



Financial
Intelligence Unit



Annual Report 2021

Financial Intelligence Unit

Annual Report 2021

Financial Intelligence Unit

Table of Contents

Preface	7
Overview of the FIU	9
Suspicious Transaction Reports (STRs)	13
Total Number of STRs for Reporting Year 2021	15
Total Number of STRs, Categorised by Subgroups of Reporting Entities	16
Assessment Results for STRs in 2021	20
Feedback Reports from Public Prosecution Authorities	22
Temporary Freezing Orders	23
Proliferation Financing	25
Transactions	26
Typologies and Trends	29
Description and Continuation of Key Risk Areas	30
Special Topic COVID-19	33
Focus on Real Estate	38
Focus on Serious (Tax) Criminal Acts, e.g., Carousel Fraud	42
Focus on the Use of New Payment Methods	46
Assessment of Reports on Cash Discoveries	54
National Cooperation	57
Cooperation with Law Enforcement Agencies (LEAs)	59
Cooperation with Supervisory Authorities	61
Requests from Domestic Authorities	66
Cooperation with Reporting Entities under AMLA	70
International Cooperation	75
Information Exchange with Other FIUs	76
International Committee Work	87

List of Figures	94
List of Tables	95
List of Abbreviations	96

Dear Readers,

The FIU is constantly developing and doing so under challenging framework conditions. In 2021, the year covered by this report, the FIU was reorganised as a functional authority and Directorate X under the Central Customs Authority (GZD). Furthermore, the FIU opened a new location in Dresden, to complement the head office in Cologne. These developments were accompanied by a continuous growth of the staff, something you can read more about in section “Overview of the FIU”.

This lets us not only implement the FIU’s potential for optimisation as determined in the course of the ongoing evaluation, but also react to an area of responsibility that has expanded with amendments to the German Anti-Money Laundering Act (AMLA) and the Criminal Code, a constantly increasing number of suspicious transaction reports (STRs) and new ways of committing crimes that the pandemic and current economic policy developments have given rise to. Accordingly, the analysis process was adjusted to intelligently complement controlling and prioritisation by using the key risk areas, which were already introduced in previous years. In this regard, I wish to draw your attention specifically to the “Typologies and Trends” section. A total of just under 300,000 STRs, which is the highest absolute increase during a year since the relocation of the FIU, confirms that we are on the right path. You will find additional information on the figures in the “Suspicious Transaction Reports (STRs)” section.

Since the final phase of the Germany Audit by the Financial Action Task Force (FATF), which was actually planned for the year 2020, had to be postponed due to the pandemic, the FIU welcomed the international audit committee at its head office in Cologne for an onsite audit in November 2021. In the runup, numerous interviews were conducted



in the Federal Ministry of Finance (BMF). The final report on the FATF Germany Audit was published on 25 August 2022. Its recommendations for action to fight money laundering in Germany are further motivation to work with our partners to decisively address deficiencies mentioned and to keep improving good achievements.

In the preface to the Annual Report 2019, I wrote that the publication of that annual report came during an unusual time. What I meant by that was the spread and fight against the novel Sars-CoV-2 virus and the consequences of the pandemic resulting from it. Now, the world is facing new threats as a result of a war of aggression being fought in Europe, the effects of which are already influencing the FIU’s work on preventing and fighting money laundering and countering terrorist financing. The FIU Germany will also confront these challenges flexibly and decisively and continue to grow with its responsibilities.

Christof Schulte

Head of the FIU

Overview of the FIU

Overview of the FIU

The FIU is the German national central agency for investigating financial transactions. It is established under the umbrella of the Central Customs Authority (GZD) as an independent and administrative authority for the receipt, collection and analysis of suspicious transaction reports (STRs) in terms of the German Anti-Money Laundering Act (GwG, AMLA).

In accordance with the requirements of each EU Anti-Money Laundering Directive and the international standards of the Financial Action Task Force (FATF) to prevent and combat money laundering and terrorist financing, an operationally independent central agency was set up in the Federal Republic of Germany to receive suspicious transaction reports (STRs) to be submitted by reporting entities in accordance with the Anti-Money Laundering Act (AMLA). The central agency for investigating financial transactions (FIU) analyses in varying depth the facts of the reported suspicious financial transactions, which could potentially be related in particular to money laundering or terrorist financing. As a central hub, it combines its own data with a wide range of relevant information from other authorities and other domestic as well as international agencies and then shares the actions identified as valuable with the law enforcement agencies (LEAs) and other competent authorities.

In a non case-specific strategic analysis, the FIU also identifies new methods and trends in the area of money laundering and terrorist financing

and provides the insights it has gained and the patterns it has detected to its own operational analysis units as well as to reporting entities and partner authorities in the form of clues and typologies papers and in other formats, such as on the occasion of anti-money laundering conferences or via the Anti Financial Crime Alliance (AFCA). Furthermore, the FIU keeps the statistics required under the respectively applicable EU Anti-Money Laundering Directive and the Anti-Money Laundering Act, and publishes them in particular in the annual report.

The FIU makes a significant contribution not only to discovering money laundering and terrorist financing in a comprehensive manner, but also to effectively preventing such by continuous monitoring and regular exchange with the reporting entities on the one hand and close cooperation with cooperating domestic authorities and international partners on the other.

Continued Development of the FIU – Processes and Handling of Responsibilities

On schedule in September 2021, the FIU, together with an external advisor, was able to complete an in-depth, process-oriented analysis of how it handles its responsibilities. The aim of the analysis was to continue the future-oriented development of the FIU and to keep strengthening the handling of its responsibilities, while simultaneously mapping to the most adequate organisational structure. The continuous monitoring and support of the Federal Ministry of Finance (BMF) ensures this.

In 2022 the FIU has attached the highest priority to the implementation and operationalisation of

the resulting proposals and outcomes. Partner authorities and reporting entities are thoroughly involved into this process to effectively strengthen the fight against money laundering.

As a result, the technical processes should also be complemented by what is referred to as a “2 level model”. This is to be understood as the future differentiation between a standardised processing of simple cases to keep increasing efficiency and the addressing of complex larger-scale cases that will continue to be the focus of the FIU’s analytical activity.

Continued Development of the FIU – Implementation of the New Organisational Structure

The FIU has seen a substantial increase in staff, especially due to the impact of the amendments to the Anti-Money Laundering Act that entered into force on 1 January 2020¹ and due to the constant increase in suspicious transaction reports (STRs). The plan is for staff to be increased to over 700 employees. To expand the FIU’s technical processes with an eye to the future and to continue optimising its handling of tasks and external perception commensurate with need, an organisational adjustment took place establishing the FIU as the new Directorate X within the Central Customs Authority (GZD) on 1 May 2021.

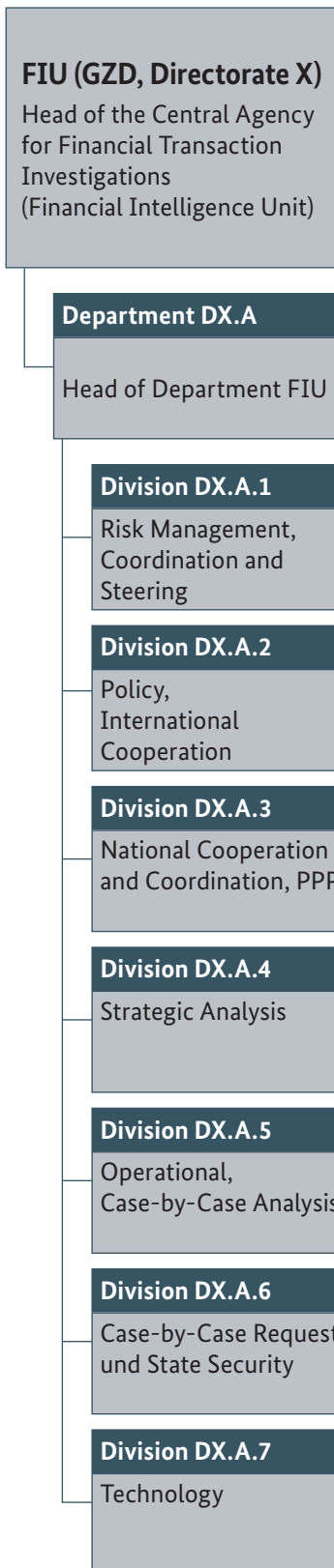
To start with, the restructuring of Directorate X shall not result in any change to the previous division structure. Solely the brief descriptions of the FIU’s organisational units will change on account of this – along with the implementation of a Head of Directorate as the permanent representative of

the authority management. Accordingly, the FIU is still composed of seven divisions that are split into departments and units. Parallel to this, the FIU began to implement the results of the above described, in-depth, process-oriented analysis of the handling of tasks and to set up a new organisational structure within Directorate X, which should include two departments in the future.

Furthermore, in addition to the head office in Cologne, the FIU opened another FIU location for operational and strategic analytic tasks in Dresden on 1 December 2021.

You will find additional technical information and recent developments on the FIU’s website at www.fiu.bund.de.

¹ Law on Implementing the Fourth EU Anti-Money Laundering Directive, on Executing the EU Funds Transfers Regulation and on Reorganising the Central Agency for Financial Transaction Investigations of 23 June 2017 (German Federal Law Gazette [BGBl.] I, p. 1822); Act on the Implementation of the Fourth EU Anti-Money Laundering Directive of 12 December 2019 (BGBl. I, p. 2602).



Organisational Structure in the Year under Review

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

Division DX.A.2 bundles the following tasks: policy (including policy activities), centralised technical management (including specific organisational development and controlling) and international cooperation.

Division DX.A.3’s mission is to ensure cooperation and exchange with the national law enforcement agencies and supervisory authorities as well as with the reporting entities according to the German Anti-Money Laundering Act. This also comprises cooperation within the scope of public-private partnerships (PPP).²

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

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

Division DX.A.6 analyses suspicious transaction reports related to terrorist financing or state-security matters and is the main contact point for all national and international partners in the area of operational cooperation (money laundering and terrorist financing).

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

² See the “National Cooperation” section for more information on the topic of PPP.

Suspicious Transaction Reports (STRs)

Total Number of STRs for Reporting Year 2021

Total Number of STRs, Categorised by Subgroups of Reporting Entities

Assessment Results for STRs in 2021

Feedback Reports from Public Prosecution Authorities

Temporary Freezing Orders

Proliferation Financing

Transactions

Suspicious Transaction Reports (STRs)

As the central agency, the FIU receives all STRs and information about suspicious financial transactions that are potentially related to money laundering or terrorist financing and analyses them. The following explanatory remarks address these incoming STRs in detail. All reports and notifications that the FIU received in 2021 from reporting entities, fiscal authorities and supervisory authorities are relevant in this context.³ Information shared with the FIU in accordance with Section 30 (1) No. 3-4 of the Anti-Money Laundering Act (AMLA) is not considered as STRs from reporting entities.

The electronically received STRs are subject to a multi-step operating analysis with a risk-based method systematically applied.

Receipt of Report – Analysis – Decision

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

An STR is continuously assessed by applying the risk-based approach (RBA) to determine which information should be subject to further analysis. During the initial assessment, the reports are prioritised. STRs that can be assigned to a key work or risk area⁴ of the FIU, that constitute a reason in accordance with Section 46 (1) AMLA or include possible connections to terrorist financing and state-security matters are immediately handed

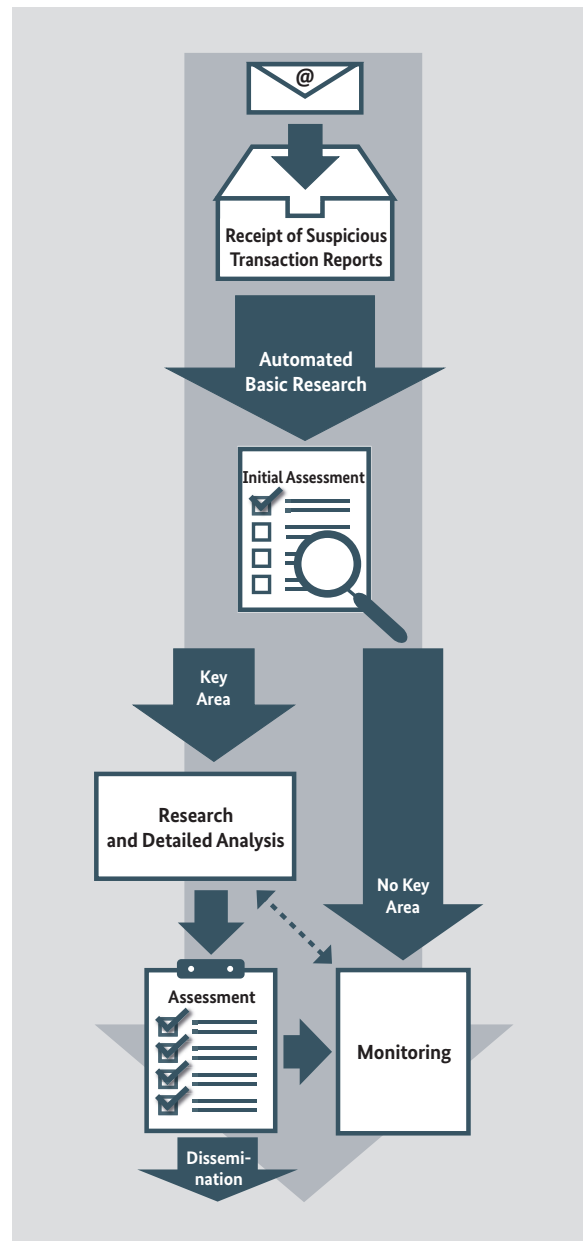


Figure 1: Process Sequence in Operational Analysis

over for in-depth analysis. Otherwise, the STRs initially remain in the monitoring phase. From there, they are continuously compared to the existing database and may be collated with other information at a later date and transferred for a detailed analysis.

³ Reports submitted in accordance with Sections 43 and 44 AMLA and Section 31 b of the German Tax Code (AO) are considered here. Thus, all reports and notifications that fall under Section 30 (1) No. 1-2 AMLA are listed.

⁴ For a list of the key risk areas, see the “Typologies and Trends” section.

If the in-depth analysis determines that an asset is connected with money laundering, terrorist financing or other criminal acts, an analysis report

is disseminated to the respectively competent law enforcement agencies and other agencies.

Total Number of STRs for Reporting Year 2021

The total number of STRs received by the FIU in 2021 reached 298,507 reports. This constitutes an increase of around 154,500 reports, which is the highest absolute rise in STRs within a year since the relocation of the FIU and corresponds to an increase of over 100% in comparison to the STRs received in the previous year. The total number of STRs has increased more than twentyfold over the last ten years, starting at just 13,544. Thus, the upward trend in the total number of STRs also continued in 2021. The reason for this is primarily

the all-crimes approach that took effect during the year. Other reasons for the increase in the total number of STRs are, inter alia, the Ordinance on Matters in the Real Estate Sector Subject to Reporting under the Anti-Money Laundering Act (GwGMeldV-Immobilien),⁵ which entered into force on 1 October 2020 and took effect in 2021, as well as the dynamic development of the market for cryptocurrencies.⁶

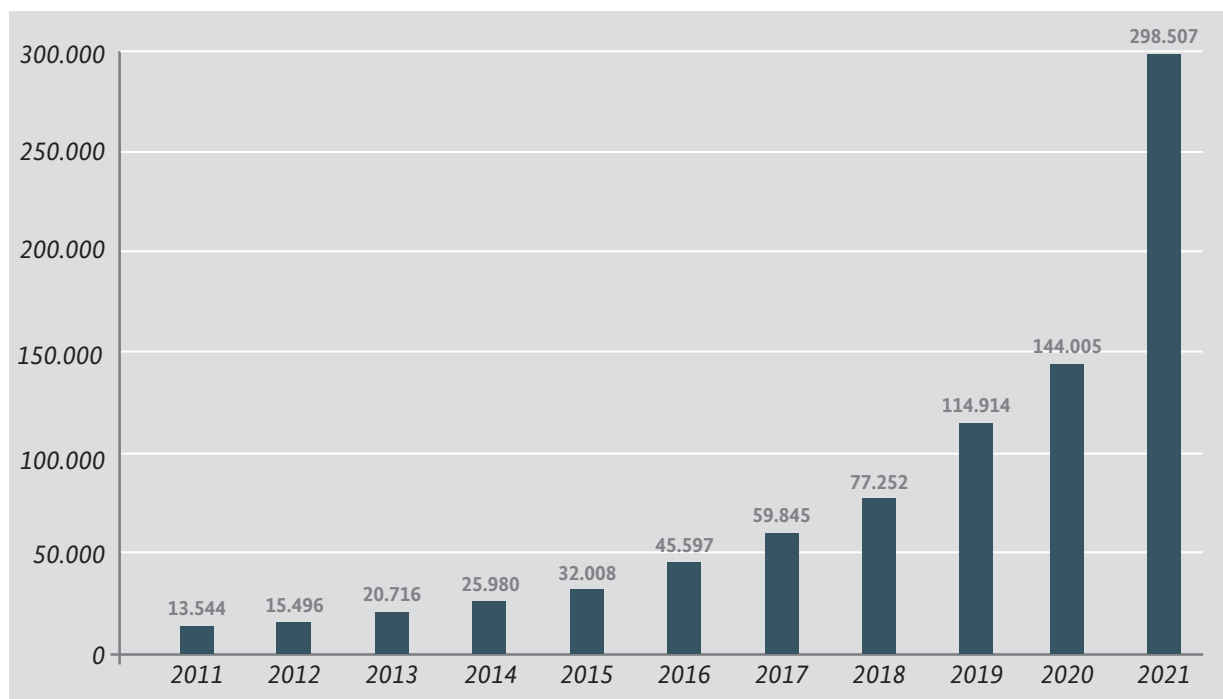


Figure 2: Development of the Number of STRs according to the AMLA (2011 - 2021)

⁵ The Ordinance on Matters in the Real Estate Sector Subject to Reporting under the Anti-Money Laundering Act specifies the reporting obligations for specific professions – especially lawyers, notaries, auditors and tax consultants – for transactions in connection with real estate transactions. Certain typified actions that exhibit suspicious characteristics in regards to a possible connection to money laundering are to be reported to the FIU by these professional groups.

⁶ See the explanatory remarks in the “Typologies and Trends” section for more information on the STRs in individual key risk areas.

The number of STRs potentially related to terrorist financing and other crimes relevant for state security totalled 3,183 received reports, which was a slight decline from just under 3,600 reports in the previous year. These STRs as a percentage of the total STRs declined from 2% in 2020 to 1% in 2021. Only relevant STRs are designated for in-depth analysis in the area responsible for terrorist financing and state security due to the systematic implementation of the risk-based approach and the associated prioritisation. If a connection to terrorist financing or state security can be ruled out after the initial assessment, the report is not included in the number of STRs potentially related to terrorist financing or state security.

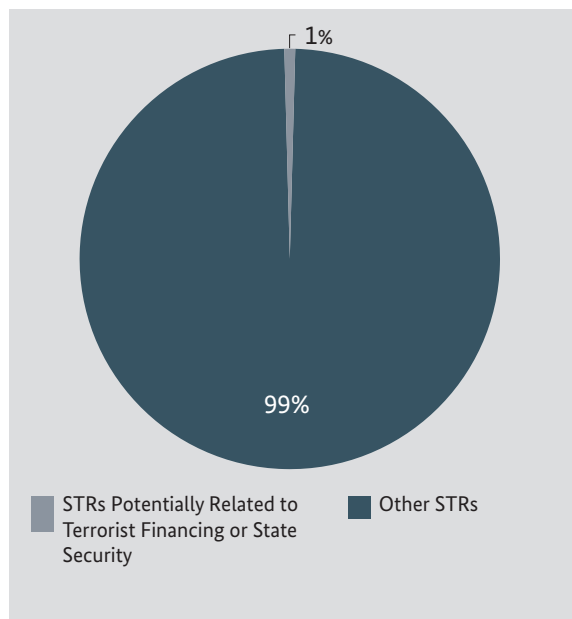


Figure 3: Relative Share of STRs Potentially Related to Terrorist Financing or State Security

Total Number of STRs, Categorised by Subgroups of Reporting Entities

As in recent reporting years, the FIU has seen an increase in the total number of STRs in both the financial and non-financial sector. For the first time in two years, the total number of STRs from authorities and other reporting entities also ticked up once again. The total number of STRs increased by 107%.

The overwhelming majority of the reports, around 97%, come from the financial sector. The increase of over 148,000 reports corresponds to a rise of 106%. After a drop in the previous year, the FIU saw an extraordinary leap in STRs submitted by payment and electronic money institutions. These increased from 238 STRs received in 2020 to 95,386 reports in 2021. The reason for this is the adjustment in behaviour by individual payment and electronic money institutions as a reaction to the all-crimes approach.

In this year, there was also a disproportionate increase in STRs in the non-financial sector. In comparison to the previous year, the number of STRs for this group of reporting entities almost tripled. This increase is primarily due to the rise in the total number of STRs from the group of reporting entities classified as notaries. This is connected with the Ordinance on Matters in the Real Estate Sector Subject to Reporting under the Anti-Money Laundering Act, which took effect on 1 October 2020. Furthermore, substantially more STRs were received in the area of financial companies and estate agents. A moderate decline in reports by insurance undertakings and organisers and brokers of games of chance can be seen. In comparison to the previous year, the number of reports from the non-financial sector as a percentage of total reports rose by 0.7 percentage points to 2.7%.

Suspicious Transaction Reports (STRs)

Total Number of STRs, Categorised by Subgroups of Reporting Entities

Annual Report 2021
Financial Intelligence Unit

	Reporting entities ⁷	2019	2020	2021	Change 2020/2021
Financial sector	Credit institutions	103.697	129.108	180.394	↗
	Financial service institutions	7.528	9.983	12.289	↗
	Payment institutions and electronic money institutions	290	238	95.386	↗
	Agents	650	730	911	↗
	Independent business persons	0	0	0	→
	Insurance undertakings	232	233	222	↘
	Asset management companies	42	33	33	→
	Total STRs from the financial sector	112.439	140.325	289.235	↗
Non-financial sector	Financial companies	39	338	378	↗
	Insurance intermediaries	17	6	11	↗
	Lawyers	21	23	83	↗
	Legal advisors who are members of a bar association	0	0	0	→
	Patent attorneys	0	0	0	→
	Notaries	17	1.629	6.471	↗
	Legal advisors	3	0	0	→
	Auditors and chartered accountants	0	7	23	↗
	Tax advisors and authorised tax agents	8	15	36	↗
	Trustees, service providers for trust companies	15	13	6	↘
	Estate agents	84	135	177	↗
	Organisers and brokers of games of chance	754	252	220	↘
	Traders in goods	554	436	782	↗
	Total STRs from the non-financial sector	1.512	2.854	8.187	↗
Other	Supervisory authority	149	144	173	↗
	Fiscal authorities	697	608	754	↗
	Other STRs	117	74	158	↗
	Total	114.914	144.005	298.507	↗

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

⁷ Groups of reporting entities according to the German AMLA.

Registered and Active Reporting Entities

The Anti-Money Laundering Act (AMLA) was amended as of 1 January 2020⁸ such that reporting entities must electronically register with the FIU independently of the submission of an STR (Section 45 (1) (2) AMLA). This obligation is tied to the start of the new information network of the FIU – which will occur on 1 January 2024 at the latest.

The number of reporting entities registered with the FIU was just under 16,000 as of 31 December 2021, of which around 3,700 are from the financial sector and almost 12,200 from the non-financial sector.

Even if not as pronounced as in the previous year, the FIU observed a high number of registrations by reporting entities in 2021 as well. Just under 3,400 reporting entities (2020: around 7,700) from the financial and non-financial sector have registered in total.

In the financial sector, there were just under 700 new registrations, with financial service providing companies (Section 2 (1) No. 2-5 AMLA) showing the greatest increase with almost 500 new registrations (2020: just under 300 new registrations). The largest share of new registrations was in the non-financial sector at just under 2,700 reporting entities and extends to all subgroups of reporting entities. With 1,306 new registrations, just under half of them belonged to the subgroup of reporting entities of designated lawyers, legal advisors and notaries (Section 2 (1) No. 10, 11 AMLA).

The amendment of the Anti-Money Laundering Act expanded besides the registration obligation also the subgroup of reporting entities, inter alia, to include income tax assistance associations. The FIU informed chambers and associations to make them aware of this. In the course of this, 162 of around 800 total income tax assistance associations (Section 2 (1) No. 12 AMLA) in Germany registered with the FIU in 2021.

On account of the positive experience and development in 2022, the FIU is planning more information activities related to the registration obligation and the associated interaction between the FIU and various chambers and associations. The increasing integration and successful deployment of chambers and associations as multipliers has shown that this is the best way to get information to individual subgroups of reporting entities.

