealer assumed that the payment was a down payment on the new car. Mr X withdraws from the purchase of the vehicle and demands a transfer of the alleged down payment, which had previously been paid in cash by Mr Y, to one of his accounts.

FIU Analysis and Dissemination

The FIU’s analysis showed that Mr Y had already made appearances with regard to the non-taxation of importable goods. The facts of the case were disseminated to the competent State Office of Criminal Investigation (LKA).

22 The described case study is a real case from FIU practice.

Watch and Jewellery Trade

The commodities traded in this sector are often high-priced, transportable and stable in value and therefore carry an increased risk for money laundering. In 2018, sales in the jewellery industry in Germany were estimated at € 4.65 billion.²³ In 2018, the FIU received only a low double-digit number of STRs from five different reporting entities in the jewellery sector. The main reasons for suspicion were higher cash payments and conspicuous customer behaviour such as a particularly urgent transaction. On the part of the financial sector, a mid-double-digit number of STRs were received stating the reporting reason “unusual activities in connection with the purchase or sale of jewellery and watches”, which accounts for less than 0.1% of

the total reporting volume of the financial sector. Often an unknown or implausible source of funds was reported for the payment of jeweller’s items and implausible cash payments by jewellers.

As the success of Europol’s investigation mentioned at the beginning of this section illustrates, the specialist watch and jewellery trade is thus an area that can be used for money laundering activities. In view of the low number of STRs, it is particularly necessary to raise the awareness of the reporting entities, especially since even STRs from the financial sector can only provide limited insights.²⁴

²³ Publication of the Bundesverband der Juweliere, Schmuck- und Uhrenfachgeschäfte e.V. (Federal Association of Jewellers, Jewellery and Watch Retailers), www.bv-juweliere.de.

²⁴ See page 41 on the future intensification of cooperation between FIU and reporting entities.

Risks to the Fight against Money Laundering and Terrorist Financing as a Result of New Technologies

From a strategic perspective, new technologies and innovations can be identified that represent challenges in the fight against money laundering and terrorist financing. Progressive digitisation has led to an acceleration of transactions (e.g. through real-time transfers) and new and alternative ways of transferring assets that may also be connected with money laundering and terrorist financing.

Real-time transfer

(Instant Payment) describes the processing of payments in which the amount is available to the recipient within a few seconds.

Internet payment methods (e.g. PayPal) now account for the largest share of online commerce, contactless card payments and smartphone payments are likely to continue to grow strongly following the entry of new major market players.²⁵

In addition, an even stronger internationalisation of payment and asset transfers can be observed, which are primarily handled by companies located abroad and can be conveniently initiated via Internet applications. As a result, some of these payment procedures elude national regulatory requirements relating to money laundering and terrorist financing. Domestic users can access services and applications from FinTechs and virtual currencies regardless of national borders. However, STRs must be submitted to the FIU in the company's country of domicile. Close cooperation and a comprehensive, rapid exchange of information between FIUs are therefore necessary to effectively combat money laundering and terrorist financing.

²⁵ Cf. Deutsche Bundesbank (2018): Payment behaviour in Germany 2017. Fourth study on the use of cash and non-cash payment instruments, pg. 35ff.

FinTechs

FinTech, an artificial term made up of “financial services” and “technology”, is understood to mean “[...] technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services”.²⁶ The business models of FinTechs can be roughly assigned to the areas of payment transactions and securities settlement; deposit business, credit and capital procurement; investment, asset management and insurance and finally the supporting applications. Depending on the business model, the FinTech companies registered with the FIU are predominantly credit institutions (Section 2 (1) no. 1 AMLA) or financial services institutions (Section 2 (1) no. 2 AMLA). From the FIU’s point of view, there is a risk that certain innovative business models of FinTech could facilitate financial transactions and asset transfers and thus also be used for money laundering and terrorist financing (e.g. peer-to-peer payment service providers, online platforms for crowdlending or crowdfunding, trading platforms for virtual currencies). A particular challenge is posed by providers domiciled abroad that are not bound by the national regulatory framework but can nevertheless be used by domestic customers. The key to effectively combating money laundering and terrorist financing is above all the complete traceability of transactions and uniform legal treatment of FinTechs’ business models across national borders.

Individual FinTechs are consistently mentioned in STRs. These include, for example, companies that offer mobile banking services and bank accounts as well as payment transaction services and are frequently misused in suspected cases of fraud (e.g. eBay fraud, so-called “fake shops”) or for financial agent activities. Also conspicuous are trading platforms for virtual currencies, most of which are located abroad, to which third-party funds are directly transferred, that were previously entered into accounts with apparent fraudulent intent. Financial agent activities by involving the use of virtual currencies can be concluded in these cases as well. In addition, the FIU has individual STRs on alleged FinTechs that offer financial investments or participations (e.g. Initial Coin Offerings [ICOs]), which in some cases are cases of fraud and pyramid schemes.

Initial coin offerings (ICOs), oriented to the IPO, Initial Public Offering, are a type of funding, mainly referring to the issuance and sale of a kind of virtual share certificate, often in the form of digital coins or “tokens”.

²⁶ Definition of the Financial Stability Boards (FSB), see <http://www.fsb.org/what-we-do/policy-development/additional-policy-areas/monitoring-of-FinTech/>

Virtual Currencies

The term “virtual currencies” means a “digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored and traded electronically”²⁷. This definition sums up the essential characteristics of these currencies: virtual currencies are digital, immaterial, suitable as means of exchange and units of account. While the trust of the transaction partners in the currency is traditionally ensured by a legal currency monopoly and the role of the central banks, virtual currencies are technology-based. Transactions are stored in decentralized registers that are unchangeable and verifiable. This enables transactions to be clearly fixed and updated in so-called blocks (blockchains), making the currency technically robust against counterfeiting. Values in virtual currencies are stored in electronic, password-protected wallets. Each transaction is uniquely identified by the transaction number, amount, transaction date, sender and recipient addresses of the electronic wallet²⁸. While in theory there is now transparency as to the source and destination of the virtual assets, the background of the transactions and, above all, the owners of the virtual money and the wallets are largely unknown. This represents a significant contrast to conventional transactions via bank accounts.