The registration of a reporting entity does not necessarily mean that there is “suspicion” of money laundering or terrorist financing. Consequently, the number of registered reporting entities diverges from the number of active ones. The following table gives an overview of the number of active reporting entities, i.e. those who submitted at least one report in 2021.

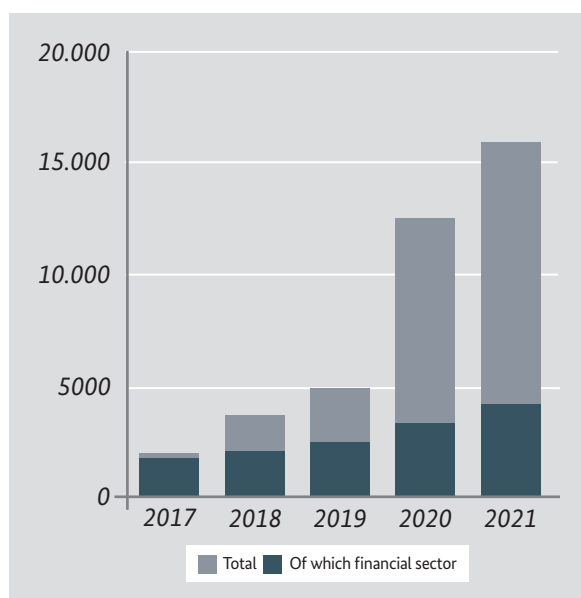


Figure 4: Total Number of Registered Reporting Entities and Portion in Financial Sector

⁸ See Law on Implementing the Fourth EU Anti-Money Laundering Directive, on Executing the EU Funds Transfers Regulation and on Reorganising the Central Agency for Financial Transaction Investigations of 23 June 2017 (German Federal Law Gazette [BGBl.] I, p. 1822); Act on the Implementation of the Fourth EU Anti-Money Laundering Directive of 12 December 2019 (BGBl. I, p. 2602).

	Reporting entities ⁹	2019	2020	2021	Change 2020/2021
Financial sector	Credit institutions	1,274	1,290	1,302	↗
	Financial service institutions	87	90	114	↗
	Payment institutions and electronic money institutions	21	18	23	↗
	Agents	21	15	19	↗
	Independent business persons	0	0	0	→
	Insurance undertakings	57	51	59	↗
	Asset management companies	13	18	14	↘
	Total reporting entities from the financial sector	1,473	1,482	1,531	↗
Non-financial sector	Financial companies	4	5	5	→
	Insurance intermediaries	5	3	7	↗
	Lawyers	18	18	57	↗
	Legal advisors who are members of a bar association	0	0	0	→
	Patent attorneys	0	0	0	→
	Notaries	15	723	1,510	↗
	Legal advisors	2	0	0	→
	Auditors and chartered accountants	0	6	5	↘
	Tax advisors and authorised tax agents	4	11	23	↗
	Trustees, service providers for trust companies	4	4	3	↘
	Estate agents	47	75	74	↘
	Organisers and brokers of games of chance	116	74	59	↘
	Traders in goods	174	164	203	↗
		Total reporting entities from the non-financial sector	389	1,083	1,946
	Total	1,862	2,565	3,477	↗

Table 2: Number of Active Reporting Entities

The number of active reporting entities increased again. In the financial sector, the number of active reporting entities ticked up slightly, rising by 3.3%. The majority of the uptick in active reporting entities is ascribed to the non-financial sector. The total number of active reporting entities rose by 863 to 1,946 here. This corresponds to an increase of just under 80%. As in the previous

year, the FIU primarily saw an increase in the subgroups of reporting entities designated as lawyers and notaries. This is connected with the Ordinance on Matters in the Real Estate Sector Subject to Reporting under the Anti-Money Laundering Act, which took effect at the end of the previous year (1 October 2020).

⁹ Groups of reporting entities according to the German AMLA.

Assessment Results for STRs in 2021

From over 298,500 STRs received by the FIU in 2021, around 40,200 reports in total were sent to the competent authorities. This equates to a rate of disseminations of 13.5%.

	2020	2021
Received Suspicious Transaction Reports	144.005	298.507
Of which disseminated by the end of 2020 (rounded) ¹⁰	24.700	
Rate	17,2%	
Of which disseminated by the end of 2021 (rounded) ¹¹	29.300	40.200
Rate	20,3%	13,5%

Table 3: Share of Disseminated STRs

The rates of disseminations for the two years discussed could still converge somewhat over the course of 2022. The reason for this is that in 2022 more reports with a receipt date from 2021 will probably be disseminated compared to reports from 2020. This convergence can also be observed on the change in the rate of disseminations in the previous year. Relative to January 2021, it was around 17.2%, but rose to 20.3% relative to January 2022. The rates indicated in the table above will be updated and adjusted in the Annual Report 2022. The sharp rise in the absolute number of disseminated reports with a simultaneous decrease in the rate of disseminations shows the

tremendous importance of the FIU’s filter function in an environment of extremely high increases in the total number of STRs. From the increasingly large quantities of data, the facts which are valuable for law enforcement agencies must be extracted and analysed.

STRs are often disseminated in bundles. If the FIU’s case analysis finds sufficient clues for a justified suspicion of money laundering, terrorist financing or other crimes, a bundle of all the associated STRs is disseminated to the responsible authorities. In 2021 a total of around 29,000 (2020: around 18,000) of such analysis bundles were sent to the respectively responsible recipients. This substantial increase of over 61% reflects the FIU’s continued technical and methodological development.

As in previous years, most of the analysis reports were disseminated to the state offices of criminal investigation (LKÄs) and public prosecution authorities (2021: 97.1%; 2020: 97.4%). The rate of disseminations to the customs investigation service offices totalled 1.6% and was thus slightly higher than in the previous year (2020: 1.5%). As in the previous year, 0.9% of all analysis reports were shared with the tax investigation authorities. Other authorities such as the intelligence services or the Federal Criminal Police Office (BKA) received twice as many disseminations proportionally as in 2020 (2021: 0.4%; 2020: 0.2%). The following figure shows a differentiation according to recipients of the disseminations.

10 Comprises all disseminated STRs until 31 January 2021, to include also those STRs that were received only shortly before the end of 2020 and could be analysed only in the following days.

11 Comprises all disseminated STRs until 31 January 2022, to include also those STRs that were received only shortly before the end of 2021 and could be analysed only in the following days.

In accordance with Section 8 of the Code of Criminal Procedure (StPO), the transmission of the analysis results is handled according to the principle of residence. Consequently, analysis reports are always transmitted to the law enforcement agency in whose district the residence of the (main) suspect or the registered office of the (main) involved organisation is located.

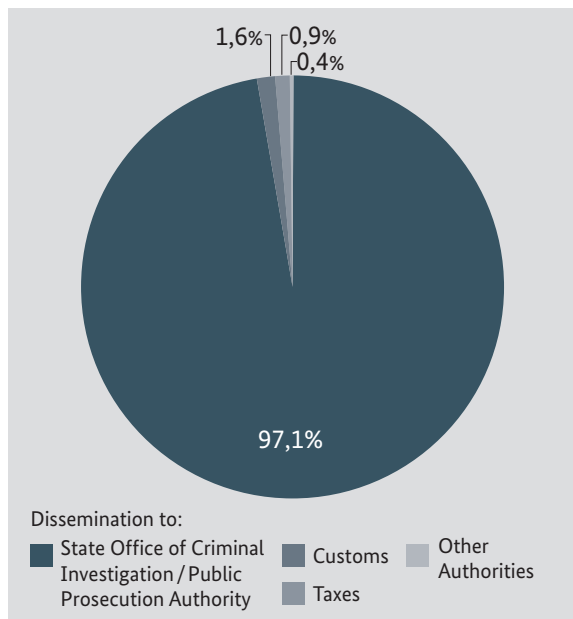


Figure 5:
Breakdown of Reports by Recipients of Disseminations

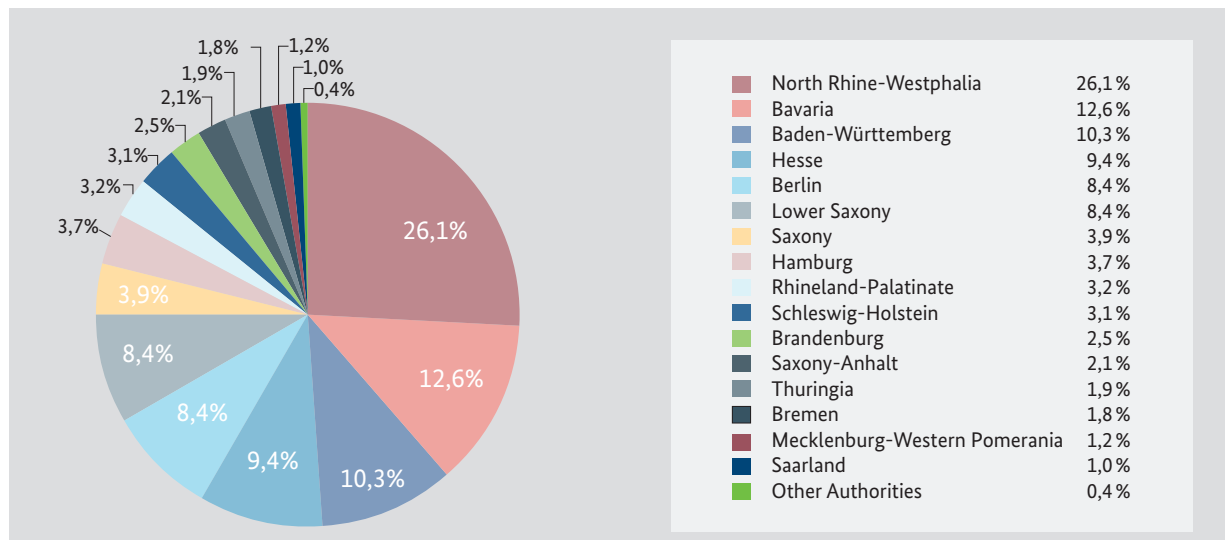


Figure 6: Breakdown of Analysis Reports Disseminated to the Federal States

In 2021 the most reports were again disseminated to the federal state of North Rhine-Westphalia (roughly 21.5% share of the population), although also less than in the previous year

(2021: 26.1%: 2020: 33.6%).¹² 12.6% (2020: 10.9%) of the reports were disseminated to Bavaria (15.8% share of the population).

¹² North Rhine-Westphalia was the recipient of many disseminations primarily because of circumstances related to the pandemic, especially corona emergency aid fraud. In the meantime, a change in the recording rules has caused the simple forwarding of STRs related to emergency aid fraud to no longer be considered as a “dissemination” in these statistics.

Feedback Reports from Public Prosecution Authorities

By sending a copy of the indictment, penalty order, a discontinuation decision or a judgement, the competent FIU's public prosecution authority notifies the FIU of a charge and the outcome of the proceedings, including discontinuation decisions, provided that the FIU has shared information in regards to these proceedings. In 2021 the FIU received a total of 14,186 such feedback reports from public prosecution authorities (2020: 12,618). This equates to a 12% increase year on year.

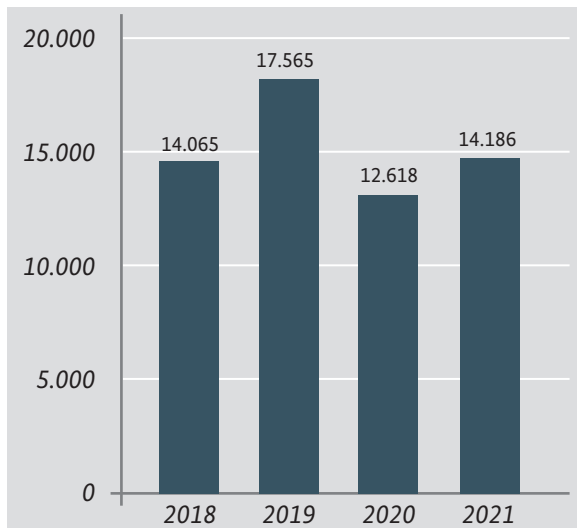


Figure 7: Number of Feedback Reports from Public Prosecution Authorities

The total of 1,352 feedback reports were convictions, penalty orders, decisions and indictments (2020: 783). This is another increase, from 6.2% in 2020 to 10% in 2021. 90% of the feedback reports from public prosecution authorities, that is, the vast majority, consist of orders for the withdrawal of prosecution.

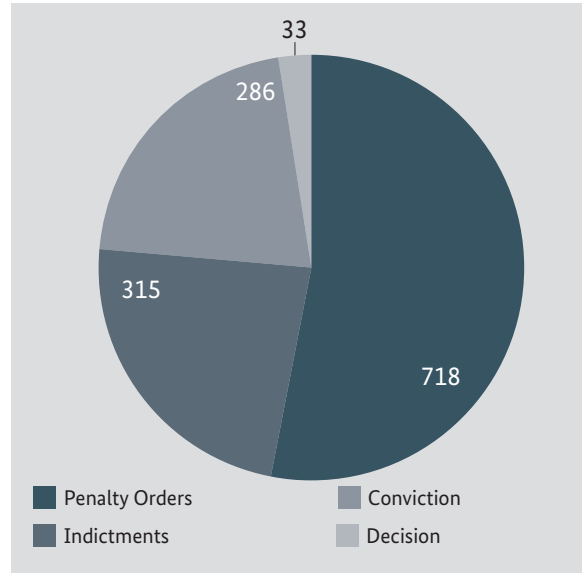


Figure 8: Overview of the Convictions, Penalty Orders, Decisions und Indictments

The number of received decisions increased disproportionately from two in the previous year to 33 in 2021. In this connection, it was possible to seize cash amounts of over EUR 280,000 which stemmed from an illegal activity and for which the person in question could not be prosecuted or convicted for the underlying crime.

Illegally obtained assets were confiscated in around 700 cases overall.

If a conviction was coupled with a fine, its average amount was roughly EUR 2,200. In 54 cases, the conviction entailed custodial sentences, with 25 cases on probation. Custodial sentences (without probation) totalled an average of 16 months.

A fine was also usually imposed by penalty order. This totalled an average of EUR 2,800. In 49 cases, custodial sentences were imposed by penalty order,

with 31 cases on probation. Custodial sentences (without probation) by penalty order totalled an average of 8 months. In 25 cases, cautions were issued, with fines reserved during a probationary period.

Around 75% of all convictions, penalty orders and decisions in feedback reports involved a conviction for committing subsidy fraud. This is primarily associated with emergency aid, as in the previous year, which was granted on account of the corona pandemic. Intentional money laundering crimes accounted for 10% of these feedback reports.

Temporary Freezing Orders

The possibility of issuing a temporary freezing order gives the FIU an important and effective means to prevent money laundering or terrorist financing. If there are clues that suggest a transaction is related to money laundering or terrorist financing, the temporary freezing order can be used to prohibit the execution of the transaction for up to 30 days. This lets the FIU analyse the transaction until it reaches a final assessment of the reason without letting incriminated funds be removed from the state's area of influence by cash withdrawals or transfers. The need to execute a temporary freezing order is carefully considered in each individual case. In 2021 the FIU ordered a total of 48 temporary freezing orders (2020: 14). Transactions with a total volume of roughly EUR 19 million (2020: EUR 1.4 million) were frozen. 11 of the 16 total national temporary freezing orders showed evidence of concrete facts after further analysis, leading to dissemination of the reason to the competent authority.

The option of issuing a temporary freezing order can also be used in international cooperation with foreign FIUs. In 2021 the FIU successfully issued a total of 32 temporary freezing orders with a transaction volume of around EUR 4 million on account of information received from foreign partners.

In regard to terrorist financing or state security, there were three temporary freezing orders in total. They accounted for a total transaction volume of around EUR 1.3 million. Two of the underlying reasons were disseminated to the responsible law enforcement agencies.

Case Study – Temporary Freezing Order¹³

Received Suspicious Transaction Report

A person initiated the transfer of a five-figure amount to Türkiye via an association account. The reporting entity checked the transaction circumstances and determined that the account held there was recently used as a donation account for a Salafist association, against which the Federal Ministry of the Interior and Community had already initiated proceedings to ban the association. The association's activities were directed against the ideas of international understanding and constitutional order, and contrary to the criminal laws. Furthermore, parallel to the proceedings to ban the association, the Office of the Attorney General had initiated criminal proceedings for suspicion of terrorist financing in accordance with Section 89c of the Criminal Code (StGB). The association switched the donation account used for this and the bank multiple times due to the prosecution pressure from the authorities. This led to the submission of an STR as a so-called "urgent case" (Fristfall) to the FIU.

FIU's Analysis and Dissemination

The FIU issued a temporary freezing order for the account in question on that very day due to the connection to what appeared to be a misused association. In its analysis, the FIU was able to trace the acting persons and their transaction trails to establish an actual connection between the association targeted in the ban and criminal proceedings for the association and its responsible members. When the temporary freezing order was issued, it was determined that donations of over EUR 320,000 were received in the account as a result of more than 500 individual transactions by various persons. Furthermore, a total of eight requests for information were sent to FIUs outside of the European Union to obtain additional information on the use of the funds. Multiple central agencies then shared information that suggested the funds were not being used solely for humanitarian purposes. After assessing the overall reasons, it could not be ruled out that the funds were being forwarded following a certain system and possibly used for terrorist financing. The analysis report with the previously described research results was then disseminated in close coordination with the competent state office of criminal investigation (LKA). The seizure and confiscation of the assets, which in the meantime had grown to over EUR 600,000, was seamlessly ordered by the court.

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

Proliferation Financing

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

In the context of proliferation, embargoes in place against high-risk countries cause them to acquire and distribute such goods by concealing, for example, the transport routes or trails of money via unsuspecting, but now known third countries. Other possible means of circumventing export controls are, for example, the involvement of companies, persons or state institutions (e.g., universities) that are free from suspicion as recipients for a delivery.

Proliferation-relevant deliveries cannot usually be identified solely on the basis of observing technical criteria. This is due to the fact that products involving key technologies can have both military and civil potential uses (see, inter alia, the EU Dual Use Regulation¹⁴).

Indications of proliferation, proliferation financing or violations of existing embargo regulations or the EU Dual Use Regulation come from STRs

submitted by reporting entities and also communications from intelligence services and notifications from foreign agencies. In comparison to combatting money laundering, the movement of goods and the transaction routes are of particular importance in the fight against proliferation. The FIU is in close contact with the Customs Investigation Service and in particular with the Customs Criminological Office in connection with the analysis of individual transactions. To prevent and combat proliferation and its financing, there are international standards that are aimed at detecting or preventing the proliferation or transfer of such goods, technologies and know-how.

Despite strict export controls, Germany can be a target of acquisition efforts by high-risk countries. The processing of the transactions and thus the disguised transaction routes associated with this are diverse and subject to constant changes to circumvent export control procedures. The analysis of STRs and especially the financial trails contained in them thus serve - besides already existing export control procedures - for detecting proliferation activities and violations of embargo requirements at an early stage.

In 2021, 50 STRs with a connection, among others, to countries such as Iran, North Korea, Pakistan, Syria, Belarus and Russia and indications of possible proliferation, embargo or sanction-violating activities were transmitted to the FIU. In the previous year, 34 STRs were received.

¹⁴ The EU has adopted Regulation (EU) 2021/821 (EU Dual Use Regulation) for all Member States, thereby stipulating common approval obligations and procedures for the export, brokerage, technical support, transit and transfer of dual-use products. This involves, for example, chemicals, but also software and technologies.

Transactions

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

A single STR does not necessarily have to contain just one transaction. It can also report on a number of different transactions. This leads to a discrepancy between the number of total incoming STRs and the number of transmitted transactions in total. In 2021 the FIU received reports on around 958,000 suspicious transactions (2020: around 481,000). In comparison to the previous year, this equates to a near doubling of the reported transactions, which is roughly consistent with the rise in STRs received.

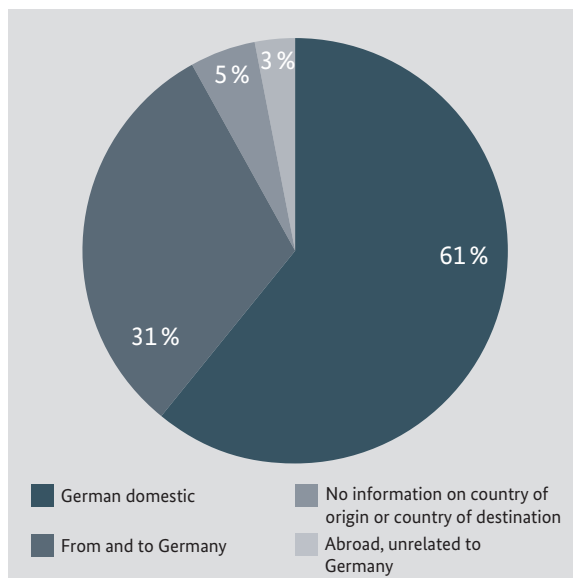


Figure 9: Foreign Involvement in Suspicious Transactions

The share of German domestic incidents as a percentage of all transactions rose to approximately 61% in 2021. This share was around 50% of all transactions in the previous year. By contrast, the share of transactions that have solely Germany as the country of origin or destination declined slightly to 31%. Approx. 3% of all transactions are purely international, as Germany is listed as neither the country of origin nor as the country of destination. This can, for example, be the case for correspondent banking activities in which the reporting credit institution is a reporting entity in Germany but acts exclusively as a service provider for settling cross-border transactions. 5% of the transactions were not possible to assess in terms of the country of origin or destination.

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

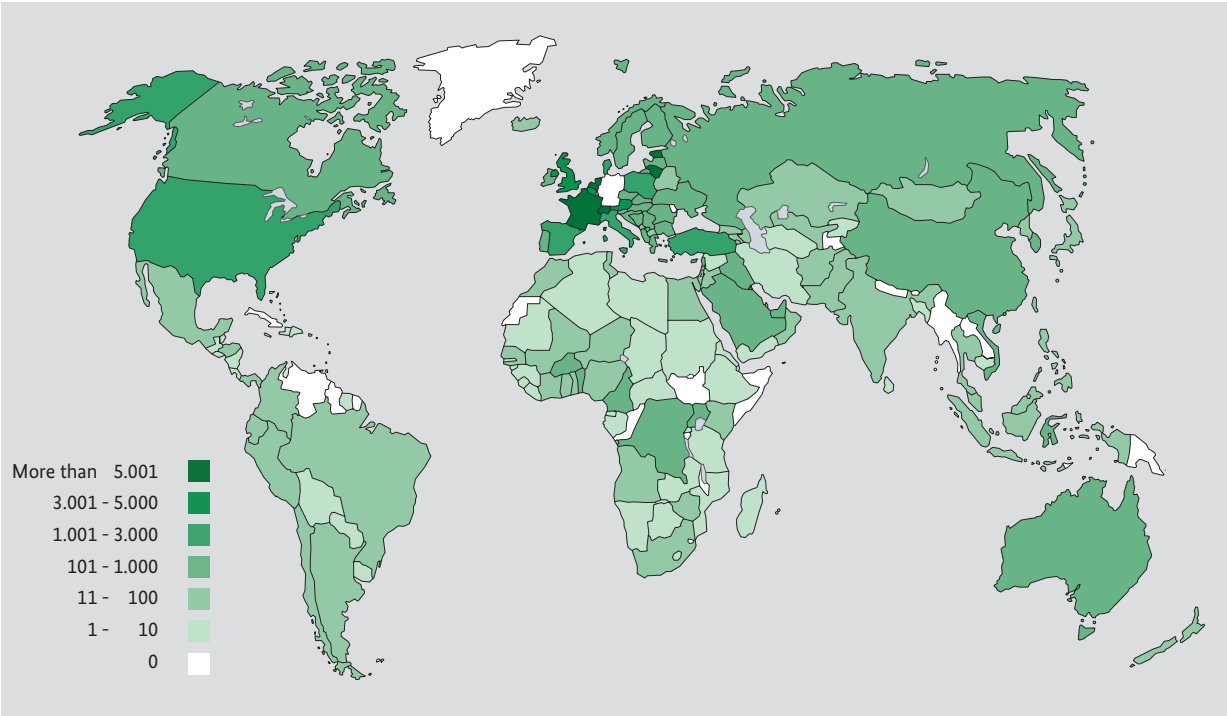


Figure 10: Number of Suspicious Transactions by Country of Origin

A total of more than 104,000 suspicious transactions with Germany as the country of destination were received in 2021. This equates to an increase of 140% compared to the previous year. When the transactions are considered by countries of origin, the Netherlands with over 28,000 transactions, Switzerland with over 11,000 transactions and France with over 9,200 transactions stand out in particular. As in the preceding years, suspicious

transactions that had Germany as their destination come primarily from countries in the EU, the UK, Türkiye and the major economies of China, Russia and the USA. Conspicuous changes were additional increases in the number of suspicious transactions from Lithuania (rising more than six-fold to over 6,600 transactions) and Estonia (more than tripling to almost 8,500 transactions).

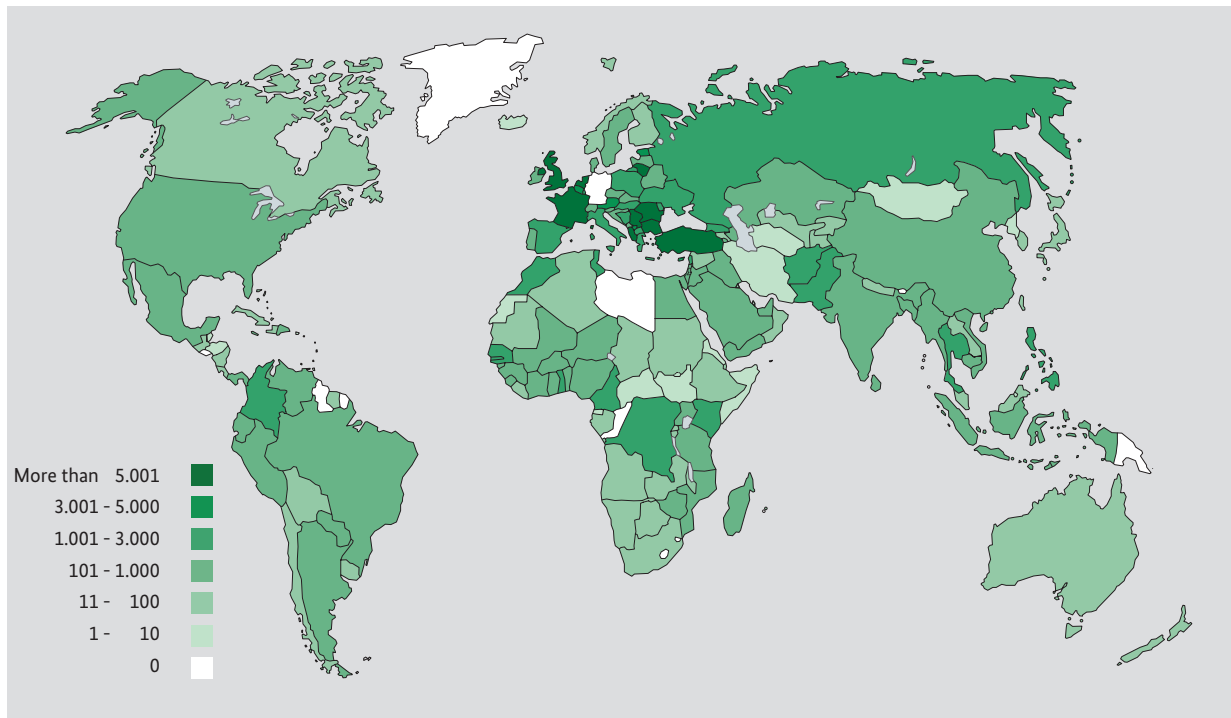


Figure 11: Number of Suspicious Transactions by Country of Destination

The number of outgoing transactions from Germany to other countries reported as suspicious totalled 203,000 and was around 52% above the previous year. The focal point of the suspicious transactions originating in Germany continues to be, as in previous years, Türkiye as the country of destination (over 29,000 transactions). Besides the Netherlands (just under 16,200 transactions),

France (over 9,000) and the UK (around 7,300), the countries in eastern Europe also play a major role. Bulgaria (around 9,200), Romania (just under 8,600) and Albania (around 6,900) are three eastern European countries that fall in the top 10. There were also sharp increases in transactions to Malta (around 6,300), Lithuania (just under 6,000) and Cyprus (around 4,800).

Typologies and Trends

Description and Continuation of Key Risk Areas

Special Topic COVID-19

Focus on Real Estate

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

Focus on the Use of New Payment Methods

Assessment of Reports on Cash Discoveries

Typologies and Trends

Description and Continuation of Key Risk Areas

All information received by the FIU – especially STRs in accordance with Section 43, 44 AMLA – is continually assessed on a risk basis to determine whether it requires further analysis in terms of the FIU’s core statutory mandate. STRs received are matched largely automatically to certain data sources or databases at the beginning of the analysis process and in part automatically prefiltered on the basis of defined key risk areas (risk-based approach, RBA). Artificial intelligence is also used to support this. Reports initially not filtered out in the course of this process remain alongside the reports analysed on a risk basis during the so-called monitoring phase and are continuously compared with the FIU’s newly received information. In this

way, they are always included in the analysis process and repeated assessments are made available.

The key risk areas applied include both sector-related and phenomena-related risks. Fundamentally, a difference is made between the areas of money laundering and terrorist financing, although a common key risk area is set with the use of new payment methods as a result of new technologies.

Key Risk Areas Regarding Money Laundering



Real Estate

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



Use of Cash (when procuring high-value goods)

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



Trade-Based Money Laundering

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



Games of Chance/Betting

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



Figure 12: Key Risk Areas of the FIU

The key risk areas introduced are continuously checked by the FIU in light of crime developments in Germany and on a case-by-case basis to ensure their applicability as a steering and prioritisation

instrument. This lets the FIU make the required adjustments at any time to have an immediate effect on the operating analysis activity.

Adjustment of Analytical Processes for Simple Cases of Fraud

In coordination with the appropriate law enforcement agencies, the FIU introduced a simplified analytical process for simple cases of fraud in particular at the beginning of 2021, as the understanding of crime has evolved.

If a potential “simple” case of fraud or another crime is detected where its underlying reason is less complex, the case is handled in a simplified process to ensure quick dissemination to the responsible law enforcement agency. Expressly excluded from this

are all reasons that may be allocated to the existing key risk areas.

In this way, over 23,800 analysis reports were disseminated in 2021. Of these, over 17,800 reports were disseminated after a simplified process.

Special Topic COVID-19

In terms of the development of crime, the second year of the pandemic was defined by a continuation of crime patterns already known from the previous year. These cases involve fraud in connection with the application and payout of various aid funds or with fictitious offers for safety masks and other medical products in particular. In isolated instances, however, new cases of fraud were detected where the changes in the procedures for the application of government support services and changes in strategies and resources to cope with the pandemic were systematically exploited.

However, the number of reports that were potentially related to COVID-19 decreased significantly overall in comparison to the previous year. As a result of the numerous cases of fraud in connection with the emergency aid programmes in 2020, the obligations to provide proof for the recipients of state subsidies such as the interim aid and the new start-up aid were made more stringent. Especially the required inclusion of an “auditing third party” such as a tax consultant or auditor and the audits by the granting agencies ensured substantially better control.

Nevertheless, a number of cases associated with systems of fraud were reported in 2021 – in part also on account of downstream systematic analyses of reporting entities in the financial sector. Examples include reports related to billing fraud via corona testing centres. For example, some companies tried to set up an alternative activity by erecting testing centres when the free “citizen tests” (Bürgertests) were introduced. This was especially the case with companies that experienced particular economic hardship during the pandemic, such as companies in the gastronomy and event industry. Since the establishment of these centres and the associated operational processes took place under time pressure, effective controls with regard to tests actually carried out did not exist at first and the activity promised a lucrative opportunity for income, this provided scope for corresponding

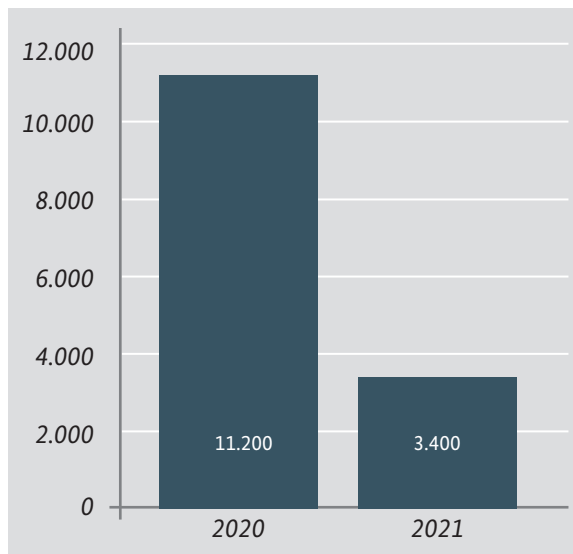


Figure 13: Received Suspicious Transaction Reports with Reference to COVID-19

billing fraud at the expense of the health insurance funds or the health care system. When analysing STRs, the FIU noticed both persons who had actually suffered from revenue losses due to the pandemic and persons who had already come to light due to other offences and for whom it can be assumed that opportunities for fraudulent activities were systematically used.

Relative to the previous year, however, both reporting entities and authorities were more aware of the situation and able to react at short notice, identifying any gaps in processes and review procedures. The FIU’s published typologies paper on COVID-19 and its annexes were modified in regards to the change in payout modalities.

The exchange between the involved authorities, ministries and payout offices was also strengthened by setting up a “task force” at short notice, which the FIU was also involved in. This task force conducted a systematic audit of the steps in the application and payout process for subsidies to counter possible cases of fraud by preventing them. In this cooperation, it was learned, among others, that individual cases of identity theft had occurred at “testing third parties”.

Case Study – Billing Fraud with Corona Testing Centres¹⁵

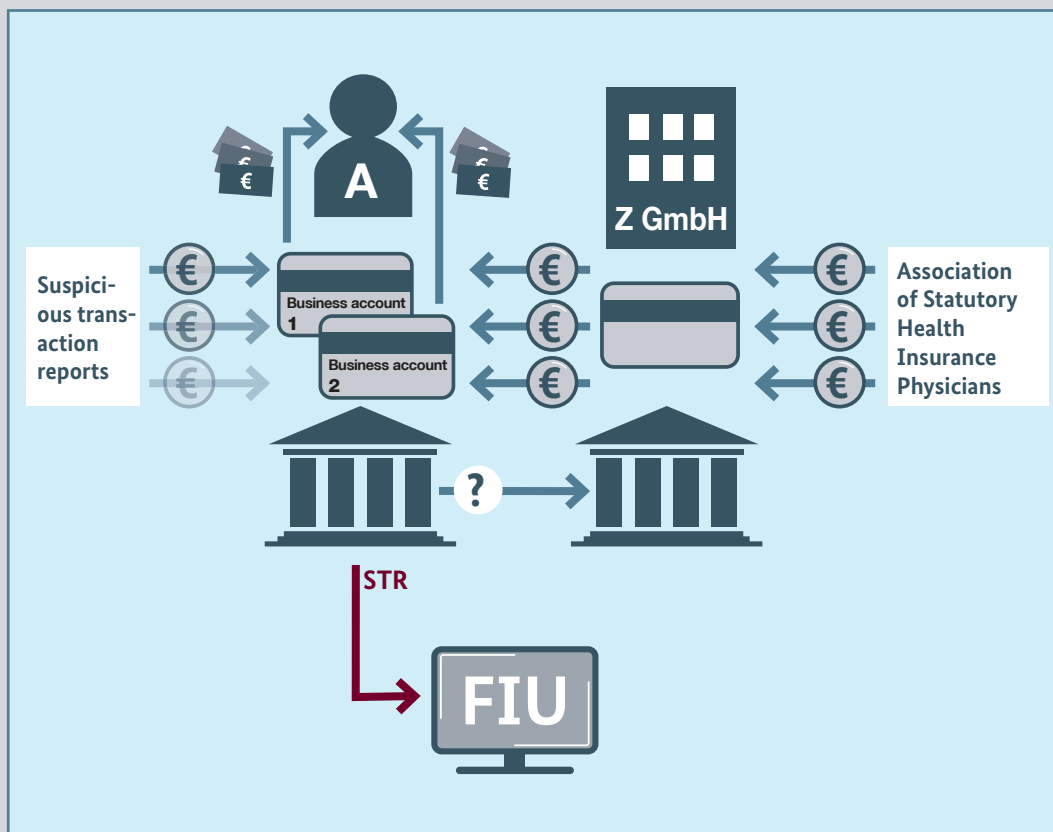


Figure 14: Case Study – Billing Fraud with Corona Testing Centres

Initial STR

A credit institution reports a business relationship with person A due to high cash withdrawals and deposits that cannot be traced. Person A has multiple business accounts for different businesses in the service sector. The account management had shown suspicious activity multiple times in the past, since the credit transactions were almost exclusively offset by high cash withdrawals on the debit side. The cash withdrawals totalled multiple millions of euros. The client’s use of funds and business activity could not be traced in the past. At that time, an STR was submitted.

¹⁵ The present case study is a real case from the FIU’s practice.

The account activity became suspicious again, when multiple millions of euros were received in multiple tranches in one of the business accounts within one day. The funds received all had the same sender, Z GmbH. An enquiry sent to the institution where Z GmbH held its account revealed that the millions there had been received for operating a corona testing centre.

Several hundred thousand in euros were withdrawn immediately in cash from this money that had been received in the business account of A. Another cash withdrawal of a low, single-digit million amount was announced.

The high amounts of money received, which had no identifiable connection to the business purposes of person A, and the high cash withdrawal announced caused the matter to be forwarded to the FIU as an “urgent case” (Fristfall). Furthermore, there was the suspicion that the funds of Z GmbH came from billing fraud in connection with the operation of corona testing centres.

FIU’s Analysis and Dissemination

The FIU performed an analysis and determined that person A had a criminal background in the past. Furthermore, person A was able to be brought in connection with other STRs, suggesting a possible connection to a clan milieu. The analysis report with the previously described research results was then disseminated to the competent state office of criminal investigation (LKA).

There were also isolated reports in connection with the falsification of vaccination cards and various kinds of fraud related to vaccines. Even though relevant reports were disseminated to law

enforcement bodies in each case, there was no indication so far that the cases involved larger networks of fraud or a mass phenomenon.

Flood Relief

Similar to the corona pandemic, the flooding disaster in Rhineland-Palatinate, North Rhine-Westphalia and Bavaria also had the potential for fraudulent activities in the summer of 2021.

For this reason, the STRs received after the flooding in Rhineland-Palatinate, North Rhine-Westphalia and Bavaria during the summer were reviewed in light of the experiences with regard to the government support programmes offered during the pandemic to see whether similar crime patterns could be identified here, e.g. with regard

to the granting of government aid money. The analyses by the FIU showed that applications were primarily filed by persons who did not reside in the disaster area. In isolated cases, these persons had already generated suspicion in connection with illegal enrichment from corona emergency aid. Furthermore, flooding aid was paid out to illegitimate third parties. In multiple cases, applications were filed with account details that did not belong to the (fraudulently acting) applicant in order to circumvent the applicant’s account from being seized in the event of discovery. The funds were

then withdrawn in cash. Furthermore, there were case constellations in which multiple applications were filed for the same subsidy object.

A special aspect of flood disaster fraud was that some individuals used this opportunity as a pretext for depositing funds or assets in newly opened bank accounts. The affected persons had allegedly stored assets in safes at other banks and lost some of them due to the flooding there or now had to store them elsewhere due to the flooding. Proof of where the assets ultimately came from could not be provided.

Furthermore, isolated, allegedly aggrieved persons brought damaged banknotes to the bank, sometimes in large quantities. The money was said to have been hoarded at home or in a bank safe of another bank. The origin of the funds could not be plausibly explained in these cases either.

Fundamentally, the number of such reports in comparison to the reports in connection with corona emergency aid were low, however.

Flood Relief

In order to overcome the emergency after the flooding disaster and satisfy the most urgent needs, immediate financial aid was promised to the affected parties. The federal government contributed half of the emergency aid to the affected states, initially up to EUR 400 million. A total of up to EUR 800 million was available for emergency aid.

The emergency aid was supposed to be paid out to the affected parties quickly and unbureaucratically. The application was submitted at the resident's municipal office and granted without an extensive review. When an application was submitted, it was sufficient to provide credible proof that the main residence was in the flooded area and a self-declaration by the damaged party stating that there was damage of at least EUR 5,000 in the household. In Bavaria, proof of the use of the emergency aid also had to be provided. A check of whether the claims were actually legitimate was supposed to take place afterwards.

Terrorist Financing and Other Crimes Relevant to State Security

The FIU also observed in the second year of the corona pandemic how the exceptional situation was being used by extremist groups to generate financial resources for their organisations. The groups primarily made use of social media to place their topics and generate financial resources accordingly. For example, they requested donations or called for persons to support groups by becoming fee-paying members. Offered payment routes were often classical bank transfers or the option of donating via a so-called crowdfunding platform or with virtual assets.

In the phenomenon area of Islamism, the groups called for donations to help crisis areas abroad that were particularly affected during the course of the pandemic. Associations known from the same context and also individuals tried to obtain state corona emergency aid in a presumably fraudulent manner. The FIU has isolated reports from reporting entities in the context of corona emergency aid fraud related to this phenomenon area. Furthermore, the parties reported on were already known due to corresponding activities in the scene and donation payments in other connections.

Since the beginning of the pandemic, persons and organisations from the so-called “Querdenker” (alternative thinker) scene tried to mobilise against the measures of the federal government to fight the corona pandemic. However, the large number of persons who cannot be classified as radical or extremist in principle also include an increasing number of adherents, especially of potentially anti-Semitic conspiracy theories such as “The Great Reset” or “QAnon”, but also of anti-democratic narratives, and individuals from right-wing extremist groups as well as so-called “Reichsbürger” (Reich citizens) or “Selbstverwalter” (self-administrators). The entire protest scene

is characterised by strong ideological heterogeneity, making it hard to match participants to one of the groups previously defined by the Federal Office for the Protection of the Constitution (BfV). It also became substantially more radical with the expansion of restrictive measures and showed increasing potential for violence.

However, the anti-democratic and state-delegitimising tone of these demonstrations unites the protest scene, which is why the Federal Office for the Protection of the Constitution defined a new phenomenon area called “Delegitimation of the state relevant to constitutional protection” in April 2021. The new nationwide collective observation object designated “Delegitimation of the state that is hostile to democracy and/or endangers security” contains individual, particularly relevant protagonists in the “Querdenker” movement. Neither the “Querdenker” movement as such nor the protest scene in general were observation objects of the Federal Office for the Protection of the Constitution in the reporting period.

The FIU has more than 40 STRs from the reporting year on this new phenomenon area, mostly related to donation payments and also frequently under the pretext of a “gift” to known individuals in the so-called “Querdenker” scene. In part, these funds are held in cash, used for paying down own credit or bills, transferred to other accounts, in part abroad, or converted to virtual currencies.

Focus on Real Estate

The significance of the real estate sector for money laundering activities was also a special focus of the FIU in 2021. The unchanging dynamic development of prices on the real estate market and low interest rates on the capital market continued to make the real estate sector highly attractive for investors of all kinds, including money launderers. In connection with constantly rising purchase prices and rents, especially in large cities, and the lack of affordable residential space, it appears more necessary than ever to ensure that real estate is not misused as an object for money laundering.

Assignment to the key risk area of real estate ensures that STRs related to real estate transactions are always prioritised in terms of handling. Furthermore, the reports are analysed for the detection of new typologies to provide appropriate information in exchanges with reporting entities and law enforcement agencies, among others as part of the AFCA working group called “Money Laundering in the Real Estate Sector” (Geldwäsche im Immobiliensektor). This enables the ways of committing crimes to be updated, putting the reporting entities in the position to identify actions that must be reported even more systematically.¹⁶

Amendments to the Law to Improve Transparency regarding Beneficial Owners

The possibility of misusing real estate for money laundering or concealing the beneficial owner for real estate companies was reduced by amendments to the law in 2021.¹⁷ Since 1 August 2021, foreign companies must report the beneficial owner to the Transparency Register (Transparenzregister) if they hold a stake in a company with property in Germany. The Transparency Register was expanded from a collection register to a full

register, and the conditions for avoiding the real estate transfer tax by means of “share deals” were made more stringent by lowering the shareholding threshold from 95 to 90 percent and extending the holding period until possible resale from five to ten years. These measures make a contribution to improving transparency and thus also combating money laundering.

¹⁶ For more details on the AFCA, see the explanatory remarks on “Public-Private Partnership – AFCA” in the “National Cooperation” section.

¹⁷ Act on the European Interconnection of Transparency Registers and on the Implementation of Directive (EU) 2019 / 1153 of the European Parliament and of the Council of 20 June 2019 on the Use of Financial Information for the Purpose of Combating Money Laundering, Terrorist Financing and Other Serious Criminal Offences (Transparency Registers and Financial Information Act) (BGBl. I, p. 2083).

Ordinance on Matters in the Real Estate Sector Subject to Reporting under the Anti-Money Laundering Act (GwGMeldV-Immobilien)

The Ordinance on Matters in the Real Estate Sector Subject to Reporting under the Anti-Money Laundering Act (GwGMeldV-Immobilien) entered into force on 1 October 2020 and also showed its impact in 2021. The Ordinance specifies the reporting obligations for certain professional groups such as professions involving legal consulting. Transactions in connection with real estate that exhibit suspicious characteristics possibly related to money laundering are to be reported to the FIU by these professional groups. In addition to a significant increase in the registration figures for reporting entities, the number of reports submitted by the reporting entities in accordance with Section 2 (1) No. 10 and 12 AMLA also stabilised on a high level at over 500 STRs per month. Toward the end of the year, the number increased again to more than 600 reports per month. These reports are regarded as especially valuable when viewed together with reports submitted by other reporting entities.

The analysis of the reports submitted by the reporting entities in legal advisory and tax consulting professions showed that repeated factual constellations make up the overwhelming majority of the total number of STRs for this group of reporting entities.

In terms of the frequency of the underlying reasons for the reports, the following should be emphasised in particular:

- the purchase price was paid in whole or in part before the conclusion of the legal transaction and the amount exceeds EUR 10,000 (Section 6 (1) No. 3 GwGMeldV-Immobilien),
- the real estate was resold within three years after the preceding acquisition at a price that substantially deviates from the previous price without an understandable reason being provided for this (Section 6 (2) No.1 GwGMeldV-Immobilien),
- the full price or parts of the price were paid by third parties or to third parties (Section 6 (1) No. 4 GwGMeldV-Immobilien),
- the purchase price payments were made in cash (Section 6 (1) No. 1a GwGMeldV-Immobilien) and
- the transactions exhibit a connection to risk countries (Section 3 (1) GwGMeldV-Immobilien).

The corresponding reports did not necessarily all have a background relevant for money laundering, but especially the incomprehensible or lacking explanations for specific actions and transactions and the simultaneous presence of multiple clues suggested that the reports should be subject to an in-depth analysis.

Case Study – Real Estate¹⁸

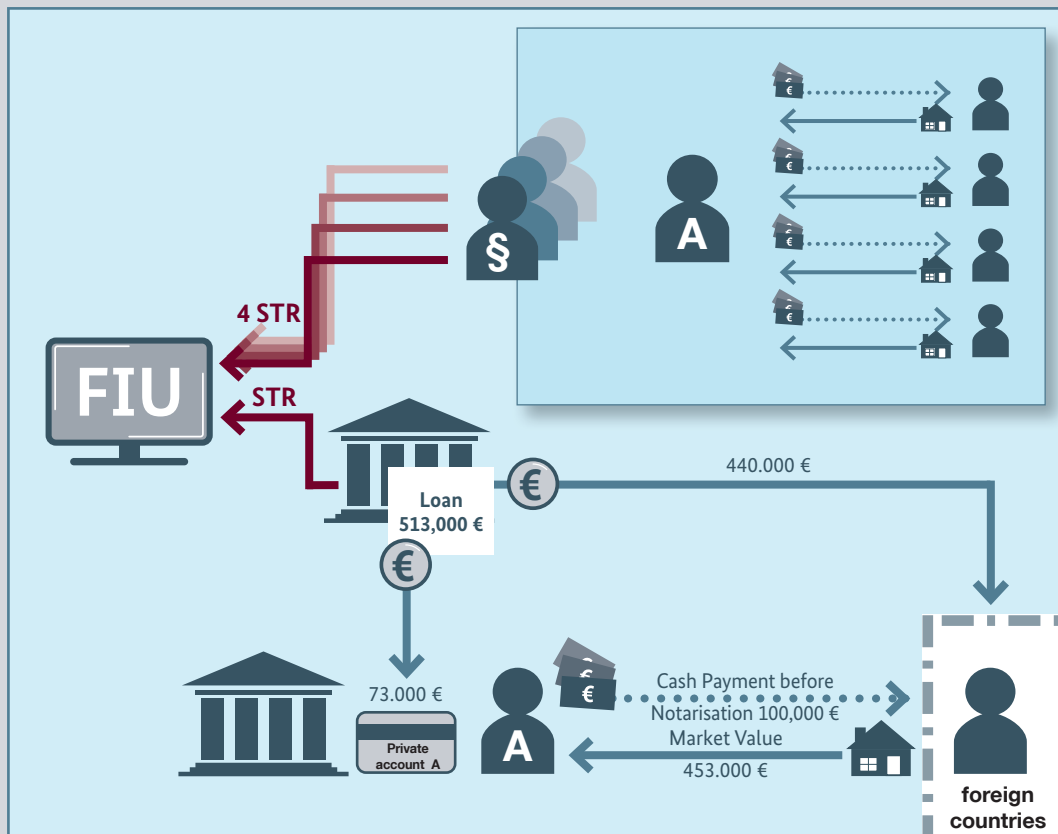


Figure 15: Case Study – Real Estate

Initial STR

A credit institution reported a real estate purchase by person A. The reporting entity reported that A financed the purchase of a flat with a total purchase price of EUR 540,000 by means of a loan for EUR 513,000 from the bank. On the due date for the purchase price, A informed the bank that he had already paid the seller, at the request of the seller, EUR 100,000 in advance. The seller, however, has already moved abroad so that his statement can no longer be checked. EUR 440,000 of the loan itself was paid out to the seller. The client has the remaining, still available loan amount of EUR 73,000 transferred to his own account at another bank.