The FATF has already addressed the risks associated with the use of virtual currencies in 2014 and Europol also dealt extensively with this topic²⁹. The identification of transaction partners and the clarification of the source of funds for transactions based on virtual currencies are made more difficult by the fact that providers of trading platforms for virtual currencies and providers of electronic wallets are not yet globally regulated. Therefore, international cooperation in the fight against money laundering and the creation of a uniform legal framework is of particular importance.

At first glance, the use of virtual currencies results in largely anonymous or pseudo-anonymous transactions between unknown market participants. Some virtual currencies have been developed with the aim of making the path of assets untraceable, which makes their use attractive for transactions with an illegal background. In fact, relatively transparent virtual currencies are and have been used in the so-called “darknet” to handle arms and drug deals, to acquire child pornographic material, for money laundering and terrorist financing, and to circumvent financial sanctions.³⁰

Darknet

describes a separate address space on the Internet that is not visible from the outside and whose participants communicate with each other directly or via a decentralized server system. The aim is to allow access only to insiders and to guarantee an anonymous exchange of information or data.

27 Directive (EU)2018/843 of the European Parliament and the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and amending Directive 2009/138/EC and 2013/36/EU, pg. 12.

28 It should be noted that under certain circumstances the blockchain can be manipulated, cf. Budish, Eric (2018): The Economic Limits of Bitcoin and the Blockchain, NBER Working Paper No. 24717.

29 See FATF (2014): Guidance for a Risk-Based Approach to Virtual Currencies, Europol (2017): Crime in the age of technology.

30 Cf. Bundeskriminalamt (2018): Cybercrime. Bundeslagebild 2017, and Houben, Robby; Snyers, Alexander (2018):

Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion, (www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf, Status: 31.01.2019).

In 2018, the FIU received around 570 STRs from reporting entities (mainly credit institutions) with unusual activities in connection with virtual currencies. A low double-digit number of transactions are due to requests and spontaneous information from foreign FIUs, domestic LEAs and fiscal authorities.

In the STRs submitted to the FIU, the reporting entities stated “fraud” and “unknown source of funds” as the main reasons for suspicion. Further, comparatively often reported reasons were a presumed action of the customer for third parties (front man function) and a generally conspicuous behaviour of the customer. Approximately 55% of these STRs finalised to date have been disseminated to the competent LEAs. The rate of disseminated STRs with unusual activities in connection with virtual currencies is thus slightly lower than the overall rate of disseminated STRs for 2018 (58%).³¹

On the basis of the experience gained to date, it can be summarised that the FIU regularly deals with STRs and transactions relating to virtual currencies. A challenge lies in the fact that the FIU is not able to clarify the background of these transactions and the owners of virtual money directly and that the trace of money very often leads to trading platforms for virtual currencies abroad.

In the future, it is to be expected that the number of STRs in connection with virtual currencies will increase as the technology becomes more widespread. In addition, once the 5th EU Anti-Money Laundering Directive is transposed into national law, also service providers carrying out the exchange between virtual currencies and fiat money as well as providers of electronic wallets will be obliged to submit STRs.³²

Fiat money

is money without a value of its own that is not covered by the value of goods or raw materials, but is accepted as a medium of exchange. Today, this includes practically all currencies defined as legal tender such as the euro or the US dollar.

This expansion of all reporting entities which, among other things, entails an obligation to report suspicious transactions as well as obligations to identify the owners of electronic wallets, represents an important contribution to limiting the risks associated with the use of virtual currencies.

³¹ See page 17.

³² Directive (EU) 2018/843 of the European Parliament and the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing and amending Directives 2009/138/EC and 2013/36/EC (OJ L 156/43 of 19 June 2018).

National Cooperation

Cooperation with Law Enforcement Agencies

Cooperation with Supervisory Authorities

Requests from Domestic Authorities

Cooperation with Reporting Entities

National Cooperation

With the rapid development of complex economic issues and new technologies, the challenges for effective prevention of money laundering and terrorist financing are growing. This makes it all the more important to cooperate closely with all national authorities within the network.

The main national partner authorities of the FIU are:

- the competent law enforcement and judicial authorities (federal and state police, public prosecution authorities, financial control of illicit employment, customs investigators, tax investigators),
- the competent supervisory authorities (including the Federal Financial Supervisory Authority (BaFin), various Länder supervisory authorities in the non-financial sector),
- the authorities of the fiscal administration (Federal Central Tax Office, fiscal authorities of the Länder) as well as
- the Federal Office for the Protection of the Constitution (BfV) as well as the Federal Intelligence Service and the Military Counter-Intelligence Service.

A further essential factor for the FIU in fulfilling its legal tasks, in particular the receipt and analysis of information in connection with money laundering or terrorist financing, is the intensive exchange with the reporting entities pursuant to Section 2 (1) AMLA.

Cooperation with Law Enforcement Agencies

In 2018, the FIU maintained a continuous exchange with the various LEAs of the Federation and the Länder. In addition to bilateral talks and participation in various events organized by LEAs, the FIU ensured, for example, a regular exchange with national police authorities (State Offices of Criminal Investigation and Federal Criminal Police Office), representatives of the financial investigations of the Länder, as well as representatives of public prosecution authorities of the Länder North Rhine-Westphalia, Schleswig-Holstein, and the Central Organized Crime and Corruption Office Celle by organizing two conferences in spring and autumn. These meetings were accompanied by telephone conferences with the same group of participants. At management level, the FIU also made several inaugural visits to State Offices of Criminal Investigation (LKAs). In addition, the FIU was a guest at the semi-annual meetings of the Federal Criminal Police Office (BKA) and the State Offices of Criminal Investigation (LKAs), the AG Kripo.