In the assessment by the reporting entity, the market value for the flat is determined to be EUR 453,000. The purchase price for the property was thus EUR 87,000 above the value of the property as determined by the appraiser.

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

Furthermore, A initially stated that he wanted to occupy the property himself. However, the acquired flat was now rented out by A. In the meantime, the credit institution had refused another financing request by the client.

FIU's Analysis and Dissemination

The FIU analysed the case and determined that there were four other STRs for person A. Different notaries had each reported real estate purchases by A. The notaries reported cash advance payments for flats that were made before the drafting of the purchase and sale agreement and thus before certification by the notary.

The collating of the STRs from the various notaries and credit institutions made it possible to discover the unusual business activity of A. It was determined that A had acquired real estate with a value of over EUR 2.6 million within a period of six months. He had made cash advance payments of EUR 630,000 before the conclusion of the purchase and sale agreement and certification. Person A had completed each transaction according to the same pattern: A loan granted for the financing of a real estate purchase was transferred by A only in part to the seller and the remaining amount was transferred to another account. The purchase price of the real estate was much higher than the market value. The report on these facts was disseminated to the competent law enforcement agency.

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

Public sector taxes, charges and duties are the bedrock of every political system. This is how the Federal Republic of Germany covers its financial needs, mainly in the form of tax revenue. Violations of tax law such as tax evasion and avoiding duties prevent the community from having the proper financial base. Even if it is difficult to quantify illegally evaded taxes, the cases settled by tax investigation authorities in 2020 throughout Germany – where evaded taxes of EUR 3.3 billion were discovered – suggest the order of magnitude of the amount evaded.¹⁹

When funds obtained from tax offences are reintroduced into the legal economy and financial system, this can fulfil the criteria for money laundering. Therefore, the key risk area of serious (tax) criminal acts ensures that reports and notifications received and exhibiting a potential connection to tax crime are given priority in terms of handling.

In the reporting year, just under 3,600 STRs and notifications from reporting entities, supervisory authorities and fiscal authorities were assigned to this key risk area. The steady increase in the number of STRs received on this key risk area has

The new version of Section 261 of the Criminal Code, which took effect on 18 March 2021, and the related abandonment of a selective catalogue of predicate offences (all-crimes approach) also have an impact on the assessment of tax evasion as a suitable predicate offence to money laundering. The characteristic of commercial or clan-like evasion, as required in the old version of Section 261 of the Criminal Code, is no longer a necessary requirement. However, the previous expansion for certain tax offences contained in the old version of Section 261 (1) (3) of the Criminal Code no longer applies so that especially expenses that were saved through tax evasion are no longer a suitable object of the offence of money laundering.

been seen since the introduction of the risk-based approach and clearly continued over the course of 2021. Of these, 94.8% were attributable to the reporting credit institutions, while 1.6% were received from fiscal authorities.

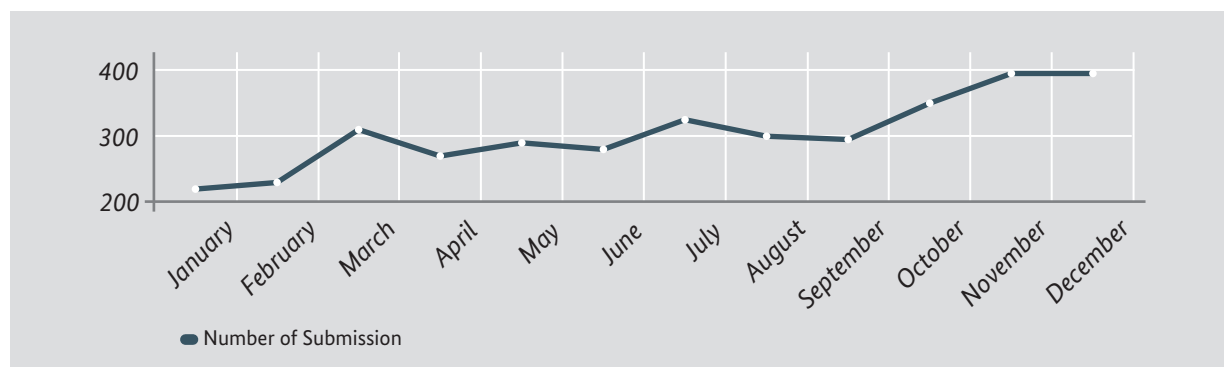


Figure 16: Total Number of Reports and Notifications in the Key Risk Area of Serious (Tax) Criminal Acts

19 See Federal Ministry of Finance (BMF) Monthly Report October 2021, p. 39 et seqq.

In almost every fifth report or notification, the reporting entities found an unusually high cash payment or cash withdrawal and in 5% of the reports an unusual cash payment in business transactions. The origin of the funds was referred to as unknown in more than a quarter of the reports.

The value-added tax was named most frequently as the type of tax in the reasons of the STRs. References to possible carousel fraud were also frequently observed in the information transmitted to the FIU in connection with the terms value-added tax, sales tax or input tax.

Excursus – Carousel Fraud

“Carousel fraud” to evade value-added tax (VAT) is a common form of tax evasion in the EU that has been engaged in for years and involves a large number of companies with their registered offices in different EU Member States.

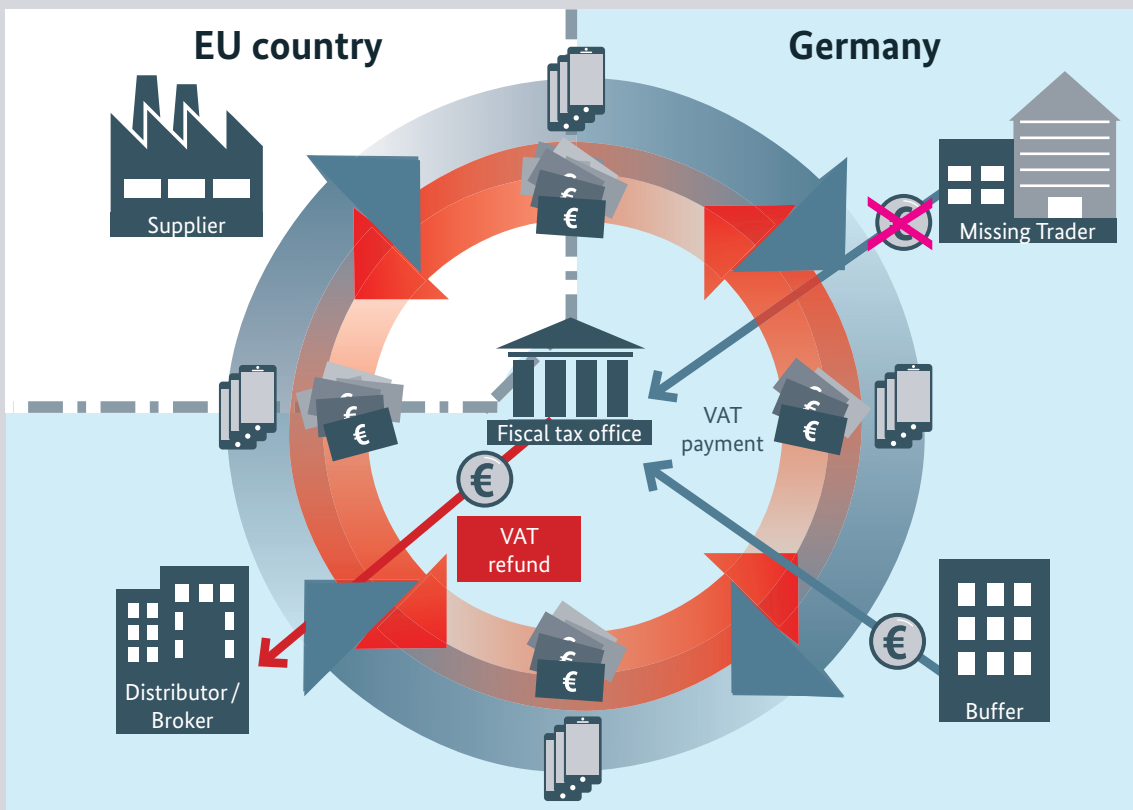


Figure 17: Simplified Representation of a VAT Carousel

Basically, small, but high-priced consumer goods are resold in a circular system. It begins with a supplier located in the EU abroad; the goods then pass through at least three actors located in the EU and then return to the supplier. The process is designed quickly so that as many goods as possible can pass through the carousel or the carousel can be completed as frequently as possible before detection by the tax investigation authorities. Depending on the design, value-added taxes incurred in different ways in this carousel are not paid in full or only in part and, overall, unjustified VAT refunds are obtained.

The possible range of designs makes it impossible to assess in general whether and where assets are obtained that could be the subject of money laundering.

In an intra-Community delivery according to Section 4 No. 1b of the VAT Act, the goods are initially sold by the above mentioned supplier in the EU abroad to the so-called missing trader based in the EU without the supplier billing the missing trader for the VAT. By buying the goods, the missing trader is obligated to pay the VAT to the fiscal tax office. An input tax deduction is possible, however. The rule has been in place since the elimination of border controls between the EU Member States in 1993 and is intended to ensure that the VAT is paid exclusively in the Member State of consumption.

The actual abuse begins with the resale to a second recipient, the so-called buffer. The missing trader sells the goods and disappears from the market with the VAT paid by the buffer. From then on, he is “missing”. The owed payment of the VAT to the responsible fiscal tax office is not made – it is evaded.

The subsequent sale by the buffer to the so-called distributor/broker is usually completed in accordance with the law. The VAT incurred is paid to the fiscal tax office. This transaction is generally intended to conceal the carousel fraud.

Finally, the goods are sold by the distributor/broker back across the border to the supplier located abroad in the EU. The distributor/broker paid the VAT upon purchase of the goods, but does not charge the supplier for this in turn when reselling the goods in an intra-Community delivery. He receives an input tax refund. This means that besides the supplier, the missing trader and usually the distributor/broker are involved in the plan to ensure that the transfer cycle of goods is closed and the carousel keeps turning.

The method described here is carried out in such a short period of time that the profiting companies no longer exist by the time the fiscal tax office attempts to collect the VAT. The tax losses for the European Member States resulting from this intra-Community VAT fraud are estimated to be in the doubledigit billions.²⁰

To prevent tax investigation authorities from discovering the carousel fraud, it is usually concealed with a complex network of companies. Furthermore, the origin of the goods is concealed with both fake and cover invoices. In addition, multiple buffers can be lined up in sequence or integrated parallel to each other. This makes the discovery process more difficult for the authorities and gives the fraudsters time for more illegal revenue. The involvement of companies without their knowledge is also intended for concealment: already existing companies without a criminal past do not draw the direct attention of the tax investigation authorities.

Indications of carousel fraud include high revenues shortly after the establishment of a company and a frequent change in the registered office or management of the company. Furthermore, high VAT refunds, cross-border trade and high as well as even sales amounts can also be signs of carousel fraud. In addition, companies involved may exhibit abnormalities due to a lack of warehouse capacities in the case of a warehouse-intensive business model, for example. Besides small, but high-cost consumer goods, other goods and rights are also misused for carousel fraud. Vehicle trading as well as emissions rights trading can be listed here as examples.

²⁰ See Federal Court of Audit (Bundesrechnungshof), Report on Measures to Improve the Fight against VAT Fraud – Using the Opportunities of Digitalisation, 2020, p. 9 et seqq.

Case Study – Carousel Fraud²¹

Initial STR

A reporting entity in the financial sector reported the accounts of two corporations at the beginning of 2021. The legal representatives and beneficial owners of the organisations were identical. Both accounts came to the attention of the reporting entity on account of suddenly received payments of millions and the immediate forwarding of these to the European abroad. The purposes of the companies largely suggested trading in electronic products. Other sales typical for business were not evident. In a follow-up report, the FIU was informed a little later that transfers of over one million euros had initially been stopped in the European abroad.

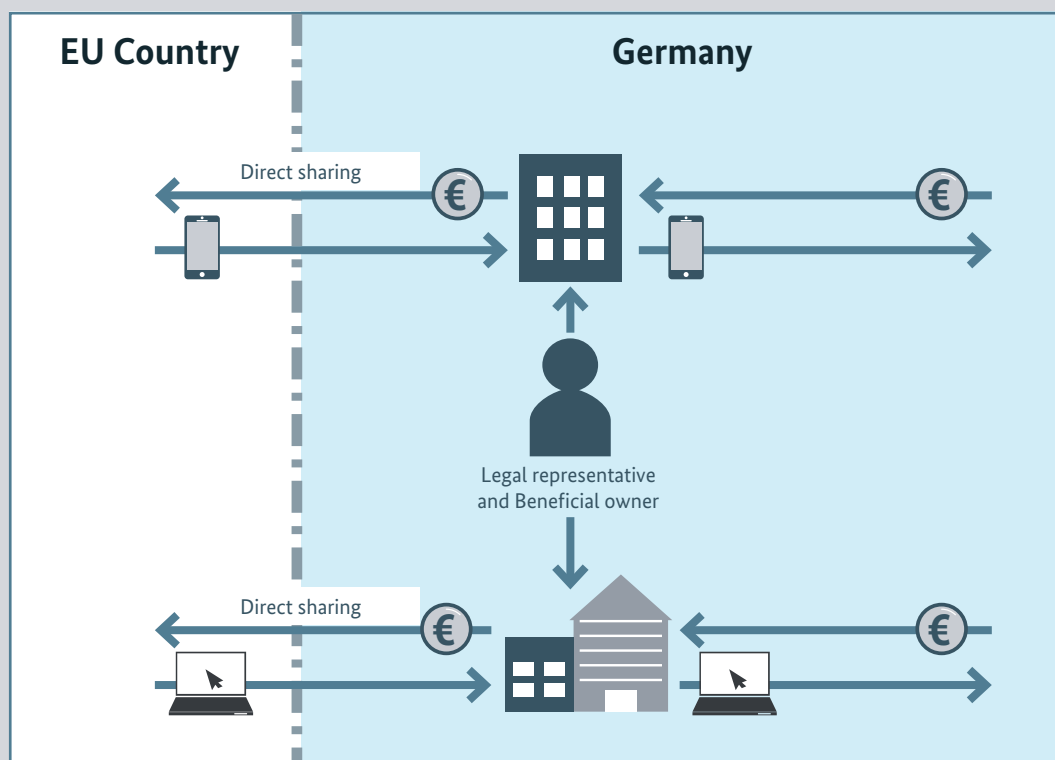


Figure 18: Case Study – Carousel Fraud

FIU's Analysis and Dissemination

To analyse the transactions, the FIU issued a temporary freezing order²² and locked the accounts of the reported organisations for any outgoing payments. During the subsequent analysis, the FIU became increasingly convinced of its suspicion that the reported organisations were part of a carousel fraud. The analysis of the sales was able to identify other potentially involved persons and organisations nationally and internationally. The corresponding

²¹ The present case study is a real case from the FIU's practice.

²² See also the explanatory remarks on temporary freezing orders in the "Suspicious Transaction Reports (STRs)" section.

FIUs in the European Member States were informed about the findings. After the reports were disseminated to the competent law enforcement agency, an amount of around EUR 631,000 was seized.

Focus on the Use of New Payment Methods

The use of new payment methods is constantly increasing, as has also been observed in the total volume of STRs submitted in this connection. Reports related to virtual assets make up the vast majority of the reports assigned to this key risk area. STRs with indications of other new payment methods play a subordinate role in terms

of quantities. It is necessary to remember that reports with a connection to virtual assets are not exclusively assigned to the key risk area of “Use of new payment methods”. Virtual assets can also be relevant in connection with other key risk areas such as “Games of chance / Gambling” or “Serious (tax) criminal acts”.

Virtual assets

The market for virtual assets also developed very dynamically in 2021. Newer technological developments such as the increasing number of financial services on the basis of decentralised solutions, so-called **DeFi**, or the spread of (digital) goods and services by means of digitally unique

and non-fungible tokens (**NFTs**) have recently come to the attention of the broader public. In addition, there has been a significant increase in the total market value of all virtual assets, including significant price fluctuations.

DeFi

The abbreviation **DeFi** stands for **decentralised finance**, i.e. decentralised financial services. These are financial services that are offered for direct use between users (peer-to-peer) on the basis of distributed ledger technology (e.g., blockchain) and smart contracts (automatically executed contracts). The services are used via applications (dApps – decentralised apps) that now cover a range of typical financial services. Typical areas of application are exchange between different virtual assets, e.g., in the case of decentralised exchanges (Dex) or the awarding of loans in virtual assets by means of DeFi apps such as aave or compound.

NFT

The abbreviation **NFT** stands for **non-fungible token**. These are tokens that cannot be exchanged with another token. For example, they refer to digital art (“crypto art”) or other digital objects, increasingly also physical objects, and should document their uniqueness and originality in this way. At the present time, NFTs are primarily used in connection with digital art, digital collectors’ cards and collectable objects in computer games (“items”), but the potential areas of application certainly go beyond this.

Both the development of some new, innovative solutions on the basis of distributed ledger technology as well as the high monetary value of virtual assets continue to make them attractive for money laundering and terrorist financing. Many of the new financial services available via decentralised apps automate transactions between (anonymous) transaction participants without any identification of the transaction participants or a check of the origin of funds. The prices for NFTs and pricing system are often difficult to understand due to still unclear valuation criteria or market nuances and open up potential for misuse in transactions.

At the present time, the number of reports related to these relatively new developments is still manageable in terms of numbers.

The number of reports received by the FIU in connection with virtual assets continued to tick up in 2021. The number of reports that exhibited such a connection according to the information provided by the reporting entities (Reason for suspicion: “Abnormalities in connection with virtual currencies”) totalled around 5,230 in the full year. In the previous year, there were around 2,050.

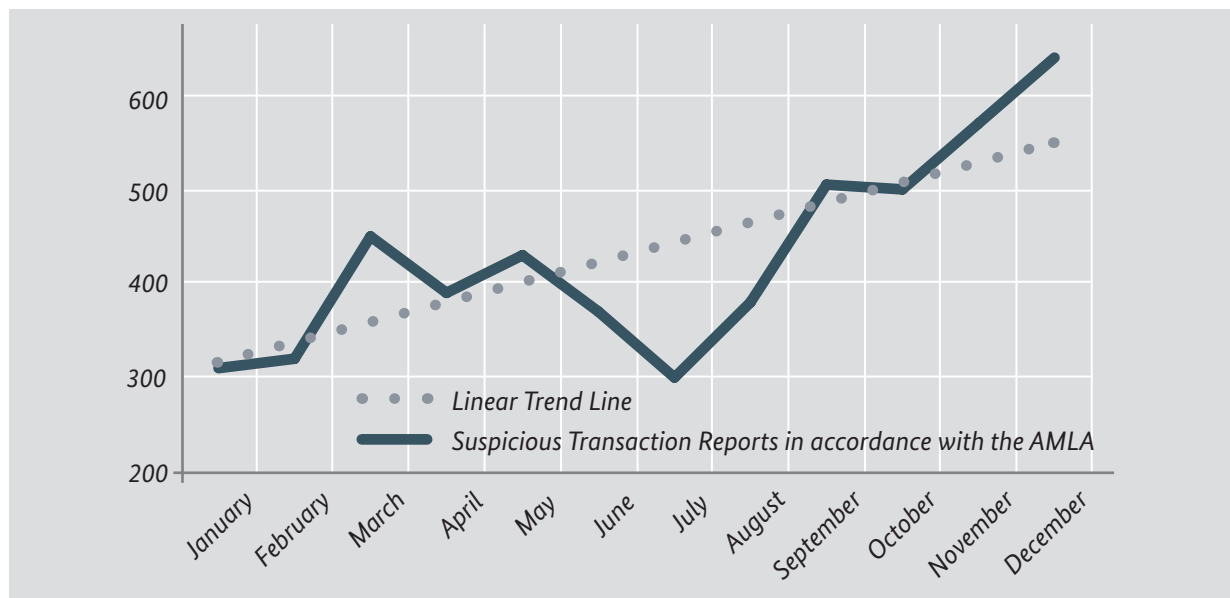


Figure 19: Suspicious Transaction Reports with the Reason for Suspicion Being “Abnormalities in Connection with Virtual Currencies”

The percentage of the reports from financial service institutions in 2021 increased to around 7.5% year on year (2019: around 1%). The majority of the reports – accounting for just under 92% – continue to come from credit institutions. The number of reports that are classified as an express matter or urgent case (Firstfall) is relatively high here. The first effects of the changes in legislation were noticed, as the virtual asset custodian business is classified as a financial service and service providing companies that do business in

this sector require the approval of the supervisory authority.²³ The classification of these service providing companies as reporting entities within the meaning of the AMLA goes hand in hand with this. Beginning in 2020, individual companies registered for the first time with the FIU, because they offer virtual asset custodian services or other banking/financial services in connection with virtual assets.

23 Law on Implementing the Fourth EU Anti-Money Laundering Directive, on Executing the EU Funds Transfers Regulation and on Reorganising the Central Agency for Financial Transaction Investigations of 23 June 2017 (German Federal Law Gazette [BGBl] I, p. 1822); Act on the Implementation of the Fourth EU Anti-Money Laundering Directive of 12 December 2019 (BGBl. I, p. 2602).

Case Study – Financial Agent Activity in Connection with Virtual Assets ²⁴

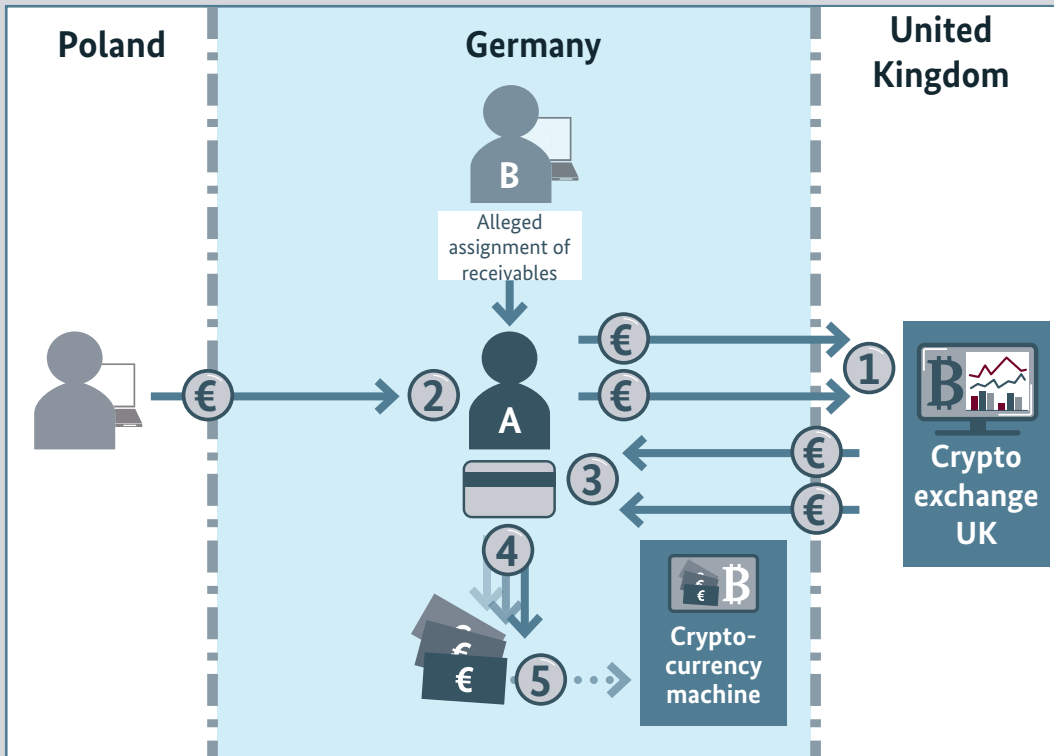


Figure 20: Case Study – Financial Agent Activity in Connection with Virtual Assets

Initial STR

A credit institution had held a current account for the reported client since the middle of 2020. Abnormalities were observed with two instructed payments to a payment service provider in the UK for a total of around EUR 3,000 each (1). Preceding that was an incoming payment for a similar amount from an account in Poland (2). Client A contradicted herself when the bank asked her about these transactions. Initially, she said that she had placed an order and had business relationships with persons in Poland. She had indicated that she was a pensioner to the bank, however. Furthermore, she stated that she did not know the party making the payment, that the person owed money to a third person B who had assigned the receivables to the client. From the incoming payment, she said she was supposed to place orders in England for the third party, a person she knew through the internet. She was supposed to earn a little bit on the transaction as well, according to her statements. The recipients of the payments in the UK were clients of a trading platform for virtual currencies, according to research by the reporting entities. The transfers to the UK were transferred back (3). The

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

client withdrew almost the entire amount received in three cash payouts immediately after receipt of the first reverse transfer to her account (4). She stated to the bank that she deposited the amount in cash at a “cryptocurrency machine” as requested by the person she knew from the internet. The bank then blocked the payout of the second reversed amount and reported the case to the FIU as an “urgent case” (Fristfall).

FIU’s Analysis and Dissemination

The FIU analysed the case, identified clear indications of financial agent activity by A and disseminated the report to the competent law enforcement agency. Person A evidently acts as a straw person for the person known through the internet. The information provided by her in regards to the origin of funds is not convincing. Contrary to what she stated, the funds should be used for the purchase of virtual currencies. After the reverse transfer by the British financial service providing company, she withdraws the money immediately in cash to use it for the purchase of virtual assets at a machine.

Findings and Developments beyond the Area of Virtual Assets

The overwhelming majority of reports that are assigned to the key risk area designated use of new payment methods are associated with a reason for suspicion referred to as “Abnormalities in Connection with Virtual Currencies”. In addition, however, there are still reports that do not exhibit any connection to virtual assets. The vast majority of these were submitted by credit institutions. One focal point of these reports are transactions processed via less well-known, often foreign, financial service institutions and payment service providing companies, some of which offer new and low-cost, often internet-based services (e.g., free debit/credit cards, low transaction costs, e.g., for payments to (non-European) foreign countries) or process payments for (online) gambling providers.

In addition, there are isolated reports on the use of alternative ways of transferring assets, such as the use of sometimes multiple intermediary payment instruments, such as digital credit/debit cards integrated into apps, which are also provided as physical cards upon request by the customer. The payment instruments are offered in part independently of an existing account at the issuing institutions and can be tied to other accounts at other banks or other payment alternatives of the customer. Abnormalities according to the reported actions are besides the transaction volume the fact that frequently the transactions were made without evident reason with the payment instrument as an intermediary. Transactions from or to other financial service providing companies, such as

ones that facilitate peer-to-peer payments or providers of prepaid card and voucher cards, without an evident economic reason for this means of executing the transaction being possible to identify, also lead to the submission of the report. Suspicious incoming payments, e.g. in e-wallets that are traced back to transactions by peer-to-peer transfers instead of bank transfers, frequently do not allow for any immediate identification of the transaction participants and do not contain any

information on the origin of the funds, which is why the reporting entities are inclined to submit an STR. In such transactions, there are in part multiple layers and payment instruments (“layering”) between the original person ordering the payment and the person ultimately receiving it, and these “layerings” are issued from financial service providing companies based in various jurisdictions.

Case Study – Suspicious Use of Intermediary Payment Instruments²⁵

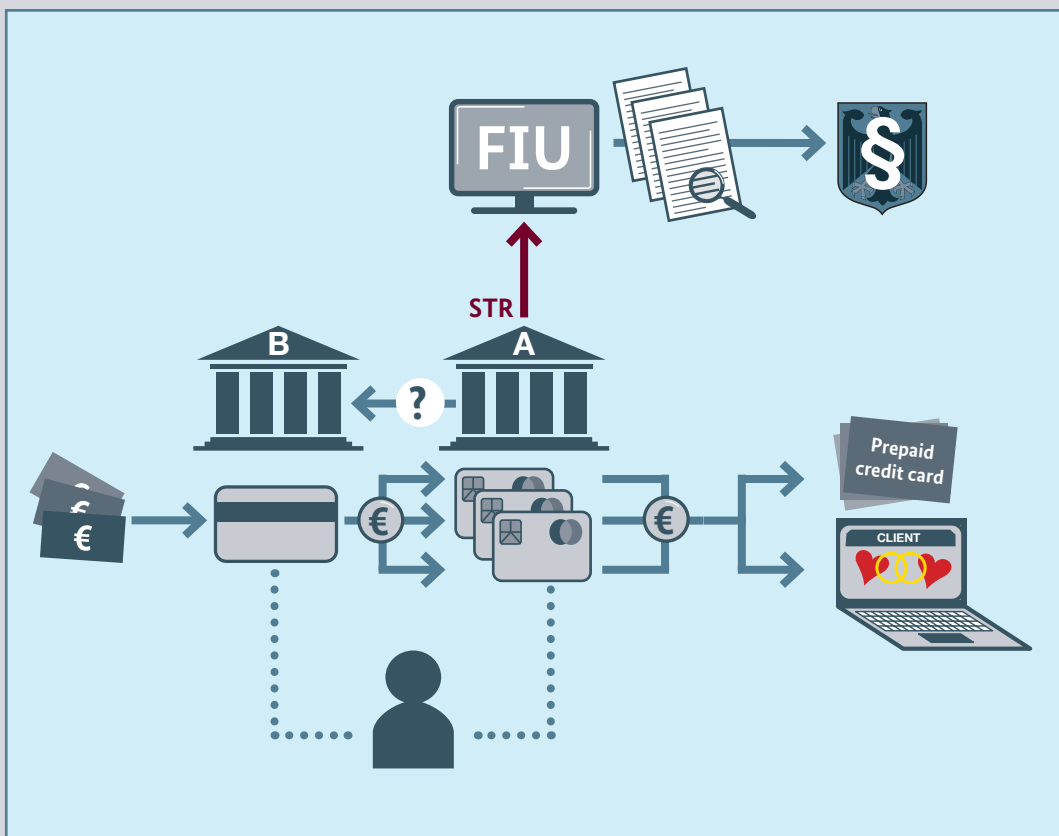


Figure 21: Case Study – Suspicious Use of Intermediary Payment Instruments

²⁵ The present case study is a real case from the FIU's practice.

Initial STR

The client of credit institution A uses multiple credit cards issued by the credit institution and has a bank account without income. Credit card transactions are settled by transfers from an account of the client at bank B. In the credit institution's assessment of the transactions, it noticed a substantial increase in the monthly transaction volume, which did not match the client's income information. The credit card transactions suggested in particular purchases of prepaid credit cards and payments to chat/dating platforms where user accounts can be topped up and the balance can be transferred to other users. A request at bank B, which held the account the client used for the settlement of the credit card transactions, revealed according to the reporting entity that the account was not covered by income but exclusively by cash deposits.

FIU's Analysis and Dissemination

In its analysis the FIU found that it had received other STRs concerning this person in the past, and the person was already known to investigators. The investigation was still ongoing. On a large scale, the client uses an intermediary payment instrument to buy, among others, prepaid cards that may be transferred anonymously to third parties. The origin of the large amount of cash that is deposited in the account to settle the payment instrument transactions does not match the client's income data and the employment situation. The new information was disseminated to the investigating law enforcement agency.

Isolated STRs assigned to the key risk area suggest the use of alternative ways to transfer monetary assets to other persons, e.g., by purchasing "app credits", voucher cards or transferable credits on social media platforms, which are accepted as a means of payment by some providers in e-commerce.

Looking back on the year 2021, we can say in summary that the trend toward increasing numbers of STRs in connection with virtual assets continued.

Growing awareness and a further increase in (media) attention on account of price developments in virtual assets and the recent rise in popularity of such assets as a result, along with changes in legislation, have also contributed to this. The recent developments are being carefully tracked by the FIU.

Financing Terrorism and Other Crimes Relevant to State Security in Connection with Virtual Assets

The key risk area referred to as “Use of new payment methods” as a result of new technologies has been set as a common key risk area for both money laundering and terrorist financing.

The typical characteristics of terrorist financing can be divided into what are referred to as “Raising”, “Moving” and “Using”. This internationally recognised triad can also be applied to the misuse of virtual assets.

Raising:

Initially, financial resources are provided or generated. These funds are collected by extremist groups, among others, in campaigns for donations. Although relatively few STRs related to virtual assets are received in connection with possible terrorist financing, transactions that indicate fundraising campaigns are often seen alongside payments to or from virtual currency exchanges. The majority of the STRs received in connection with possible terrorist financing are in the phenomenon area of Islamism. Last but not least, references to fundraising by Islamist associations are evident here. Strategic research also revealed that some right-wing extremist actors are increasingly soliciting financial donations via virtual assets. In the past year, isolated STRs have also revealed possible connections to right-wing extremism and conspiracy theories.

Moving:

The characteristic of “moving” is understood as the storage or forwarding of financial resources to conceal their actual purpose. The collected funds can be used to purchase virtual assets and then forwarded to the actual recipients or other intermediaries. The use of virtual assets from this point on makes it more difficult to trace the further financial movements than classical bank transactions. Furthermore, the reported suspicious transactions cannot be used to determine whether the abnormalities that include the suspicion of possible terrorist financing or another offence relevant for state security also exhibit a causal connection to the acquired virtual assets or the profits from the sold virtual assets.

Using:

Finally, the virtual assets are transferred to the recipients of the fundraising campaigns and resold, if need be. The concealed transactions frequently make it difficult to determine from where and why the funds landed with the recipients. Presumably, previously acquired virtual assets can also be transmitted directly to terrorist organisations and used either directly for terrorist financing or indirectly to pay out the funds as bank money or in cash for further use.

Case Study – Right-wing Extremist Athlete in Connection with Virtual Assets²⁶

The reporting entity noticed the private account of a client due to multiple credits that were forwarded immediately after receipt to a virtual currency exchange for the purchase of virtual assets. The STR was positively checked within the FIU for possible relevance to state security or terrorist financing based on background hits for the reported person in police databases and further processed by the responsible unit. It was discovered that the participant was already known to the investigative authorities due to, among others, the use of symbols of unconstitutional organisations, terrorist financing, incitement of people and a manhunt to avert danger. The credit notes flagged by the reporting entity, each for five-digit amounts, indicate in the memo (Verwendungszweck) a private loan by a third party on the one hand and credit by a dealer in precious metals pointing towards the proceeds from the sale of precious metals or jewellery on the other.

A previous STR by another reporting entity and open source research by the FIU showed that the reported account holder was an athlete and entrepreneur who belonged to the right-wing extremist scene. In light of the aforementioned abnormalities, a connection to money laundering or terrorist financing could not be ruled out. The STR was then disseminated to the competent law enforcement agency. The Federal Office for the Protection of the Constitution was also notified.

²⁶ The present case study is a real case from the FIU's practice.

Assessment of Reports on Cash Discoveries

Trading in high-priced goods such as art and antiques, vehicles and luxury goods like jewellery and watches is still often done with cash in Germany. In combination with the increasing diversification of the asset portfolio through which art, gold and especial vehicles can be viewed as investment building blocks, this can cause the areas to be susceptible to an elevated risk of money laundering activities. Thus, the use of cash (when procuring high-value goods) was identified as another key risk area in money laundering. The topic of monitoring cash in third country transport does not fall directly under the key risk area. Nonetheless, the FIU views the monitoring of cross-border cash transport and equated means of payment to be an important instrument for fighting money laundering and terrorist financing.

As the national central agency, the FIU acts as a hub and receives information from the activity of other custom's units on the monitoring of the reporting duty for accompanied cash and the public disclosure of unaccompanied cash. Accompanied cash is cash that a person takes with them. Unaccompanied cash is cash that is sent in postal packages, shipments by courier services, unaccompanied luggage or container freight to the EU or taken from the EU. In accordance with Section 30 (1) No. 3 AMLA, the FIU receives information on the cash registrations and controls in third country transport and in intra-Community transport within the framework of the clearing procedure²⁸ of the Customs Investigation Service. This information is intended as another important information building block for operational case analysis alongside the reports by the reporting entities and the supervisory authorities as well as the notifications by the fiscal authorities in accordance with Section 31b of the Tax Code (Abgabeordnung, AO).

Cash

Cash within the meaning of Regulation (EU) 2018/1672²⁷ are cash funds, transferable bearer instruments, credit cards and commodities as highly liquid stores of value.

Equated means of payment

Equated means of payment within the meaning of the German Customs Administration Act (Zollverwaltungsgesetz) are precious metals, precious stones, securities as defined in Section 1 of the German Custody Act (Depotgesetz) and Section 808 of the German Civil Code (Bürgerliches Gesetzbuch), if not already considered as cash.

²⁷ Regulation (EU) 2018/1672 of 23 October 2018 on Controls on Cash Entering or Leaving the Union (OJ L 284 of 12 November 2018, p. 6).

²⁸ In this context, clearing procedure means the clarification of the origin and/or the purpose of cash and possibly the seizure of this cash by customs.

So-called cash discoveries in this connection are especially relevant. The analysis presented below includes just under 450 notifications of cash discoveries in 2021. In cash registrations and controls for third country transport as well as cash controls for intra-Community transport, clues suggesting money laundering and terrorist financing were detected here. This equates to an almost 63% increase year on year. The background for this clear increase is primarily the travel restrictions due to the pandemic in 2020, which led to a sharp decline in the number of reports in the second quarter. Already by the end of 2020 and at the beginning of 2021, a clear increase was noticed despite ongoing travel restrictions. Simultaneously, it can be assumed that the travel restrictions – which had a particular impact on flying – caused an increasing shift to other means of transport temporarily. In 2021 the discovered cash or equated means of payment in air transport made up 49.8% (2020: 51.7%) of the cases. In comparison to this, 27.3% of the discoveries were reported in vehicle controls (2020: 34.7%) and 17.1% in post transport (2020: 5.3%).

For the cash discoveries examined in 2021, 87.4% of the discoveries involved cash and almost 8.8% transferrable bearer securities.

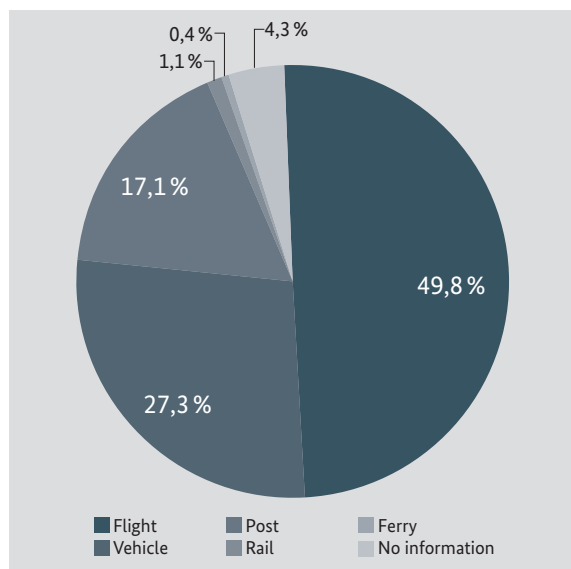


Figure 22: Means of Transport as Percentage of Cash Discoveries

National Cooperation

Cooperation with Law Enforcement Agencies (LEAs)

Cooperation with Supervisory Authorities

Requests from Domestic Authorities

Cooperation with Reporting Entities under AMLA

National Cooperation

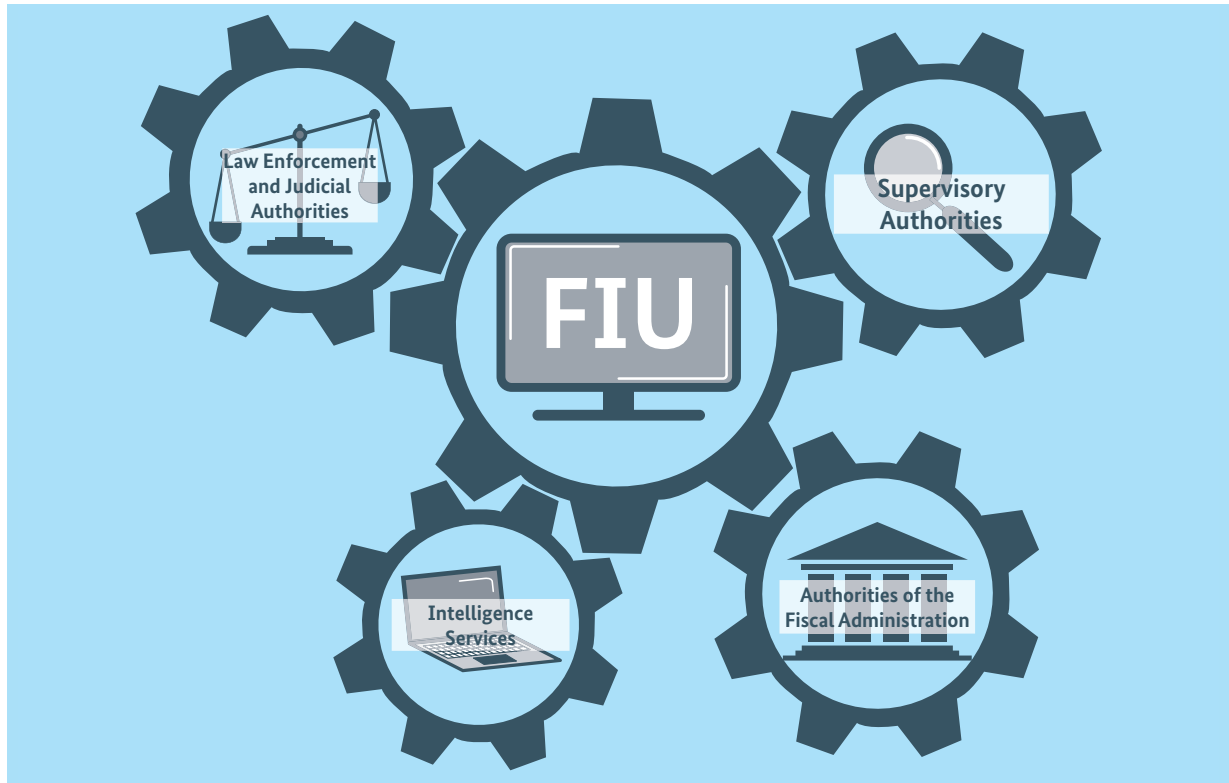


Figure 23: National Partner Authorities – An Overview

The FIU ensures the ongoing intensive cooperation with all national authorities within the network established by relevant statutory regulations. The FIU's national partner authorities are:

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

The effective prevention and combatting of money laundering and terrorist financing requires reliable cooperation with all participants against the backdrop of the increasing complexity of the economic activities and ongoing technical development. That is why the FIU continues to pursue the expansion of reliable exchange with reporting entities in accordance with Section 2 (1) AMLA. This exchange is understood to be a continuous, constantly expanded and partner-like dialogue between the FIU and the reporting entities.

Cooperation with Law Enforcement Agencies (LEAs)

The ongoing COVID-19 pandemic has meant that cooperation with national law enforcement agencies was also challenging in 2021. Established, previously in-person forms of collaboration such as workshops, conferences and trainings for partner associations were only possible to continue with limitations.

Despite the difficult circumstances caused by the pandemic, some important formats were able to be held, including the conference of the FIU's liaison officers (FIU LO), individual case-related formats such as those with the Central Agency and Contact Point for the Prosecution of Organised Crimes in North Rhine-Westphalia (ZeOS NRW), the 2nd State Security Conference of the FIU as well as various virtual lectures and trainings at the partner authorities. Furthermore, exchange with the Attorney General's Offices was intensified substantially in 2021. On-site meetings and dialogue formats were also held at all Attorney General's Offices.

Individual case-by-case topics were discussed increasingly in phone and video conferences. Accordingly, a continuous, targeted exchange could take place, in part due to the willingness of all partner authorities to cooperate despite the ongoing pandemic.

In 2021 the FIU took the lead to set up a working group with the fiscal authorities of the Länder to develop a standardised feedback form that would help with communicating to the FIU structured information on the use of its submissions. In addition to the successful development of the form, further measures to improve cooperation were identified. The format should now be continued in semi-annual meetings to keep improving cooperation between the FIU and the fiscal authorities of the Länder. This offers a framework for a trust-based exchange on specific aspects of the partnership. For example, this includes the risk-based approach of the FIU, the quality of the dissemination reports and new typologies papers.

The working group has already developed some points for improving cooperation, e.g., mutual work shadowing, further participation in meetings, technical lectures and setting up permanent contacts and partners at the fiscal authorities of the Länder.

Automatised Data Access for Law Enforcement Agencies in accordance with Section 32 (4) AMLA

In accordance with Section 32 (4) AMLA, the law enforcement agencies and the Federal Office for the Protection of the Constitution are authorised to automatically retrieve data at the FIU to fulfil their duties in cases falling under Section 32 (3) Sent. 1 No. 1 and 2 AMLA, provided that there are no restrictions on transmission. Since September 2021, the FIU has provided a corresponding interface for the law enforcement agencies to facilitate the automatised retrieval in a standardised format.

The FIU and the Federal Information Technology Centre (ITZBund), which was commissioned to develop the interface, will continue to expand it in accordance with the statutory requirements. In December 2021, the FIU jointly started the test run with the Federal Criminal Police Office (BKA).

Work Shadowing

Mutual work shadowing lets the law enforcement agencies and the FIU not only learn the methods of the cooperating authority, but also engage in direct technical exchange. Work shadowing is therefore a valuable part of cooperation.

In 2021 the pandemic still limited the scope of work shadowing. That is why only sporadic instances of work shadowing, in compliance with statutory hygiene measures, took place with cooperating authorities. The FIU was able to welcome

individual guests for work shadowing from the fiscal authorities of the Länder, police authorities and the Federal Office for the Protection of the Constitution. In 2022, work shadowing by FIU employees at the state offices of criminal investigation (LKÄ) should increase again when incidence rates are low.

Liaison Officers

FIU liaison officers (FIU LOs) deployed at the state offices of criminal investigation (LKÄ) are the FIU's first direct contact persons for questions regarding operational cooperation for the respective law enforcement agencies (police, customs, tax investigation authorities, public prosecution authorities) as well as other cooperation partners of the FIU in the federal states (Länder). In addition, they accompany further process optimisation in cooperation with the police authorities and public prosecution authorities in particular. In terms of quality optimisation, they also ensure the systematic, unbureaucratic communication of findings relevant to the situation and can support the risk-based orientation in identifying key risk areas within the FIU.

In the meantime, a total of ten FIU liaison officers (FIU LO) have been deployed for all 16 federal states (Bundesländer), some with dual jurisdiction. At a three-day conference in September 2021, both the ten FIU LOs and representatives of various specialist units of the FIU met to discuss currently relevant topics. Lectures were held, among others, on the cooperation with supervisory authorities and reporting entities as well as the focal points of strategic analysis. The goal of the annual conference is to personally integrate the decentrally deployed FIU LOs in the latest technical developments and work processes within the FIU. Furthermore, it is possible to address fundamental questions related to the cooperation with partner authorities actively and directly.

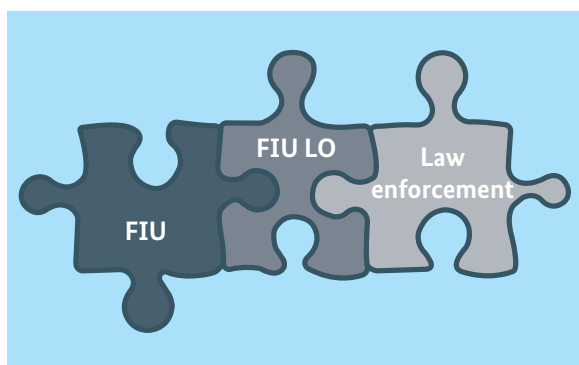


Figure 24: FIU LO

In the operational cooperation with law enforcement agencies, around 3,780 requests (previous year: 1,360) as well as additional enquiries were processed by the FIU LOs as of 31 December 2021. Thus the cooperation with the state offices of criminal investigation could also be substantially expanded and intensified as a result.

Cooperation with Supervisory Authorities

Exchanging information and coordinating with domestic supervisory authorities are key components of preventing money laundering and combatting money laundering and terrorist financing.

In 2021 the trust-based cooperation with partner authorities continued and could be accelerated as a result of already existing but also new projects.

Exchange Formats

Digital channels of communication are primarily used for exchange with domestic supervisory authorities, as in the previous year, due to the COVID-19 pandemic. Besides direct contact with supervisory authorities on account of individual case-by-case matters, new exchange formats were also offered.