In order to further optimise cooperation with the national police authorities, a special management plan was drawn up in autumn 2018 with the national police authorities, which marks the essential cornerstones for future cooperation, taking into account police requirements. This includes a comprehensive catalogue of measures. In 2018, for example, standards for optimising uniform analyses were agreed with the LEAs. The aim of these agreements was, on the one hand, to make the FIU's analysis activities more transparent for the LEAs and, on the other hand, to increase the direct usability of the analysis reports with regard to the various LEAs. In addition, work has begun on mutual work shadowing to improve the direct exchange of information and promote mutual trust. In addition, the direct exchange of information is to be substantially improved by the future deployment of FIU liaison officers in the State Offices of Criminal Investigation. These measures will be continued in 2019 and regularly evaluated.

Cooperation with Supervisory Authorities

Following the reorganisation of the FIU on 26 June 2017, representatives of the FIU also participated in several events of the supervisory authorities pursuant to Section 50 (9) AMLA in 2018 in order to promote the establishment of contacts and the exchange of information with the various supervisory authorities. In the middle of the year, the FIU hosted a first conference at which the diverse supervisory landscape of the non-financial sector and the previous cooperation with the authorities in the area of money laundering were discussed. The aim was to decide on concrete measures for improved cooperation and a closer exchange of information in order, on the one hand, to support the supervisory authorities in the exercise of their

supervisory duties and, on the other hand, to further optimize the work of the FIU through appropriate feedback.

Subsequently, the FIU created a password-protected internal area for supervisory authorities on the FIU website. In this area, the FIU makes relevant information (e.g. typology papers) available to the supervisory authorities and, on request, to other cooperation authorities, which is useful for them in the course of their tasks. These are continuously updated and expanded here.

Requests from Domestic Authorities

Pursuant to Section 32 (3) AMLA, LEAs and intelligence services in particular, as well as other authorities under certain conditions, are entitled to request personal data from the FIU, insofar as this is necessary for the investigation of money laundering and terrorist financing or other criminal offences. In 2018, this option was used in a total of 1,924 cases. Although the vast majority of requests were made by police authorities, the FIU also received numerous requests from LEAs and customs (ZFD, FKS, HZÄ), for example. Domestic requests enable the cooperation authorities themselves to initiate a formalised, effective exchange of data with the FIU.

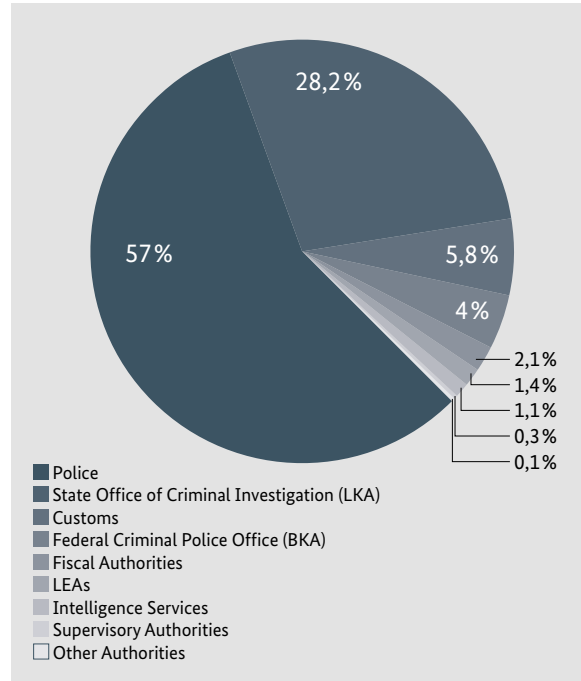


Figure 14 – Distribution of Domestic Requests by Sender

Cooperation with Reporting Entities

Intensive cooperation between the FIU and those obliged under the AMLA is an important success factor in effectively combating and preventing money laundering and terrorist financing. Regular exchanges enable the FIU to respond to the needs of the reporting entities and provide an important basis for them to submit high quality STRs. This has been achieved through the hosting of money laundering meetings and workshops, as well as numerous bilateral practice dialogues. Furthermore, representatives of the FIU participated in various external events of the financial and non-financial sector by giving specialist lectures.

In 2018, the FIU hosted two money laundering conferences for the financial sector, attended by numerous representatives of associations and selected reporting entities. The focus was on the reorganisation of the FIU as of 26 June 2017 and the associated electronic reporting obligation, the improvement of the quality of the STRs, the development of a new FIU feedback concept for reporting entities and the presentation of a typology paper for the financial sector.

The FIU also held a money laundering conference for associations in the non-financial sector. Participants came from sectors such as real estate, galleries and art dealers, car manufacturers, jewellers, jewellery and watch shops and sports betting. In addition to the reorganisation of the FIU, trends and typologies relating to money laundering and terrorist financing were presented, particularly in the non-financial sector. In addition, a supervisory authority provided information on the due diligence obligations of the reporting entities.