In summer 2021, the FIU organised a series of events systematically aimed at the operational level of the supervisory authorities in the non-financial sector to inform them about the FIU's diverse offers for supporting the supervisory authorities and about current projects. The participating supervisory authorities were simultaneously offered the opportunity to transfer knowledge among each other. Participants in this series of eleven events in total were intentionally from various supervisory authority groups with jurisdiction in the federal states and supervisory authorities of other chambered professions. In the organisation and coordination of the individual events for this heterogeneous target group, special attention was paid to getting the participants in the physical vicinity of each other to group together to encourage the local networking of the supervisory authorities as a result.

Furthermore, the trust-based partnership between the FIU and the supervisory authorities of the Länder was continued by the FIU's invitation to meeting formats like the federal-state exchange on preventing money laundering. In this exchange

of information and experience that takes place twice a year at the invitation of the Federal Ministry of Finance (BMF), the FIU receives helpful insights into the current developments and discussions of the supervisory authorities. For the first time, there was a meeting between the coordinating bodies of the federal government and the states (Länder) during the reporting period. The FIU was also actively involved and reported on the concerted campaign in the real estate sector²⁹ as well as the information events planned in this connection.

The close cooperation between the federal financial supervisory authority (BaFin) as the supervisory authority for the financial sector is characterised by continuous exchange formats from the beginning. The quarterly meeting that has been held since 2018 is well established for discussing overarching topics of strategic importance on the management level. Since 2020 this has been complemented by the biweekly meeting of the "Group of Experts on Combatting Money Laundering" and event-based working groups to discuss changing, current topics on the operational level. The "Group of Experts to Combat Money Laundering" was used in 2021, for example, to discuss topics such as the improvement of the reporting quality of incoming STRs and the misuse of video ID processes, and to coordinate suitable measures.

²⁹ For additional information on the concerted campaign, see the explanatory remarks on the "Concerted Campaign against Money Laundering in the Real Estate Sector" below in this section.

Transmission of Information

The FIU supports the supervisory authorities in the handling of their duties in accordance with the AMLA. This includes the targeted transmission of specific information from STRs received. This information may constitute actions that suggest violations of an obligation or an elevated risk of money laundering and, in this way, may support the supervisory authorities in the risk-oriented focus of their work.

At the end of 2020, the FIU had begun to provide the supervisory authorities in the non-financial sector with relevant information related to trade in art and antiques. The reason for this was an amendment to the AMLA on 1 January 2020,³⁰ which subjected the art sector to stricter regulations under money laundering law. The group of all reporting entities was expanded to include art storage companies, and the value limits that trigger due diligence obligations were decoupled from the method of payment. In consequence, reporting entities now have to comply with due diligence obligations for transactions of at least EUR 10,000, irrespective of whether payment is made in cash or by bank transfer. To date, there have been a total of 30 notifications on actions that suggest, according to findings available to the FIU, the involvement of countries with an elevated money laundering risk or the acceptance of cash payments, which have been disseminated to the competent supervisory authorities.

³⁰ Law on Implementing the Fourth EU Anti-Money Laundering Directive, on Executing the EU Funds Transfers Regulation and on Reorganising the Central Agency for Financial Transaction Investigations of 23 June 2017 (German Federal Law Gazette [BGBl] I, p. 1822); Act on the Implementation of the Fourth EU Anti-Money Laundering Directive of 12 December 2019 (BGBl. I, p. 2602).

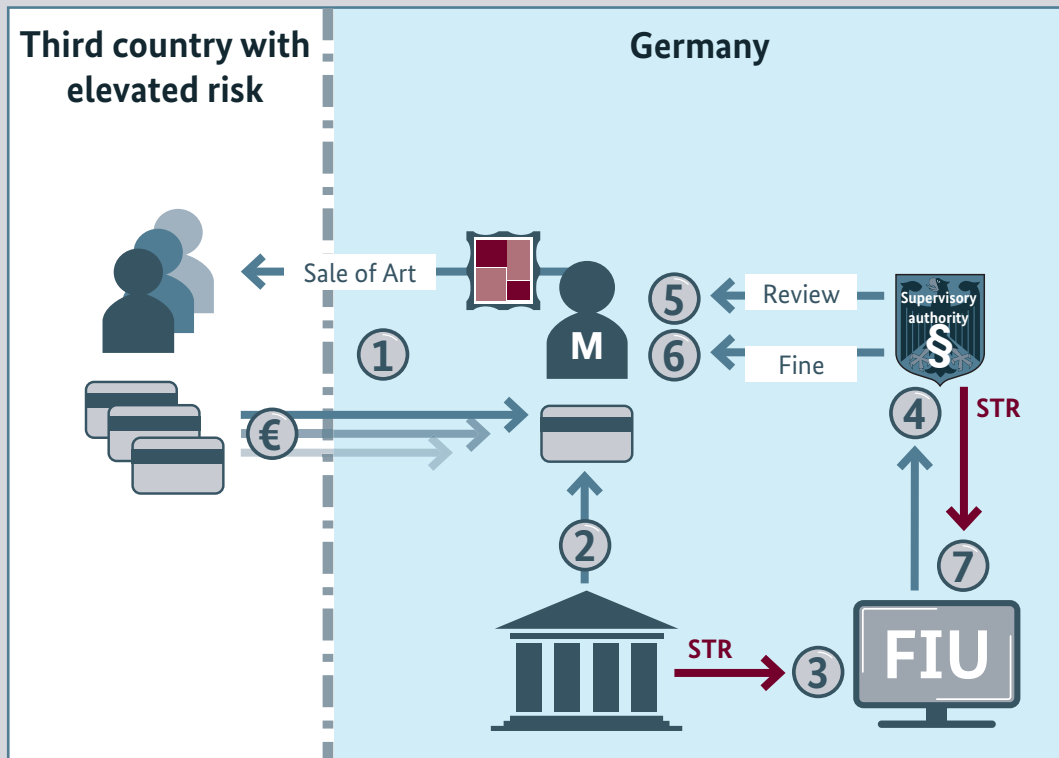
Case Study – Art Deals³¹

Figure 25: Case Study – Art Deals

A credit institution noticed the account of a client (M) due to a large number of high incoming transfers from abroad. M runs an art gallery and sells art. He is a reporting entity in accordance with Section 2 (1) No. 16 AMLA. Among others, M receives payments of considerable sums from a third country with an elevated risk of money laundering (point 1 and point 2). The credit institution reports this to the FIU in the form of an STR (point 3).

After an internal analysis, the FIU provided this information to the competent supervisory authority for fulfilment of its duties under Section 32 (3) Sent. 2 No. 3 AMLA (point 4). The supervisory authority performed an audit at the reporting entity M and discovered violations of duties under the AMLA (point 5).

M was not in compliance or not fully in compliance with his due diligence obligations to determine the beneficial owner and to identify the business partner, although a high-risk country for money laundering was involved. The considerable deficiencies in the reporting entity M's compliance with his obligations under money laundering law were punished by the supervisory authority with a fine (point 6). The supervisory authority also submitted an STR to the FIU after the audit of M (point 7).

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

Concerted Campaign against Money Laundering in the Real Estate Sector

The joint concerted campaign by the FIU and the supervisory authorities in the non-financial sector was established some years ago and could also be continued in 2021. The focus here is on both raising awareness of reporting entities and especially inter-authority cooperation between the FIU and the participating supervisory authorities.

In 2021, 60 reports on actions in the key risk area of real estate were addressed to the participating supervisory authorities to support them actively in the fulfilment of their duties. The concerted campaign against money laundering in the real estate sector was characterised in particular by not being limited to a group of reporting entities for the first time. Rather, various subgroups of reporting entities such as real estate agents, notaries and tax consultants were integrated into the campaign. Within the scope of its coordination mandate, the FIU was able to include supervisory authorities from various areas of jurisdiction under Section 50 AMLA in the concerted campaign and offered them the opportunity to discuss and transfer knowledge by organising accompanying information events.

In view of the cooperation between authorities to raise awareness among various reporting entities, the figure below shows which supervisory authorities were involved in the campaign. It also shows the percentage of disseminated reports on actions for each group of supervisory authorities.

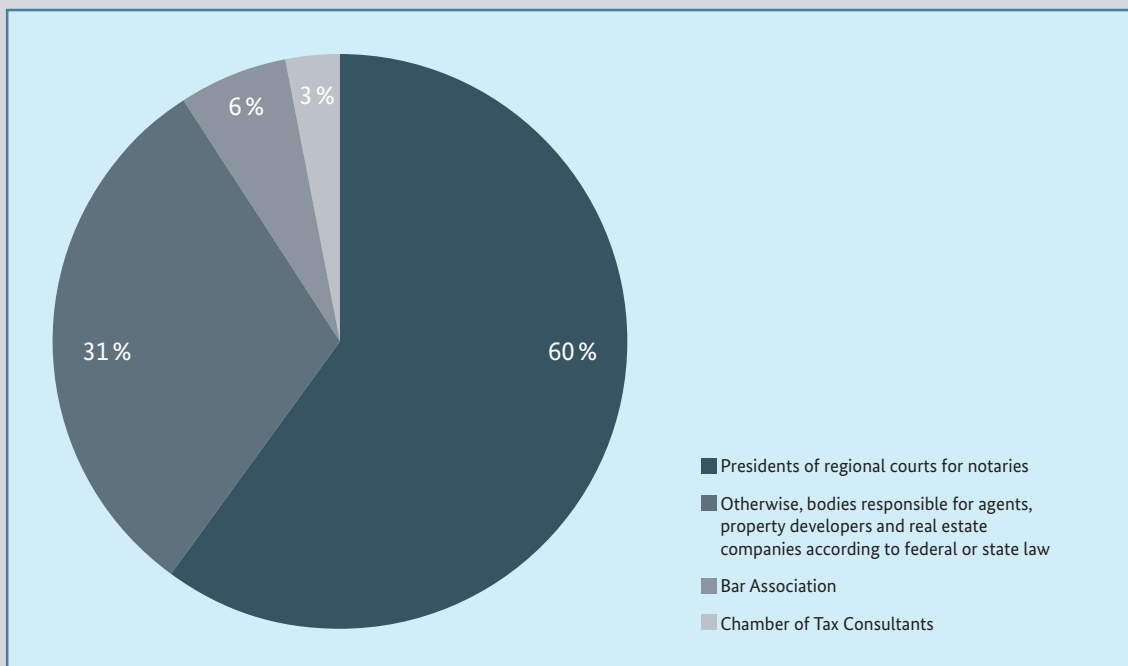


Figure 26 – Percentage of Disseminated Reports on Actions to Involved Groups of Supervisory Authorities in accordance with Section 50 AMLA

Provision of Regional Data

To support the supervisory authorities, among others in the preparation of state risk analyses, the FIU is providing the coordinating bodies of the federal states (Länder) with regional data of already registered reporting entities on the basis of its database for the first time. This allows them

to glean specific information on reporting entities already registered at the FIU. The FIU will also provide this information to the coordinating bodies of the federal states (Länder) annually in the future after the publication of the annual report for the respective period of the previous year.

Internal Area for Authorities

In the internal area for authorities at the FIU website, the FIU also provided extensive supporting information for partner authorities in the year under review. Accordingly, FIU typologies papers were revised and published, and can be used to find clues or case studies on actions relevant for money laundering or terrorist financing. Following the suggestion of the supervisory authorities, the FIU also made available, for the first time, an overview of the chronological development for the classification of countries with a high risk of

money laundering and terrorist financing. The respective classification is made by the European Commission and the FATF.³² The country lists now available and continuously updated by the FIU show the development of the classification over time, so that these overviews constitute a valuable way for the FIU to support retrograde supervisory activities.

³² See <https://ec.europa.eu/>; <https://www.fatf-gafi.org/>

Requests from Domestic Authorities

If it appears to be necessary for the clarification of money laundering, terrorist financing or other risks, or for the execution of criminal proceedings in these regards, then domestic authorities such as law enforcement agencies and intelligence services in particular may request financial information and analysis data from the FIU under certain conditions. The FIU can make a valuable contribution to existing investigations with its extensive pool of information.

The total number of incoming domestic requests increased again in 2021 and was, at 4,596 requests, around 21% above the amount in the previous year. As in the year before, the requests from police authorities and the state offices of criminal investigation in particular make up a major percentage of these.

The breakdown of domestic requests by sender is as follows.

A decline was seen in the number of requests by the federal criminal police office and the fiscal authorities. The greatest increase was noted among supervisory authorities, whose requests rose by 60%, followed by public prosecution authorities with an uptick of 45%. The police also sent more requests to the FIU than in the previous year and, in absolute terms, made the most frequent use of the opportunity to retrieve data from the FIU.

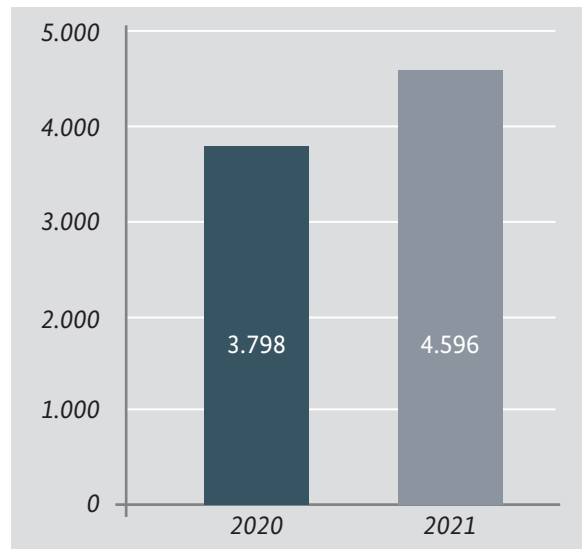


Figure 27: Incoming Domestic Requests

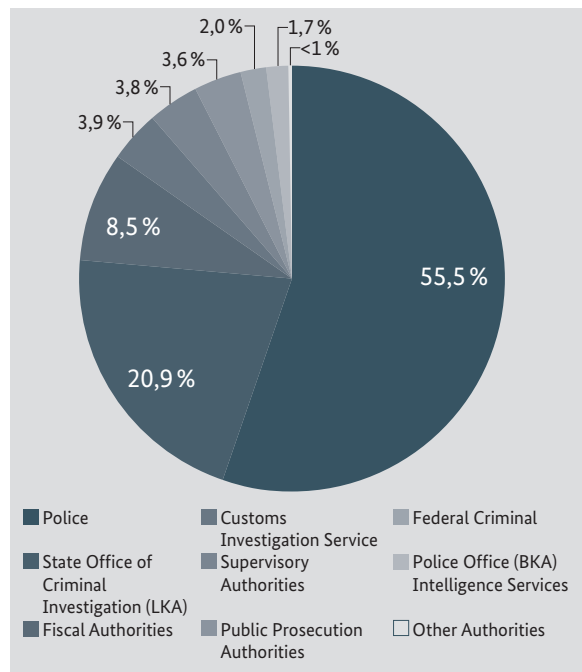


Figure 28: Breakdown of Domestic Requests by Sender

Case Study – Requests from Domestic Authorities³³

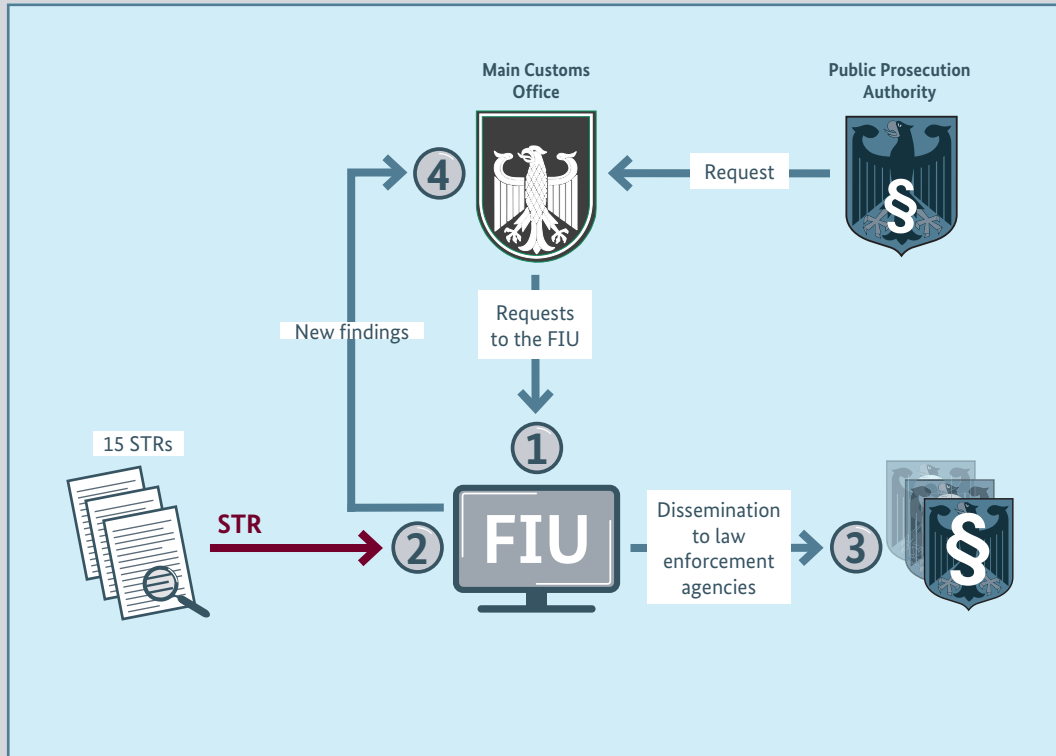


Figure 29: Case Study – Requests from Domestic Authorities

On behalf of a public prosecution authority, a main customs office investigated the suspicion of withholding and embezzlement of wages. There were indications that social security contributions and taxes were being evaded on a large scale by constantly using new companies. At regular intervals, companies are founded, usually by strawmen, to conceal the actual employer identity of the main alleged perpetrator. For the registered employees, social security declarations were submitted, but they were under-invoiced and the owed amounts were not paid. As soon as a financially damaged health insurance company filed an application for insolvency, the respective company was placed under insolvency protection in a controlled manner, and a new company was founded, to which the employees were transferred. In this way, a number of companies were established. In a request, the FIU was asked by a main customs office to share available information on the accused persons and companies (point 1).

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

The FIU was able to discover connections to the main accused persons on the basis of existing money laundering STRs. A total of 15 reports were received from reporting entities (point 2), which were disseminated to the competent law enforcement agencies (point 3).

Since customs is responsible for monitoring illicit work, the STRs were disseminated in particular to the competent customs investigation services (point 4). The transmitted money laundering STRs made it possible to identify the principal of the accused persons, who could not be discovered through conventional investigations. This led to search measures for the seizure of relevant evidence for the proceedings. This allowed for conclusions to be drawn on the order volume of the respective principals.

Furthermore, the investigating officers were able to use account summaries to gain an overview of the accused persons' cash withdrawals. The cash withdrawals were allegedly used for illicit wage payments.

Furthermore, rent payments could be identified in the money laundering STRs. This discovery was used to conduct additional searches and relevant evidence for the proceedings could also be secured as a result.

The money laundering STR also made it possible to draw conclusions on the hierarchy within the group of criminals. It was possible to determine which accused persons handled which tasks within the group. Likewise, the employees of the accused persons were discovered and questioned as witnesses during the proceedings.

A total of 271 incoming domestic requests exhibited a connection to terrorist financing or crimes relevant for state security. The exchange here is primarily between the FIU department specialising in terrorist financing and the Federal Office for the Protection of the Constitution (BfV), the Federal Intelligence Service (BND), the Military Counter-Intelligence Service (MAD) and the state security departments of the police authorities on the federal and state (Länder) level. In 2021 there was a drop in the number of requests with a connection to terrorist financing.

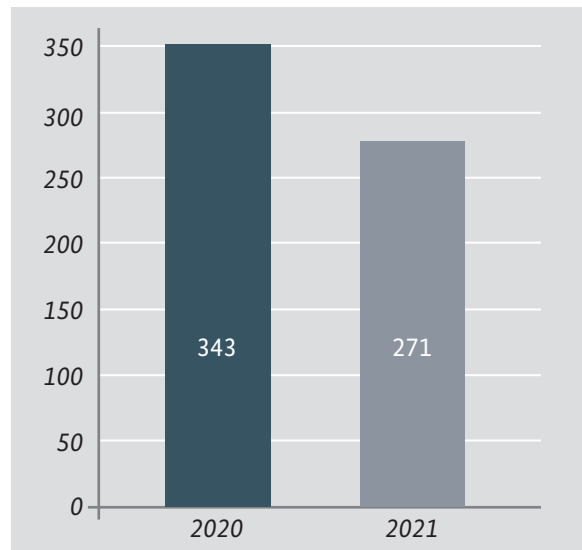


Figure 30: Domestic Requests related to Terrorist Financing and State Security

As in the previous year, most requests came from the state offices of criminal investigation (LKÄ) and the intelligence services. In 2021 the highest growth was seen in requests by the Federal Criminal Police Office (BKA).

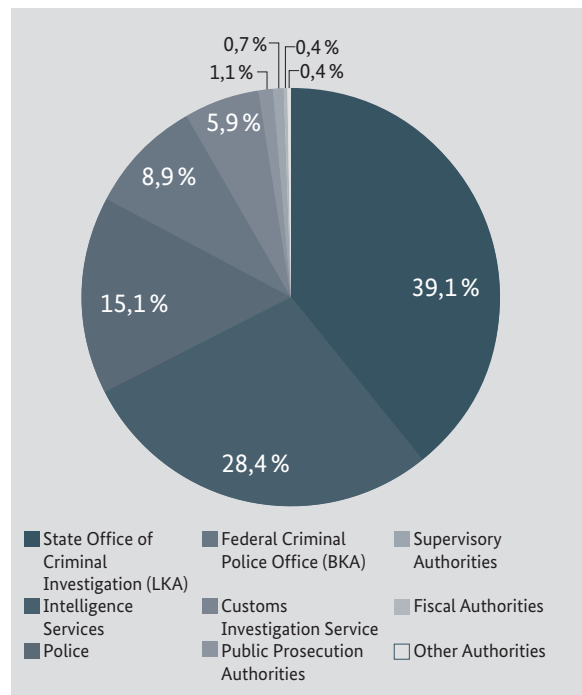


Figure 31: Breakdown of Domestic Requests related to Terrorist Financing and State Security by Sender

Cooperation with Reporting Entities under AMLA

In 2021 it was possible to maintain continuous communication and a trust-based exchange with reporting entities and associations in the financial and non-financial sector despite the pandemic. The increasing use of digital channels as introduced in the previous year continued to be expanded and intensified. Temporary restrictions in the use of previously established forms of cooperation could be compensated for the most part as a result.

The focus of the FIU's communication strategy in the last year was to continue raising awareness of ways to improve the reporting behaviour of reporting entities, especially the ones in the non-financial sector. Special events designed for specific target groups, such as an online workshop for notaries on 24 November 2021 with the Federal Chamber of Notaries made an important contribution to maintaining communication with the reporting entities during the difficult circumstances of the pandemic, besides technical lectures where the FIU supported numerous events of various subgroups of reporting entities in interactive chats.

An especially positive response was garnered by the virtual organisation of a joint money laundering conference for reporting entities and associations in the financial and non-financial sector on 10 December 2021. Various topics such as the FATF audit, new legal developments related to the AMLA and qualitative requirements for STRs were discussed constructively here. In addition, new trends and typologies in money laundering and the further development of the AFCA³⁴ were introduced.

Furthermore, the FIU supported numerous other virtual external money laundering events with various lectures on topics such as the operational key risk areas of the FIU, sector-related risks in the respective subgroups of reporting entities, individual suggestions for improving the reporting quality, but also concrete solution options for technical problems, e.g., in connection with interfaces to goAML. This gave primarily reporting entities in the areas of vehicle trade, art dealing, bar associations and real estate actors valuable information on the money laundering risk in their sector. The content-related substance of individual money laundering STRs could also be substantially improved. In particular with regard to the forthcoming registration obligation (no later than on 1 January 2024),³⁵ the speakers also gave advice on registration in goAML and reported on the development of the registration figures.

In October 2021, the FIU participated in the EXPO REAL, Europe's largest trade fair for real estate and investment, in Munich and entered into dialogue with the attendant subgroups of reporting entities, especially real estate agents and financiers. On a total of three trade fair days, numerous visitors, including still unregistered reporting entities, conversed with employees of the FIU and learned extensively about the FIU's work and the forthcoming registration obligation. Furthermore, technical questions on typologies, report dissemination and other topics related to the subject complexes of "money laundering prevention" and "combatting money laundering" were discussed.

³⁴ For more information on the AFCA, see the explanatory remarks on "Public-Private Partnership – Anti Financial Crime Alliance" below in this section.

³⁵ See Law on Implementing the Fourth EU Anti-Money Laundering Directive, on Executing the EU Funds Transfers Regulation and on Reorganising the Central Agency for Financial Transaction Investigations of 23 June 2017 (German Federal Law Gazette [BGBl] I, p. 1822); Act on the Implementation of the Fourth EU Anti-Money Laundering Directive of 12 December 2019 (BGBl. I, p. 2602).

On-site meetings of the FIU with individual reporting entities could not take place, however, due to the pandemic and were replaced by numerous conference calls. If there was a reason, the FIU contacted reporting entities to discuss the quality of the submitted STRs in particular, independent of the feedback report. This new method of entering into conversation promptly on the basis of concrete examples from STRs was regarded very positively by the reporting entities and should also be continued in future.

In addition, relevant information was published on the topic of “fighting money laundering and terrorist financing” in the open and protected area of the FIU’s website. Besides diverse publications of information from the FATF, a warning on counterfeit documents was also provided for all citizens on the website. In the protected area, new typologies papers were published, and available ones were updated:

- “Betrugs- und Geldwäscheaktivitäten im Zusammenhang mit COVID-19”
(Fraud and Money Laundering Activities in Connection with COVID-19),
- “Besondere Anhaltspunkte für das Erkennen einer möglichen Terrorismusfinanzierung”
(Special Clues for Identifying Possible Terrorist Financing),

- “Aktuelle Hinweise und Anhaltspunkte für Kreditinstitute in Zusammenhang mit einem möglichen aktiven, großangelegten, internationalen Geldwäschenetzwerk (‘Laundromat’)”
(Recent Information and Clues for Credit Institutions in Connection with a Possible Active, Large-scale, International Money Laundering Network (‘Laundromat’)) and
- “Besondere Anhaltspunkte für den Finanzsektor”
(Special Indicators for the Financial Sector).

The protected area of the FIU’s website is available to all reporting entities registered with the FIU and contains additional information on the topic of “fighting money laundering”. After registration, the reporting entities receive access data for this area.

Feedback Reports

In accordance with Section 41 (2) AMLA, reporting entities receive a feedback report on the relevance of the submitted STRs to optimise their own risk management in particular. The feedback concept discussed with the reporting entities and associations in 2018 and implemented in subsequent years envisages providing information to the reporting entities on their respective reporting behaviour, so that they can critically check their reporting behaviour and possibly make adjustments to internal processes for the fulfilment of their due diligence obligations. The FIU's feedback concept is subject to continuous improvement.

After adjustments already made in the previous year, the next step in their development in 2021 was to add the reporting date status of each report to the statement on the relevance of the individual report by the reporting entity. It is now communicated whether the report subsequently analysed

in depth ultimately led to dissemination to a law enforcement agency or was transferred back to the FIU's data pool. In the present additional step for the feedback concept, the relevance of a report is established primarily on the basis of whether the reported actions can be assigned to the key risk areas determined by the FIU. The reporting interval was set uniformly for all reporting entities and is therefore quarterly.

The feedback on the quality of the submitted reports is also now detached from the set reporting intervals, so it is individual and addressee-oriented, and preferably discussed in bilateral talks. This allows for qualitative feedback on the assessment of the submitted STRs to be provided so that the reporting entities can improve the report quality and adjust internal processes, if necessary. This procedure was welcomed by the reporting entities and should be continued by mutual agreement.

Public-Private Partnership – Anti Financial Crime Alliance

The strategic cooperation to fight money laundering and terrorist financing was also further expanded in 2021 as part of the public-private partnership called the Anti Financial Crime Alliance,³⁶ which was founded in September 2019. In the meantime, over 100 representatives from agencies, authorities and reporting entities, in total 41 institutions, are involved in the AFCA and are in regular, constructive and trust-based exchange within the individual working committees (board, team of experts, management office, working groups).

In the first quarter of 2021, the kick-off event was held for the new team of experts consisting of high-ranking representatives in the private banking sector, the judicial area and experts in science and research. The team of experts supports in particular the board of the AFCA with regard to the strategic objective of the AFCA, analyses and assesses the results of the working groups from a technical perspective and promotes cooperation with the associations. The team of experts currently includes eleven members.

Membership structure of the AFCA (as of: 31 December 2021)	
Reporting entities in the financial sector	24
Reporting entities in the non-financial sector	7
Representatives of authorities	8
Non-reporting entities ³⁷	2

Figure 32: Membership Structure of the AFCA in 2021

The operational core of the AFCA is currently made up of five working groups. New working groups can be set up if needed. This was not done in 2021. Rather, the focus was on intensifying cooperation in the existing working groups and producing corresponding work results. These are placed at the disposal of all members of the AFCA, the reporting entities and interested authorities through publication on diverse password-protected platforms.

³⁶ The Anti Financial Crime Alliance (AFCA) is a public-private partnership (PPP) under the umbrella of the FIU and was established by the private sector and the authorities and agencies involved in the prevention and combatting of money laundering and terrorist financing on 24 September 2019. The partnership approach with equal input by all participants gives state institutions and the private sector the opportunity to discuss strategic as well as problem- and phenomenon-based issues.

³⁷ These are third-parties that fulfil services for reporting entities, but are not themselves reporting entities under Section 2 (2) AMLA, as for example the federal notary chamber (Bundesnotarkammer).

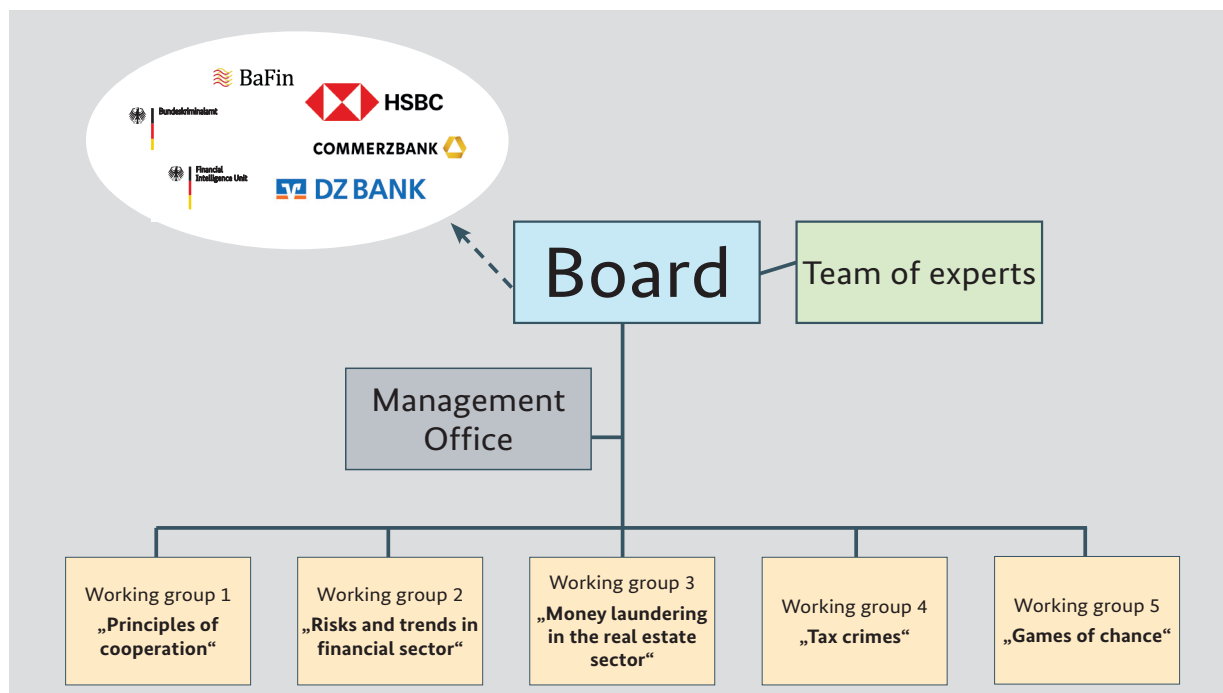


Figure 33: Structure of the AFCA

In 2021 the whitepapers by working group 2 – “Risks and Trends in the Financial Sector” were published: “COVID-19-related Money Laundering and Terrorist Financing Risks and Effects on Financial Crime”, “Shell Companies and Financial Crime in Connection with them” and “The Laundromats” (in English). Furthermore, a “Self-declaration for Payment Service Providers” (in German and English) and the manual “Identifying and Fighting Financial Flows in Human Trafficking” were published with an annex and research tool for the manual.

Working group 3 – “Money Laundering in the Real Estate Sector” prepared an extensive whitepaper titled “Findings on the Forms of Money Laundering in the Real Estate Sector” with numerous business cases (case studies), which was highly regarded.

The same applies to the situation report titled “Money Laundering Prevention in Games of Chance”, which was submitted by working group

5 – “Games of Chance” and approved by the Board of the AFCA on 8 December 2021 for publication in the protected area of the FIU’s website. It provides an overview of the current complex market situation in various sectors of games of chance as well as its classification under money laundering law, and draws conclusions for the future design of money laundering prevention measures.

On 30 November 2021, the AFCA forum, an annual event, was held for the second time. Numerous representatives from the group of reporting entities, authorities, agencies and associations took part in what was this time a hybrid event, taking advantage of the opportunity to engage in intensive exchange. The board, team of experts and acclaimed international experts also provided information in lectures on the latest challenges and developments in the area of fighting money laundering and presented other international public-private partnerships and their respective focuses and fields of activity.

International Cooperation

Information Exchange with Other FIUs

International Committee Work

International Cooperation

The global exchange of information with FIUs of other countries ensures the effective prevention and combatting of money laundering and terrorist financing that occurs both nationally and internationally. More than ever before, it is necessary to cooperate constantly with international partners

in addition to domestic authorities. The FIU Germany is in close contact with other FIUs and continues its consistent engagement in international project and committee work.

Information Exchange with Other FIUs

The information exchange with other FIUs is a major component of preventing and fighting internationally organised money laundering and terrorist financing, taking place both on the operational and strategic level. In cooperation with European and international partner authorities, relevant information is continuously and proactively shared or provided upon request. This ensures that cross-border structures and international operations are comprehensively analysed.

Another component of information exchange with other FIUs is participation in multilateral meeting formats, as well as the preparation and coordination of visits and virtual meetings by/

with staff from foreign FIUs and, as necessary, also other foreign authorities. Highlights from 2021 include participation in the meeting of German-speaking FIUs, which was held by the FIU Liechtenstein, and also participation in the meeting of French-speaking FIUs, which was aimed at a larger group of participants and was organised by the FIU Monaco.

In 2021 the FIU exchanged information with a total of 136 (2020: 145) countries. Cooperation with the EU Member States of France, the Netherlands, Poland, Luxembourg, Belgium and Austria was especially extensive.

Incoming and Outgoing Information and Requests

The processing and analysis of actions in the international operational area increased significantly in comparison to the previous year. The total number of cases amounted to 16,959 (2020: 9,270). In comparison to the previous year, the number of requests ticked up to 3,188 in 2021 (2020: 2,842). In the same period, the number of spontaneous information cases more than doubled to 13,711 (2020: 6,428). The increase shows clearly that the FIU Germany was also able to fulfil its role as a central actor in the fight against international money laundering and successfully continue its work in the second year of the pandemic.

Request

In a request, a FIU can gain access to personal data at a partner FIU under certain conditions, e.g., if it is intended to prevent, discover and fight money laundering, predicate offences to money laundering or terrorist financing.

Spontaneous information

Spontaneous information is the proactive transmission of an action that could be of importance for a partner FIU without being tied to a request sent by the partner authority.

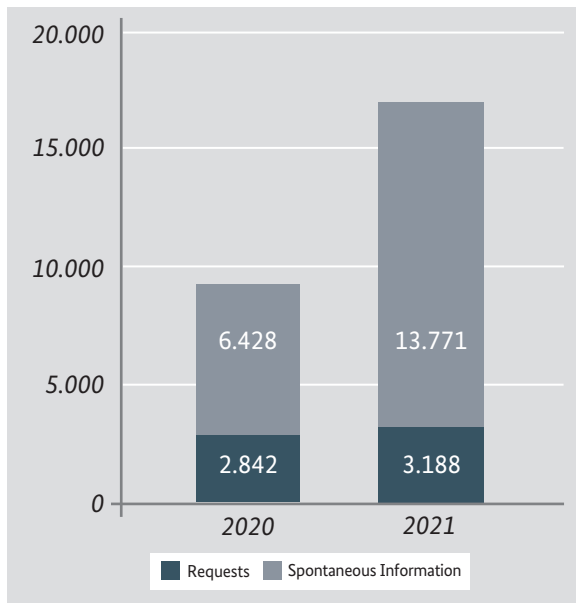


Figure 34: Cases of International Cooperation in a Year-on-Year Comparison

It is possible to differentiate between incoming and outgoing cases for both spontaneous information and requests.

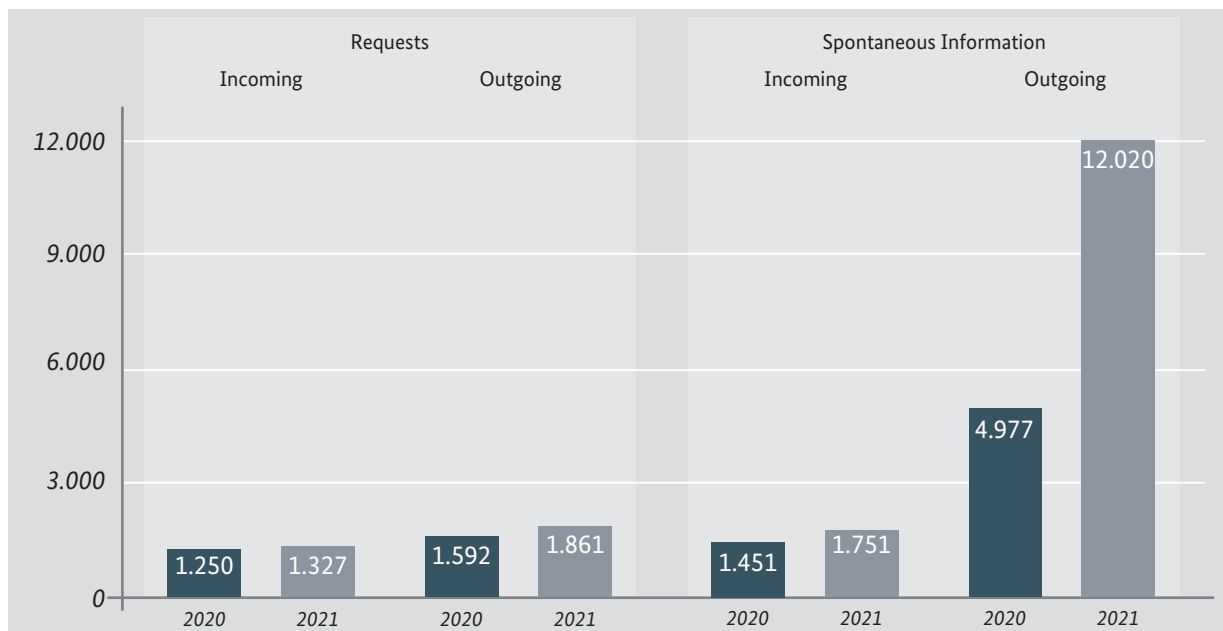


Figure 35: Request and Spontaneous Information in Year-on-Year Comparison

The number of requests received by the FIU totalled 1,327 in 2021, an increase of around 6% year on year. There were 966 requests from EU Member States and 355 from non-EU countries. While the number of incoming requests in the area of exchange with EU countries only changed slightly, the number in the area of exchange with non-EU countries rose by around 28%.

Furthermore, six requests were received from Europol in 2021, which the Federal Criminal Police Office transmitted to the FIU.

The collective 6% uptick in incoming requests reflects the positive evolution and continuous intensification of the information exchange between FIUs around the world and is the fifth consecutive annual increase in the number of such requests. The EU Member States making by far the most requests were Luxembourg and France.

The number of incoming spontaneous information incidents totalled 1,751 in 2021, an increase of around 21% year on year. There were 1,407 spontaneous information incidents from EU Member States (a roughly 12% increase relative to the previous year) and 343 from non-EU countries (a

roughly 80% increase relative to the previous year). A substantial portion of the increase in spontaneous information incidents from non-EU countries is mainly due to the UK’s departure from the EU (“Brexit”), since the FIU UK is now assigned to non-EU countries in contrast to the previous year. Furthermore, the FIU received one spontaneous information incident from Europol.

The FIU Malta sent the most spontaneous information incidents with 513 cases, which made up roughly 36% of all incoming spontaneous information incidents from the area of EU states. Various cases with possible money laundering in connection with games of chance and betting were also included here this year. In comparison to the previous year, the FIU Austria accounted for the largest increase (over 190%) in transmitted spontaneous information incidents. The FIU Ireland also raised the number of transmitted spontaneous information incidents by 90%. Liechtenstein showed the highest increase of all non-EU countries and almost doubled the number of spontaneous information incidents sent to the FIU Germany.

In this area, the increase in transmitted spontaneous information incidents reflects the positive evolution and continuous intensification of the information exchange between FIUs around the world and is also the fifth consecutive annual increase.

Outgoing requests can, in addition to the FIU's own analysis, also be traced back to domestic requests. In these cases, actions brought to the attention of the FIU in domestic requests have a foreign connection. If the action falls within the FIU's scope of responsibilities, the FIU takes the case into its own hands and sends a request to its partner authorities for subsequent analysis. The percentage of requests with this type of origin was around 78% in 2021 and is roughly comparable to the previous year.

The number of outgoing requests totalled 1,861 in 2021, an increase of around 17% year on year. There were 1,273 requests sent to EU Member States and 588 sent to non-EU countries. A substantial increase in the area of exchange with non-EU countries was also observed here. This is largely due to the UK's departure from the EU and

the associated reclassification of the FIU UK to non-EU countries.

Within the EU, the most requests were sent to the FIU Luxembourg and FIU Lithuania.

The number of outgoing spontaneous information incidents total 12,020, which, after a decline in the previous year, was nearly double the number in 2020. This is due in part to the simplified analysis process introduced at the beginning of 2021, especially for simple cases of fraud. In the course of the simplified processing applied in these cases, a corresponding number of spontaneous information incidents were sent out.³⁸

There were 11,313 spontaneous information incidents sent to EU Member States (a roughly 213% increase relative to the previous year) and 707 sent to non-EU countries (a roughly 48% decrease relative to the previous year). The most spontaneous information incidents were sent to France, the Netherlands and Poland.

³⁸ For additional information on the adjustment of analysis processes for simple cases of fraud, see the explanatory remarks under "Description and Continuation of Key Risk Areas" in the "Typologies and Trends" section.

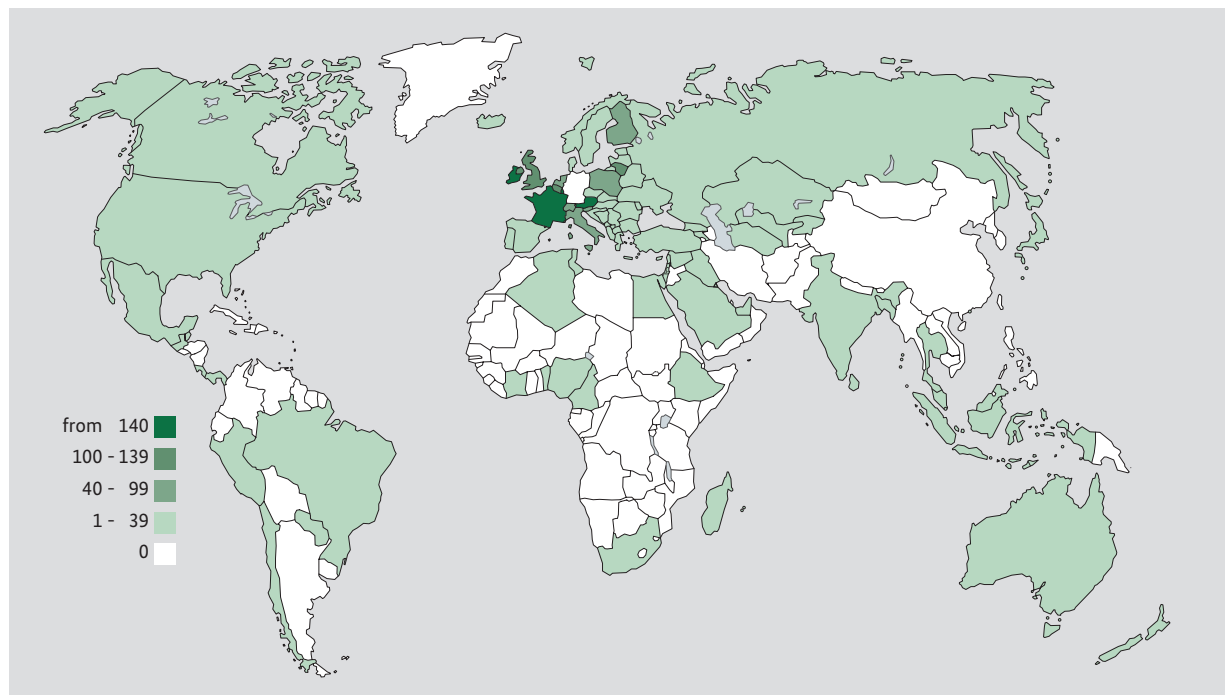


Figure 36: Incoming Cases of International Cooperation by Country of Origin

In 2021 the FIU Germany received a total of 3,078 cases from 102 countries. Most requests and spontaneous information incidents received by the FIU Germany came from Luxembourg and Malta, although in absolute terms there were more spontaneous information incidents. Furthermore,

France, Ireland and Austria sent the most cases for international cooperation. The most intensive exchange with non-EU countries involved the FIUs from Liechtenstein, the UK, Switzerland, Montenegro and the USA.

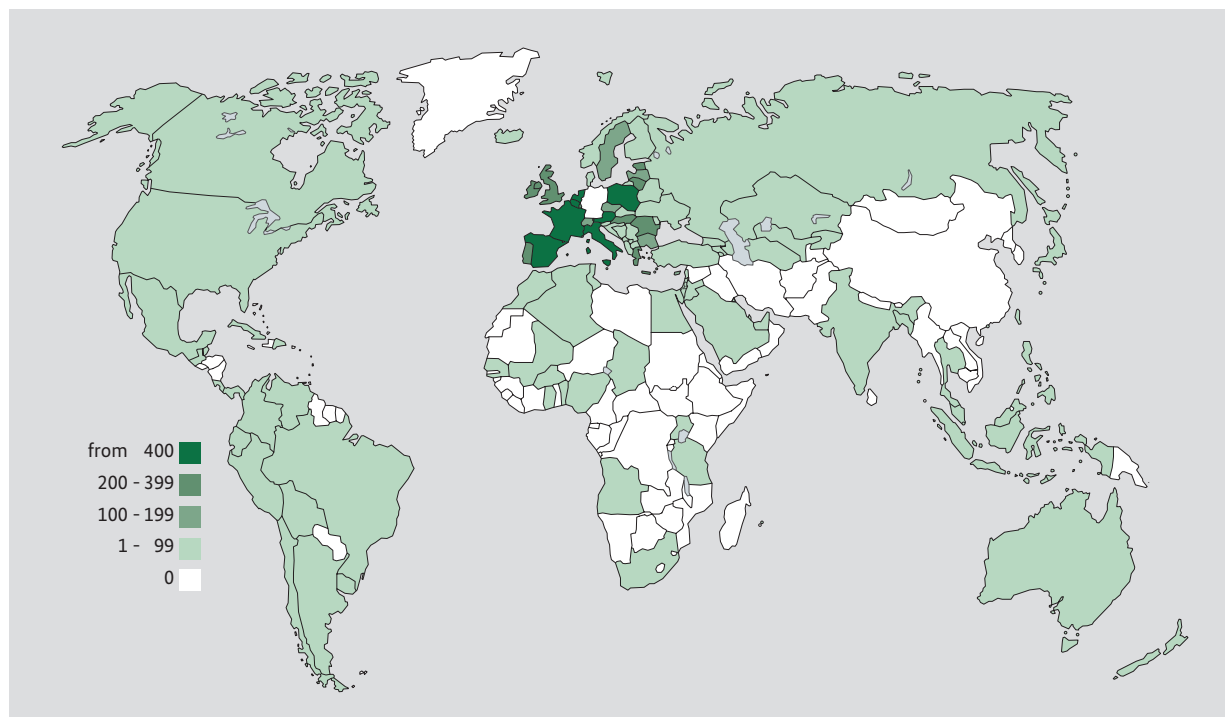


Figure 37: Outgoing Cases of International Cooperation by Country of Destination

The FIU Germany sent a total of 13,881 cases to 126 countries around the world in 2021. As in the previous year, the cooperation with France was especially intensive. Frequent addressees of outgoing

cases from Germany were the EU countries of Luxembourg, the Netherlands, Poland, Lithuania and Belgium, along with the non-EU countries of the UK, Switzerland, Türkiye and the USA.