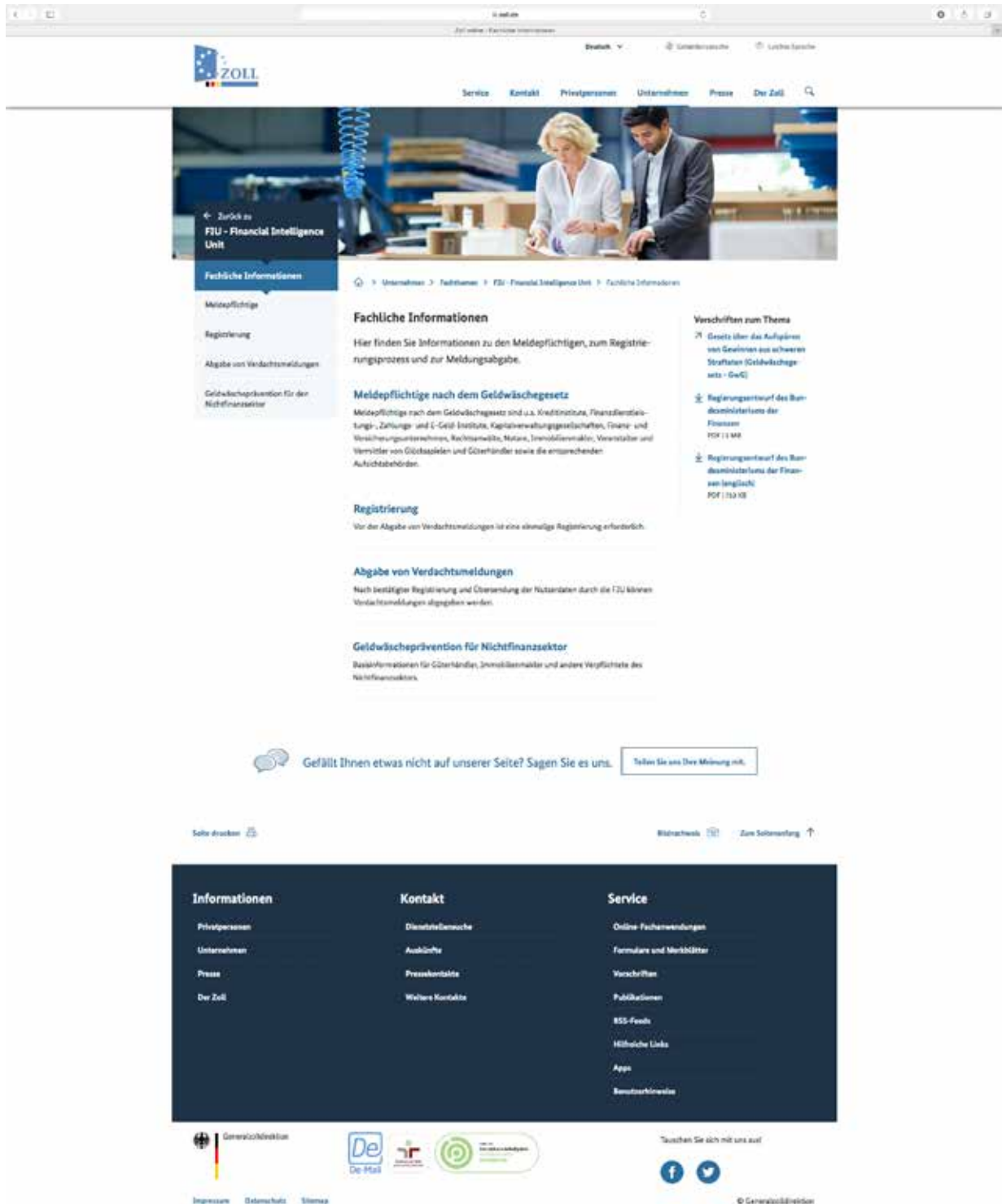
As a result of the conferences, the FIU website was expanded to include practical information on how to use the reporting software (goAML) and information on combating money laundering and terrorist financing. In addition, a consultation procedure and a workshop were held in order to better adapt the goAML software to the needs of the reporting entities.

The software **goAML** was developed especially for FIUs by the Office of Information and Communications Technology of the United Nations. goAML uses internationally agreed standards and interfaces for data exchange and enables processes and integrated analyses that are largely free of media discontinuity. AML stands for “Anti Money Laundering”.

Implementation of the results of the completed procedure is scheduled for 2019. At the first money laundering conference of the financial sector, a new feedback concept was presented, which is primarily intended to optimise the risk management of the reporting entities. The aim here is to provide the reporting entities with information so that they can critically examine their own reporting behaviour and, if necessary, make adjustments to internal procedures to fulfil their due diligence obligations. This concept was subsequently further optimised in a consultation procedure, in the course of which constructive comments were received from industry associations and reporting entities.

Detailed information regarding the conducted consultation procedure is available on the website of the FIU. The website also contains information with respect to the goAML software, numerous

technical information as well as information about organized meetings and participation in events.



International Cooperation

Information Exchange with other FIUs

International Committee Work

International Cooperation

Information Exchange with other FIUs

Money laundering and the financing of terrorism are cross-border and international phenomena, the effective combating of which requires cooperation with international partners. Therefore, there is a continuous exchange of information between FIU Germany and its international partner FIUs. Proactively relevant information is passed on between the FIUs or made available to the cooperation partners upon request. With the help of this information, the FIU Germany can

investigate cross-border structures and cases and support other FIUs in their work by transmitting information.

With a total of 135 countries, the FIU exchanged information in this way in 2018. Cooperation was particularly strong with France, Great Britain, Luxembourg, the Netherlands, Cyprus, Switzerland and Italy.

Incoming and Outgoing Information and Requests

In the international context, the FIU Germany received and analysed a total of 1,363 requests (846) and information without requests (spontaneous information: 517) related to money laundering from other FIUs in the reporting period 2018. Compared to the previous year (1,260), the number of notifications received increased slightly.³³ The requests and spontaneous information were sent by a total of 96 FIUs worldwide. The senders included all 27 European FIUs. The processed requests and notifications are distributed among the individual cooperation partners as shown in Table 3.

The FIU Germany itself sent 1,255 requests and 3,737 spontaneous information reports to 129 FIUs during the reporting period. This corresponds to a significant increase compared to the previous year and illustrates the international character of the incoming STRs. Table 3 shows the main addressees of the information sent.

³³ In the annual report 2017, 1,748 "Correspondence processes with an international dimension" were reported for this purpose. However, these included 488 domestic correspondence transactions, which, according to today's understanding, do not belong to this category. Due to the reorganisation of the FIU and the associated change in the counting method, a direct comparison of the number of correspondence processes is not possible.

Country	Request incoming	Request outgoing	Spontaneous information incoming	Spontaneous information outgoing	Total
France	62	76	5	683	826
Great Britain	48	122	19	262	451
Luxembourg	65	65	154	29	313
Netherlands	63	103	3	110	279
Cyprus	5	10	7	210	232
Switzerland	20	55	9	123	207
Italy	42	47	0	116	205
British Virgin Islands	0	1	0	193	194
Russia	24	13	12	141	190
Spain	14	78	6	89	187
Austria	17	42	41	82	182
Malta	25	23	46	67	161
Latvia	15	8	4	110	137
Lithuania	21	71	0	38	130
USA	30	30	8	62	130
Turkey	13	32	0	84	129
Belgium	50	28	3	47	128
Poland	13	48	0	52	113
Hungary	12	19	29	32	92
Other	307	384	171	1,207	2,069
Total	846	1,255	517	3,737	6,355

Table 3 – Number of Incoming as well as Outgoing Spontaneous Information and Information Requests

Temporary Freezing Orders

In eight cases, requests for information were accompanied by a request to temporarily freeze a

transaction or block an account. The transactions involved represent a total volume of € 1,040,000.

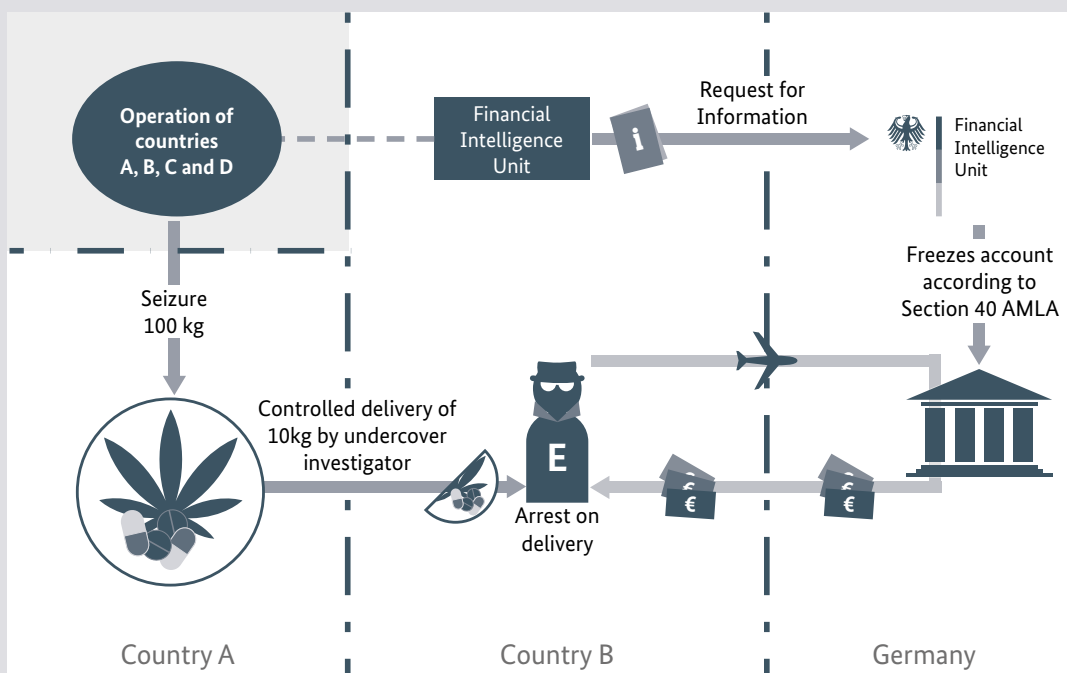


Figure 15 – Temporary Freezing Order International

Case 6 – Temporary Freezing Order International³⁴

As part of the operation in countries A, B, C and D, 100 kg of drugs were confiscated in country A. These drugs were originally intended to be shipped from country A to country B. To enable the operation to identify the consignee of the goods, part of the drugs (10 kg) were delivered to consignee E as part of a controlled delivery by an undercover investigator. On delivery, E was arrested.

It became known that E travelled to Germany before the transfer to withdraw the money for the purchase of the drugs in country B.

The FIU of country B informed the German FIU of the facts. As a result, the German FIU prohibited outgoing transactions from E’s account by ordering an urgent measure pursuant to Section 40 AMLA.

34 The described case study is a real case from FIU practice.

International Committee Work

Close cooperation with foreign partners and active participation in all major international authorities and organizations are fundamental strategic goals of the FIU. In this context, the FIU generally strives to contribute relevant aspects to the fight against money laundering and terrorist financing, to optimize framework parameters and principles, and to gain timely knowledge of new developments.

The intensification and optimization of strategic international cooperation was actively pursued in 2018.

Egmont Group of FIUs (Egmont Group)

The Egmont Group is an association of 158 FIUs (including the German FIU) providing a platform for the secure exchange of expertise and financial information to combat money laundering and terrorist financing. In this group, various technical topics for strengthening and optimizing the joint global fight against money laundering and terrorist financing are discussed and corresponding approaches to solutions are coordinated.

In addition to the FIU's active participation in various projects and work in individual working

groups, the election of the deputy head of the German FIU as chairman of the "Information Exchange Working Group (IEWG)" with a term of office until 2020 deserves special mention. The largest and most important group is to provide a forum for members to develop solutions to improve the quality, quantity and timeliness of information exchange between FIUs. With the assumption of the chairmanship, it is now increasingly possible to submit own proposals and projects and to play an active part in shaping the overall orientation of the Egmont Group in this area.

Financial Action Task Force (FATF)

The FATF is an intergovernmental body established in 1989 by the Heads of State of the G7 countries and the President of the European Commission. Its objectives are to set standards and promote the effective implementation of legal, regulatory and operational measures to combat and prevent money laundering, terrorist financing and other related threats to the integrity of the international financial system.

The FIU participated in the German delegation led by the Federal Ministry of Finance (BMF) at the FATF's three plenary meetings in 2018, focusing on participation in the meeting of FIU heads

(HoFIU forum) and the RTMG expert group (Risks, Trends and Methods Group).

Within the framework of its technical competence, the FIU examines the relevance of the various FATF drafts, e.g. guidelines and recommendations for preventing and combating certain phenomena, and integrates them into its own risk management. In addition, the FIU contributes by providing its own findings, e.g. on the phenomenon of professional money laundering or on the use of virtual currencies for the purpose of money laundering.

International Cooperation Project “Professional Money Laundering Networks“

In 2018 the FIU participated in a project of the Egmont Group on “Professional Money Laundering Networks” (PMLN). The objectives of the project included identifying cross-border payment flows, strengthening bilateral cooperation between FIUs in the field of PMLN control and sharpening risk indicators.

The FIU took this project as a starting point to initiate a strategic evaluation project in the sense of a Public Private Partnership (PPP) with partners from the private sector in Germany. The PMLN risk indicators were made available to the project participants for application to their respective data-bases. In close exchange with the participating institutions, the possibilities and limits of the use of this set of risk indicators were examined and possibilities for optimisation and adaptation discussed.

Results

- Using the risk indicators, relevant transactions with cross-border payment flows were identified, which could be delivered to the Egmont Project Group in anonymous form for further international evaluation.
- In addition, spontaneous information was sent to FIUs of countries from which senders and/or recipients of relevant transactions originate.
- The feedback of the participating institutions on the risk indicators was consolidated and sent to the Egmont Project Group to further sharpen the risk indicators.

EU-FIUs-Platform

The EU-FIUs Platform is an informal group established by the European Commission in 2006 and registered as a Commission Expert Group in 2014. Its main objective is to facilitate cooperation between FIUs and to advise the Commission on issues related to FIUs.

The FIU participated in the four platform meetings in 2018 and actively participated in two operational projects, which aimed at promoting the exchange of information between the EU FIUs.

Other focal points included participation in a working group to develop a secure communication channel for the exchange of information between the central agencies of the Member States, as foreseen by the 4th Anti-Money Laundering Directive, and extensive discussions on various European legislative procedures concerning the competences of the FIUs.

Financing of Terrorism and other Crimes relevant to State Security

Total Number of STRs with Reference to Terrorist Financing or State Security

Dealing with STRs relating to Terrorist Financing or State Security

Strategic Evaluations of the Phenomenon of Terrorist Financing and State Security

Temporary Freezing Orders

Information Exchange in the Sector of Counter Terrorist Financing

Proliferation Financing

Financing of Terrorism and other Crimes relevant to State Security

Total Number of STRs with Reference to Terrorist Financing or State Security

Between 1 January 2018 and 31 December 2018, the FIU received a total of 4,516 STRs with a first indication of a relation to terrorist financing or state security.

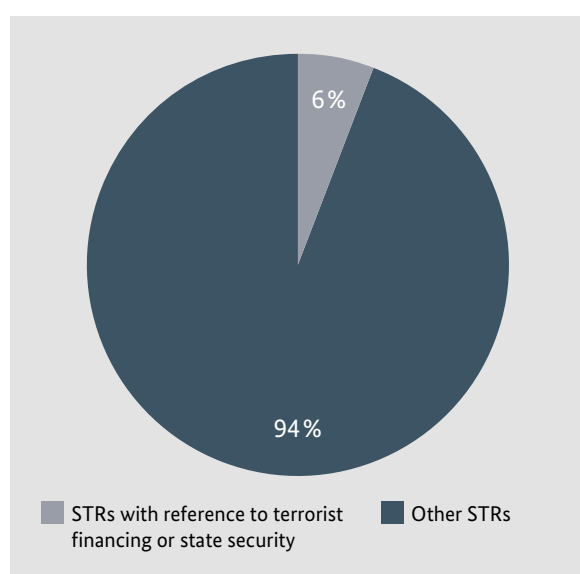


Figure 16 – Relative Share of STRs with Reference to Terrorist Financing or State Security

The share of STRs relating to terrorist financing or state security in the total volume of all STRs has risen significantly compared to the 2017 reporting year. This may be an indication of raised awareness of the reporting entities.

While the relative share of such STRs in the total number of STRs in the years prior to the reorganisation of the FIU was always between 2% and 4%, it had already reached 5% by 2017. In 2018, the share rose once again to about 6%.

In addition to current political developments or current terrorist or state security incidents, the reporting behaviour of the reporting entities is also influenced by measures taken by the FIU to increase awareness. Thus, a continued increase in the number of STRs is to be expected.

Dealing with STRs relating to Terrorist Financing or State Security

All STRs received by the FIU are first evaluated in the context of a preliminary check for a possible reference to terrorist financing and state security.

An initial indication may result from information provided by the reporting entities in the STRs. Irrespective of this, the FIU's initial evaluation can also reveal that a terrorist financing or state security reference appears possible. In both cases, these STRs are further processed by the FIU's

department specializing in terrorist financing or state security.

Pursuant to Section 32 (1) AMLA, all STRs classified as possibly relevant to terrorist financing or state security – irrespective of the result of the operational analysis – are immediately forwarded to the Federal Office for the Protection of the Constitution (BfV) upon receipt. In accordance with Section 32 (2) AMLA, the BfV is also informed of the result of the corresponding operational analysis.

Strategic Evaluations of the Phenomenon of Terrorist Financing and State Security

General Information

The strategic processing of information for intelligence and analysis purposes is of particular importance in the context of combating the financing of terrorism, since it aims at detecting preparatory and dangerous actions for carrying out an attack and can assume a preventive function in the run-up to the perpetration of an offence. Intelligence information basically contains any information that serves to provide knowledge of criminal activities. Here, among other things, findings from science, criminal prosecution and publicly accessible information are evaluated.

While the fight against money laundering is aimed at preventing the integration of incriminated funds into the legitimate economy, the fight against the financing of terrorism focuses on identifying and preventing any actions intending to financially support terrorism. The use of assets can therefore have two different aims. On the one hand, it can serve the direct financing of a concrete terrorist attack, on the other hand it can be used to maintain terrorist organisations and infrastructures. The financing requirements of terrorist groups thus go well beyond the costs of carrying out terrorist attacks and also include support for propaganda measures, the recruitment of new members, the training of potential assassins and covering living costs for existing members.

The procurement of funds for terrorist groups is manifold and adapts to the constantly changing circumstances. The assets used to support terrorism are therefore not exclusively those that were legally acquired and through their intended use become an incriminated asset and thus the subject of a STR. Current developments show, in particular, that terrorist organisations are increasingly making use of illegal sources of financing as well since the maintenance of organisational structures can no longer be guaranteed, which is also due to diminishing territories. The financing of terrorism usually does not involve large amounts of money paid in a single transaction, but lives from a multitude of supporters who are either knowingly or unknowingly involved in the process of financing terrorism. Both the low transaction amounts and the use of alternative transaction channels instead of the formal banking system make it difficult for the FIU and the reporting entities to identify indications of terrorist financing.

Insights and Trends

The STRs received by the FIU that relate to terrorism or national security can be classified into two different groups with regard to their reasons for suspicion – those with personalised or objective criteria. In the case of personal reasons, the conspicuity may be, for example, atypical customer behaviour or a listing on a terror or sanctions list. Furthermore, the FIU receives STRs which may not be related to the financing of terrorism on the basis of the persons or organisations involved, but rather on the basis of objective criteria, i.e. the characteristics of the underlying transaction. For example, geographical regions, such as countries classified as high-risk countries, play a role here. The conspicuity may also be due to the frequency, amount or lack of plausibility of the transaction.

Due to its role as central agency, the FIU is an important knowledge carrier and can contribute to the early identification of risks in the field of terrorist financing through the evaluation of STRs.

In particular, the expansion of international cooperation with the FIU's partner authorities is a crucial parameter for strengthening cooperation in the area of combating terrorist financing and identifying *modi operandi* on a cross-border level.

The characteristics of terrorist financing include various activities and can be brought into a triad in the international context: (1) the raising of funds, (2) the subsequent transfer of funds to hold or conceal them (moving) and (3) the use of funds to sustain terrorist organisations and infrastructures or to carry out specific terrorist attacks (using).

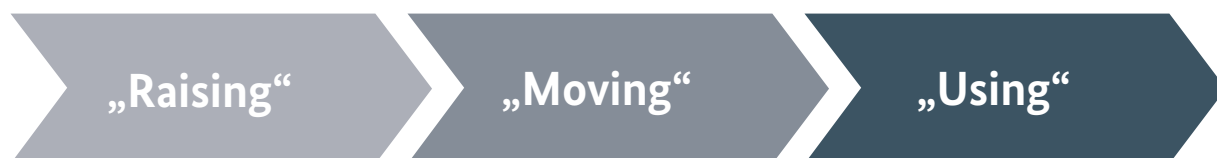


Figure 17 – Characteristics of Terrorist Financing

Raising:

The first characteristic of terrorist financing is the procurement of assets that are to be used for terrorist purposes at a later date. This procurement is carried out by both conscious and unwitting

supporters. Especially donation payments are widespread phenomena in this context.

Example: Crowdfunding

Crowdfunding is an internet-based collection of donations that has proven to be a suitable vehicle for reaching a large number of potential supporters in the context of terrorist financing, for example through the use of social networks or other online platforms. In particular unknowing donors are involved in the process of financing terrorism who are unaware of the purposeful and abusive end use of the funds.

Moving:

The second characteristic of terrorist financing is the shifting of assets that are to be used for terrorist purposes at a later date. In these cases, the affected state is involved as a transit country in the process of counter terrorist financing (CFT) and is

thus misused to conceal the terrorist purpose. In addition to the smuggling of cash, the integration of alternative remittance systems and the concealment of beneficial owners also fall into this category.

Example: NGOs/NPOs

The involvement of non-governmental organisations (NGOs) in the financing needs of terrorist organisations is often the result of the misuse of aid organisations. On the one hand, international aid funds can be channelled through the integration of legitimate aid organisations by partially misappropriating them, since the recipients of the payments are members of terrorist organisations. On the other hand, supposed aid organisations can be under the complete control of terrorist groups so that the funds are channelled through those pseudo-recipients for terrorist purposes.

Using:

The third characteristic of terrorist financing is the use of assets with a terrorist purpose. The financing of terrorism can be achieved indirectly through general financial support for terrorist

organisations or individual perpetrators as well as directly through support for a terrorist attack.

Example: E-Money Cards

E-money cards are electronic means of payment based on credit balances which hold a risk for terrorist financing because of the possibility to anonymously deposit and withdraw cash. This risk especially exists in conflict zones. Such cash equivalents guarantee the short-term and adequate capacity of terrorist organisations to act and have already been used in the past to carry out terrorist attacks.

Temporary Freezing Orders

In 2018, in four cases the operational analysis revealed the need to issue an urgent measure pursuant to Section 40 AMLA in order to further examine whether a transaction is related to counter terrorist financing or other offences relevant to state security. In these four cases, transactions with a total volume of more than € 500,000,000³⁵

were stopped for up to 30 days in order to further assess the respective facts. In the case of two measures, there were subsequently concrete indications of punishable acts, which resulted in a dissemination to the respective competent authority. In these cases, the transaction amount was € 500,150,000.

³⁵ Section “Urgent Measures” gives an overview of all 18 temporary freezing orders adopted by the FIU, four of which are related to counter terrorist financing.

Information Exchange in the Sector of Counter Terrorist Financing

As part of its responsibility to combat the financing of terrorism, the FIU exchanges information intensively at national level with the authorities involved in the security architecture. National requests are often made in the course of investigations, preliminary investigations or in situations of immanent risk. The FIU cooperates intensively with the state security departments of the federal and state police authorities as well as the intelligence services. In 2018, the FIU received a total of 190 national requests.

In addition to national cooperation in the field of terrorist financing, cooperation at the international level is an important component.

The information transmitted from abroad complement the phenomenological findings gained from the national STRs.

In total, the FIU exchanged information with 51 foreign FIUs. In 2018, the FIU received and analysed a total of 128 international requests (91) and spontaneous information (37) from abroad. These were sent to the FIU by 15 EU Member States and 16 other countries. The FIU also sent a total of 78 re-quests and one spontaneous information to foreign FIUs worldwide. In this context, information was sent to 19 EU Member States and 17 other countries.

Country	Request incoming	Request outgoing	Spontaneous information incoming	Spontaneous information outgoing	Total
Luxembourg	10	15	23	0	48
France	15	4	1	0	20
Belgium	14	0	0	1	15
Turkey	6	6	0	0	12
USA	6	2	3	0	11
Netherlands	5	1	1	0	7
Russia	3	0	4	0	7
Greece	2	4	0	0	6
Italy	2	4	0	0	6
Spain	4	1	1	0	6
Switzerland	2	3	0	0	5
Bulgaria	0	3	0	0	3
Austria	0	2	1	0	3
Slovakia	2	1	0	0	3
Czech Republic	2	1	0	0	3
Other	18	31	3	0	52
Total	91	78	37	1	207

Table 4 – Number of Incoming as well as Outgoing Spontaneous Information and Information Requests with Reference to Terrorist Financing or State Security

Proliferation Financing

Proliferation describes the distribution of chemical, biological and nuclear weapons of mass destruction or the transfer of products and know-how to produce them. Also included are so-called dual-use goods, which can be used for both civilian and military purposes so that the end use plays a decisive role. In line with the fight against money laundering and the financing of terrorism, there are also international standards for combating and preventing proliferation financing, the aim of which is to detect or prevent the distribution or transfer of the aforementioned goods, technologies and know-how. Despite strict export controls, Germany can be the target of procurement efforts by high-risk countries. In particular, the

processing 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, such as detour deliveries, at an early stage.

A total of 63 STRs with reference to the risk countries Iran and North Korea were submitted to the FIU, which contain references to proliferation financing. Unlike in the previous reporting year, no such STRs with reference to Syria and Pakistan were submitted to the FIU.

List of Figures

	Title	Page
Figure 1	Process Sequence of the Operational Analysis of STRs	12
Figure 2	Development of the Number of STRs under the AMLA (2008 - 2018)	13
Figure 3	Distribution of the STRs after Evaluation	17
Figure 4	Distribution of STRs according to Recipients	17
Figure 5	Number of Feedbacks by Public Prosecution Authorities in 2018	18
Figure 6	Overview of the Convictions, Penalty Orders and Indictments	18
Figure 7	Number of Suspicious Transactions According to Country of Origin	21
Figure 8	Number of Suspicious Transactions according to Country of Destination	22
Figure 9	Conspicuous Sale of Real Estate	26
Figure 10	Funds from Abroad	27
Figure 11	No Direct Contact with Estate Agent	28
Figure 12	Subcategories within the Group of Traders in Goods	29
Figure 13	Cash to Book Money	31
Figure 14	Distribution of Domestic Requests by Sender	40
Figure 15	Temporary Freezing Order International	46
Figure 16	Relative Share of STRs with Reference to Terrorist Financing or State Security	50
Figure 17	Characteristics of Terrorist Financing	52

List of Tables

	Title	Page
Table 1	Number of STRs by Group of Reporting Entities	14
Table 2	Number of active Reporting Entities	16
Table 3	Number of Incoming as well as Outgoing Spontaneous Information and Information Requests	45
Table 4	Number of Incoming as well as Outgoing Spontaneous Information and Information Requests with Reference to Terrorist Financing or State Security	55

List of Abbreviations

Abbreviation	Explanation
AMLA	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) vom 23. Juni 2017/ Money Laundering Act (AMLA) of 23 June 2017
AO	Abgabenordnung/Tax Code
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht/Federal Financial Supervisory Authority
BfV	Bundesamt für Verfassungsschutz/Federal Office for the Protection of the Constitution
BKA	Bundeskriminalamt/Federal Criminal Police Office
BMF	Bundesministerium der Finanzen/Federal Ministry of Finance
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FKS	Finanzkontrolle Schwarzarbeit/Financial control of Illicit Employment
HZÄ	Hauptzollämter/Main Customs Offices
ICO	Initial Coin Offering
IEWG	Information Exchange Working Group
IPO	Initial Public Offering
LEAs	Strafverfolgungsbehörden/Law Enforcement Agencies
LKA	Landeskriminalamt/State Office of Criminal Investigation
PMLN	Professional Money Laundering Networks
PPP	Public Private Partnership
StGB	Strafgesetzbuch/Criminal Code
STRs	Verdachtsmeldungen/Suspicious Transaction Reports
ZFD	Zollfahndungsdienst/Customs Investigation Service

■ IMPRESSUM:

Herausgeber:

Generalzolldirektion
Financial Intelligence Unit (FIU)
Postfach 85 05 55
51030 Köln

Redaktion:

Generalzolldirektion

Gestaltung und Herstellung:

Generalzolldirektion, Bildungs- und Wissenschaftszentrum der Bundesfinanzverwaltung

Registriernummer:

90 SAB 272

www.zoll.de

Köln, Oktober 2019