The following tables each provide an overview of the most frequent addressees and senders of incoming and outgoing requests and spontaneous

information in 2021. As in previous years, the most intensive exchange was with the neighbouring states of France, Luxembourg and the Netherlands.

Country	Incoming requests
Luxembourg	147
France	136
Netherlands	85
Finland	83
Lithuania	55
Malta	45
Italy	44
Poland	42
Austria	38
Slovenia	34
Other FIUs	618
Total	1.327

Country	Outgoing requests
Luxembourg	217
UK	188
Lithuania	128
Netherlands	91
Spain	90
Poland	81
Estonia	73
Belgium	65
Austria	61
Switzerland	59
Other FIUs	808
Total	1.861

Table 4: Number of Incoming and Outgoing Requests Broken down by Countries

Country	Incoming spontaneous information
Malta	513
Luxembourg	331
Ireland	158
Austria	111
Liechtenstein	108
Belgium	96
UK	91
Lithuania	47
Switzerland	29
Poland	26
Other FIUs	241
Total	1.751

Country	Outgoing spontaneous information
France	4.914
Netherlands	1.167
Poland	774
Belgium	510
Italy	455
Austria	444
Estonia	440
Greece	366
Portugal	316
Romania	270
Other FIUs	2.364
Total	12.020

Table 5: Number of Incoming and Outgoing Spontaneous Information Cases Broken down by Countries

Case Study – International Requests³⁹

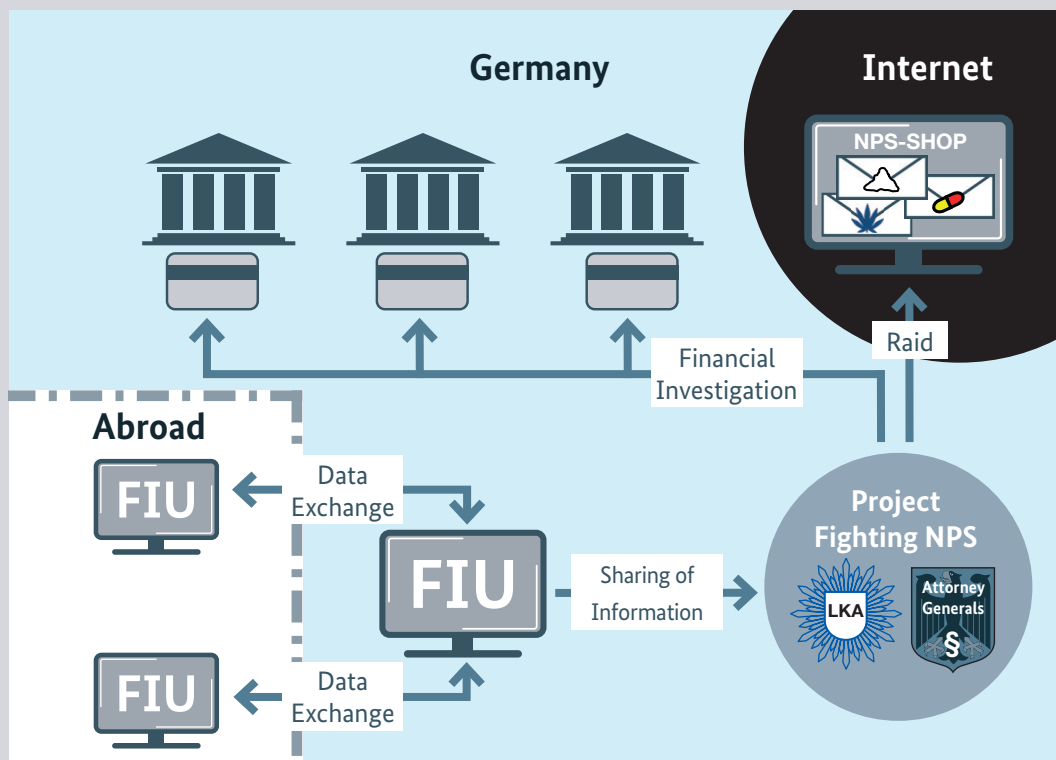


Figure 38: Case Study – International Requests

In consultation with an attorney general’s office, a state office of criminal investigation initiated a project to fight new psychoactive substances (NPS) on the internet. The aim of the project was to siphon off the operational current assets of illegal NPS shops. After the identification of an illegal NPS shop through test purchases, assets in Germany and abroad were promptly siphoned off.

In this project, the foreign information collated by the FIU Germany was included on a large scale for the investigations. It involved multiple online shops that sold psychoactive substances, in part under the guise of online shops for clothing. Due to the data exchange between the FIU Germany and two partner FIUs, it was possible to seize a considerable amount of funds before the transmission of the judicial request.

The information that was shared with the competent law enforcement agency then led to various suspicious accounts in the investigations of finances there. To cite an example, three accounts had balances of around EUR 400,000, EUR 1.7 million and EUR 500,000 each in different short timeframes.

The investigation ultimately led to a search in 2021 where investigators found a number of envelopes with psychoactive substances ready to be sent by post.

39 The present case study is a real case from the FIU’s practice.

International Cooperation – Indications of a Potentially Active International Money Laundering Network (“Laundromat”)

Criminals continue to make hundreds of millions of euros through criminal acts.⁴⁰ In order to place incriminated money in the international economic cycle and “wash” it, they make use of large-scale, complex international money laundering networks, so-called laundromats, where cross-border payment flows conceal the origin of incriminated money and allow the money to be fed into the legal cycle.

In 2020 the FIU received STRs from a reporting entity in the financial sector that contained thousands of suspicious transactions, and in which the existence of a possible active, large-scale, international money laundering network was suspected. Research by the FIU confirmed the existence of abnormalities. The transmitted transaction data was then subject to a quantitative and qualitative assessment in the course of a more in-depth analysis.

In the quantitative analysis, the payment flows were observed more carefully: Where does the money come from, where does it go? Which countries, banks, correspondence banks and companies are affected and to what degree? Thousands of transactions with a volume of over EUR 1 billion were observed in total. The analyses also showed in particular clear international connections in the reported transactions, with over 500 credit institutions and over 2,000 companies from more than 100 countries.

The qualitative analyses identified various clues and behaviours in conjunction with the reported transactions and the parties involved in them, classifying them as suspicious and calling for greater attention at the credit institutions. For this reason, the clues paper titled “Laundromat” was drafted to describe the discovered abnormalities and patterns. The paper was made available in June 2021 through the protected area of the FIU’s website for reporting entities and authorities.

In the work on this international money laundering network, the FIU engaged in exchanges with the law enforcement agencies and supervisory authorities to provide information about the respective findings and to jointly fight international money launderers on the national level. In the course of international cooperation, the FIU also informed the central agencies of the countries that appeared to a substantial extent in the underlying transaction data about their findings on this possible active, international money laundering network by sending them country-specific data and a translation of the clues paper, in order to increase awareness internationally and to enable the cross-border tracking of the laundromat.

⁴⁰ In 2020, for example, the discovered criminal revenue in the area of organised crime in Germany totalled around EUR 1 billion (source: Federal Situation Report 2020 – Organised Crime of the Federal Criminal Police Office).

The area of terrorist financing and state security also saw active international exchange. In this area, the FIU exchanged over 400 pieces of information

with a total of 52 countries. As in the years before, the cooperation with the FIUs from France and Luxembourg was especially pronounced.

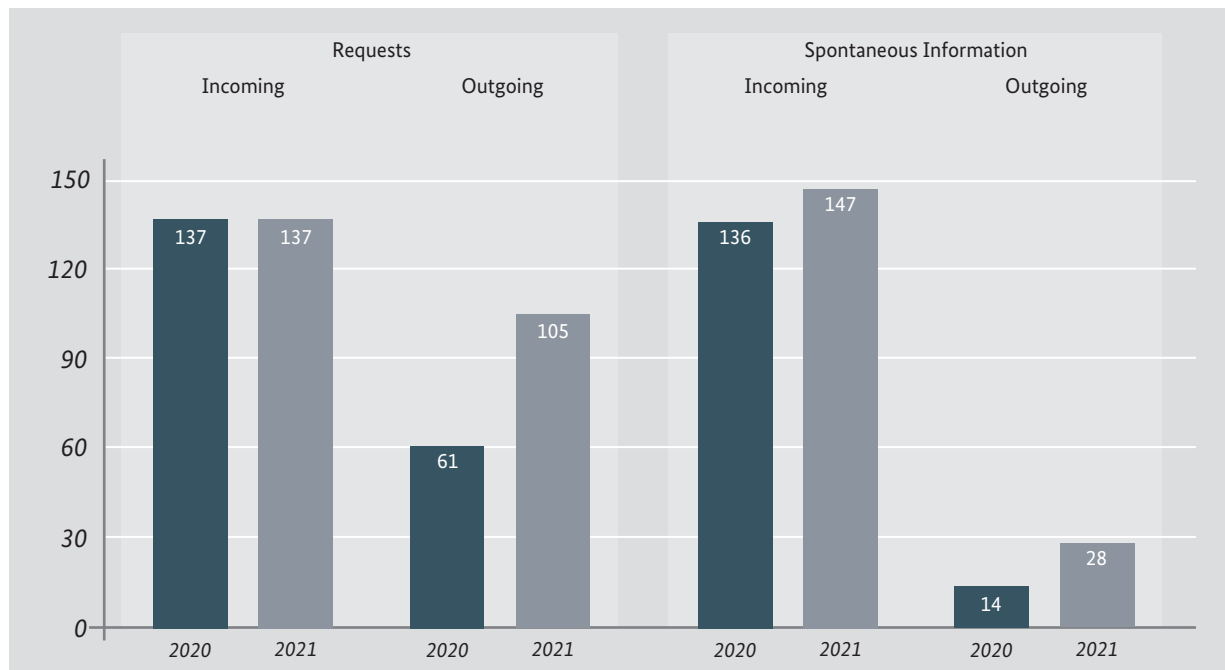


Figure 39: Cross-border Information Exchange with connection to Terrorist Financing or State Security

The FIU Germany received 284 cases from 36 partner FIUs, which were evenly divided between requests and spontaneous information. While the number of incoming requests remained at a constant level, the incoming spontaneous information incidents rose by around 8%.

To fight terrorist financing and other criminality relevant to state security, the FIU Germany sent a total of 133 cases to 35 countries around the world in 2021. This equates to an increase of 77%.

Country	Incoming requests	Country	Outgoing requests
France	38	Luxembourg	35
Luxembourg	34	UK	9
Malta	8	Belgium	4
Finland	6	Spain	4
Netherlands	6	France	4
Switzerland	5	Netherlands	4
Italy	4	Türkiye	4
Belgium	3		
Syria	3		
Other FIUs	30	Other FIUs	41
Total	137	Total	105

Table 6: Number of Incoming and Outgoing Requests with Connection to Terrorist Financing or State Security, Broken down by Countries

Country	Incoming spontaneous information	Country	Outgoing spontaneous information
Luxembourg	108	France	12
Austria	8	Austria	4
Syria	6	Belgium	3
USA	6	Switzerland	3
Switzerland	4	Spain	2
Malta	4		
UK	2		
Ireland	2		
Other FIUs	7	Other FIUs	4
Total	147	Total	28

Table 7: Number of Incoming and Outgoing Spontaneous Information Cases with Connection to Terrorist Financing or State Security, Broken down by Countries

International Committee Work

In addition to bilateral information exchange between FIUs, the committee work is an important component of international cooperation. Increasing the intensity of committee work and expanding international relationships let the FIU participate more actively in the optimisation of framework conditions to fight money laundering and terrorist financing, address developments on trends promptly and contribute to global solution strategies.

The COVID-19 pandemic sped up the digital transformation. The committee work has changed to the extent that working group meetings and plenary meetings such as the FATF plenary and the Egmont working group meeting are held virtually or in a hybrid format and are also planned as hybrid meetings in the future.

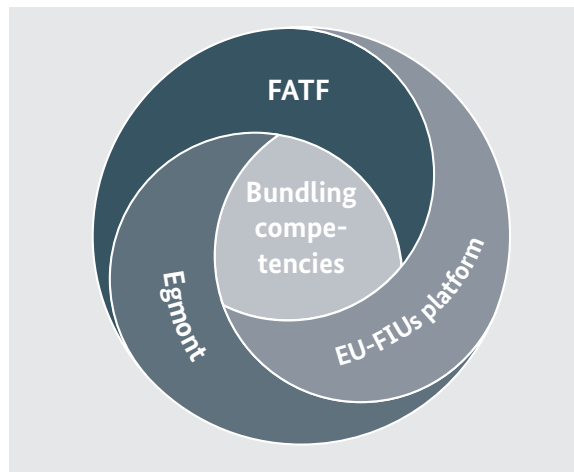


Figure 40: International Committees

Financial Action Task Force (FATF)

The FATF is a global committee to prevent and fight money laundering, terrorist financing and proliferation financing. Established in 1989 by the G7 states, 39 members now belong to the FATF, including 37 Member States, the EU Commission and the Gulf Cooperation Council.⁴¹ President of the FATF was the German Assistant State Secretary Dr Marcus Pleyer in 2021. Over 200 jurisdictions have committed to implementing the standards and recommendations set by the FATF. By regularly reviewing compliance with and effective implementation of these standards, the FATF ensures an internationally coordinated approach to money laundering and terrorist financing. Germany was initially scheduled for such an audit in

2020. After the final phase of this audit had to be postponed due to the pandemic, it was completed at the end of 2021. The final report is expected in late summer 2022. The FIU was audited by other important stakeholders, among others, from law enforcement, supervision, and the business community, and by the international audit committee of the FATF.

As part of the German FATF delegation, the FIU – under the leadership of the German Federal Ministry of Finance – actively adds its expertise to the various FATF projects. In 2021 the FIU took part especially in the projects called “Digital Transformation of AML/CFT for Operational Agencies”

⁴¹ The Gulf Cooperation Council is an international cooperation of the member states of Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates in the areas of business, foreign policy and security.

(Joint Project of the FATF and the Egmont Group) and “ML/TF Risks Arising from Migrant Smuggling”.⁴² The FIU made valuable contributions to other prioritised topics under the German FATF

presidency such as e.g., environmental crime, illegal arms trade in terrorist financing or the financing of terrorism motivated by ethnicity or race.

Egmont Group of FIUs

The Egmont Group of FIUs is an international coalition of FIUs that offers a platform for the secure exchange of technical knowledge and financial information to fight money laundering and terrorist financing. It had 167 members in 2021.

Besides the work in eight regional groups, a major part of the Egmont Group is the cooperation of the FIUs in four working groups:

“Information Exchange Working Group” (IEWG)

The largest Egmont working group dedicated to operational cooperation develops projects in central FIU-relevant subject areas. The work published in the projects is available to all FIUs that are members of the Egmont Group and in part also to the reporting entities and law enforcement agencies. In 2021 the FIU Germany’s involvement in the IEWG consisted in particular of managing the project “Conclusions from large-scale cross-border money laundering schemes”,⁴³ which began in 2019, and its membership in the project “FIUs capabilities and involvement in the fight against the financing of extreme right-wing terrorism” (ERWTF),⁴⁴ which ran from 2020 to 2021.

Furthermore, the FIU Germany contributed to the following projects:

- “Flexible, Consistent Information Exchange Standards”,
- Joint project by FATF and Egmont Group “Digital Transformation of AML/CFT for Operational Agencies”,
- Egmont “IT Renewal”, “Asset Recovery – the role of FIUs”,
- “E-Catalogue on Regulated Virtual Asset Service Providers (VASPs)”.⁴⁵

42 The original project names are in English as above.

43 See the explanatory remarks in this section.

44 The original project names are in English as above.

45 The original project names are in English as above.

“Membership, Support and Compliance Working Group” (MSCWG)

The primary aim of this working group is to check applications of candidates wishing to join the Egmont Group and considering how to proceed with Egmont members who no longer fulfil the criteria for the Egmont Group.

At the present time, the FIU Germany holds an advisory position in the MSCWG.

“Policy and Procedures Working Group” (PPWG)

The mandate for the PPWG consists of developing operating guidelines and giving advice on strategic issues that have an impact on the Egmont Group. In particular, the PPWG also addressed the use and, as needed, revision of central documents of the Egmont Group such as the Charter and the Principles of Information Exchange.

The FIU Germany made contributions to the projects “Addressing impediments to information exchange between FIUs” and “Glossary of Key Egmont Group Terminology”,⁴⁶ which could both be successfully concluded in 2021.

“Technical Assistance and Training Working Group” (TATWG)

The TATWG works constantly on improving the effectiveness and professionalism of Egmont members and candidates looking to join. This is handled in part by identifying, developing and providing technical support and training sessions for Egmont members.

The Egmont Group also provides a teaching platform called ECOFEL to make webinars and virtual workshops available on numerous topics relevant for the FIUs. In 2021, there were courses on “External FIU Communication”, “Financial Flows

of Online Child Sexual Exploitation” and “Financial Intelligence Unit (FIU) and Law Enforcement Authority (LEA) Cooperation”, among others.

⁴⁶ The original project names are in English as above.

International Cooperation Project – Follow-Up „Conclusions from large scale cross border Money Laundering schemes“

The most recent developments in international financial crime show that the topic of cross-border money laundering networks remains acute.⁴⁷

The FIU's Annual Report 2020 introduced the international strategic analysis project “Conclusions from large-scale, cross-border money laundering schemes”, which has been led by the FIU Germany in the Egmont Group since 2019. The aim of this project is to gain insights into the procedure of cross-border money laundering systems and networks identified in the past, so-called “laundromats”, and into approaches on how to use these in future to identify suspicious payment flows.

The content of the project is divided into three work strands. Work strand III involves the collection of practical knowledge, case studies and *modi operandi* from the “laundromat” context, with a thematic focus on trade-based money laundering. It was successfully completed at the end of 2020 and covered in the Annual Report 2020.

Work strands I and II focus on the data collection and analysis of transaction data:

The subject matter of work strand I is the creation of a project-internal database on potential shell companies that draws on data and information from FIUs participating in the project. The FIU Germany was supported on the domestic level by a partner authority that made data contributions. The project-internal database then served the participating FIUs as a basis for the risk-based identification of transaction data that are at the centre of the analysis work in work strand II.

The subject matter of work strand II is the consideration and analysis of transaction data. The project prepared a number of transaction-related risk indicators that were to be tested on a risk-based selected random sample of transaction data. The underlying idea was to empirically test these risk indicators on the largest possible amount of past and present transaction data by using a uniform testing method to examine whether and how these risk indicators actually apply to transaction data and which combinations between different indicators can be identified. Examples of transaction-based risk indicators were abnormalities in connection with transaction amounts or information on the purpose. According to the risk-based method, a uniform, risk-based random test selection process was defined for this international testing method and consisted of transactions where a potential shell company was involved.

By using a common, standardised testing approach that involves both the developed testing logic on the project side and the parameters for the individual risk indicators, the empirical testing method was carried out by the participating FIUs. Furthermore, the project also encouraged credit institutions in the countries participating in the project to cooperate with the testing method for transaction-related risk indicators. In Germany, the FIU introduced this initiative in the AFCA to inform prospective credit institutions and win them for participation in the empirical testing method. The initiative of the project proved to be more than successful – with a total of 19 credit institutions from seven countries, including Germany, taking part in the analyses.

⁴⁷ For the latest indications in connection with cross-border money laundering networks, also see the explanatory remarks on “International Cooperation – Indications of a Potentially Active International Money Laundering Network (‘Laundromat’)” under “Information Exchange with Other FIUs” in this section.

In the empirical testing method, it was therefore possible to include more than 1.6 million transactions in the analysis of the project by using standardised decentralised data analyses. The results delivered by the FIUs and credit institutions are consolidated and analysed under the leadership of the FIU Germany.

The conclusion of the project is planned for the beginning of 2022. The findings gained in the project bundle together wide-ranging, valuable knowledge in regards to the approaches taken by internationally operating money laundering networks, and are intended to prevent and actively combat money laundering. The project work promotes international collaboration and knowledge transfer across borders, making a valuable contribution in the common fight against international money laundering.

EU FIUs Platform

The platform for central agencies of the EU (EU-FIUs platform) was set up by the European Commission in 2006 and is intended to facilitate the exchange of information between the EU-FIUs and to promote their cooperation. The FIU Germany is a permanent member in this body.

The FIU Germany was also able to make valuable contributions to the regularly occurring expert rounds in this year, especially by presenting the current state of discussion in the so-called “CSM Working Group” led by the FIU Germany and a subgroup of the FIU platform to address the latest developments in the fight against money laundering on the EU level.⁴⁸

Furthermore, the FIU was able to successfully add its expertise in the supranational risk analysis (SNRA) and in the preparation of the workplan for 2022-2023. For example, topic proposals were

made where the main objective is to strengthen the cooperation of FIUs at the EU level, e.g., through a project that examines the existing and, moreover, desirable technical tools for FIUs and carries out an exchange in the sense of “best practice”.

The FIU Germany also joined another sub-working group on the platform. Since December 2021, the FIU Germany has been a member of the FIU.net working group on the European level. FIU.net is the communication channel that enables European FIUs to exchange data and information between each other. In the working group, there are representatives from six other EU-FIUs as well as the European Commission who address the optimisation, further development and strategic needs of the communication channel FIU.net.

⁴⁸ For more information on the CSM Working Group, see the explanatory remarks in the following section.

CSM-Working Group

The cooperation of the European FIUs increased as part of the “Coordination and Support Mechanism” (CSM) Working Group, an association of a total of eleven FIUs under the leadership of the FIU Germany, – and against the background of the newly published EU package⁴⁹ of legislative proposals to combat money laundering and terrorist financing in 2021.

The CSM Working Group, founded on the EU-FIU platform in September 2020, discusses the planned legislative proposals of the European legislative package (“AML Package”) in regular virtual meetings and prepares common opinions on the regulations particularly relevant to EU-FIUs. This includes, for example, the establishment of an EU Anti-Money Laundering Authority (AMLA) for fighting money laundering and terrorist financing

as a central EU regulation agency. Likewise, the legislative package includes rules for designing the reporting processes and procedures for suspicious cases and in regards to the competent EU joint analysis teams. This is a coalition of multiple EU-FIUs on the operational level and the cooperation of analysts from various EU-FIUs on the collective topic of European-wide phenomena of money laundering and terrorist financing.

The publications of the CSM Working Group are means of information and argumentation guide-lines for the EU-FIUs and the European Commission, and are used to support the work of ministries, authorities and agencies involved in the legislative processes.

Europol Financial Intelligence Public Private Partnership (EFIPPP)

On the international level, the FIU is also involved in cooperations with the public sector and the private economy. The EFIPPP is the first transnational mechanism for exchanging financial information in the area of fighting money laundering and terrorist financing. Launched in December 2017 at the initiative of Europol and the Institute of International Finance (IIF), the EFIPPP project includes experts from 15 major banks and competent authorities in eight states, including ones outside of the EU (BE, CH, DE, ES, FR, NL, UK, US) and the FIUs and law enforcement agencies. The focal points of the EFIPPP were new methods and typologies in money laundering and terrorist financing, proliferation, virtual currencies and virtual assets in 2021.

EFIPPP views itself as a hub and information pool in the fight against money laundering and terrorist financing. The main objectives include supporting domestic public-private partnerships (PPPs) and developing common “intelligence” and an understanding of criminal threats and risks. Gateways for the exchange of information should be determined and the exchange of operational and tactical information should be facilitated. EFIPPP supports, coordinates and initiates international measures and promotes the use of new tools and technologies.

The focal points were discussed and prepared in the working groups Legal Gateways, Threats & Technologies, Innovations and COVID-19.

49 See in this regard https://ec.europa.eu/info/publications/210720-anti-money-laundering-counteracting-financing-terrorism_en.

Besides regular participation in the quarterly EFIPPP plenary sessions, involvement in individual working groups and various surveys (e.g., Threats Radar, Annual Report) and studies, the FIU Germany has also supported the EFIPPP on staffing issues in its organisational and project-oriented daily work since the end of the year.

The heavy involvement of the FIU in PPPs on the national (AFCA) and international (EFIPPP) level is a strategic step in the creation of synergies and in bundling and increasing the FIU's expertise in the analysis and fight against money laundering and terrorist financing both nationally and internationally.

List of Figures

Figure	Title	Page
1	Process Sequence in Operational Analysis	14
2	Development of the Number of STRs according to the AMLA (2011 - 2021)	15
3	Relative Share of STRs Potentially Related to Terrorist Financing or State Security	16
4	Total Number of Registered Reporting Entities and Portion in Financial Sector	18
5	Breakdown of Reports by Recipients of Disseminations	21
6	Breakdown of Analysis Reports Disseminated to the Federal States	21
7	Number of Feedback Reports from Public Prosecution Authorities	22
8	Overview of the Convictions, Penalty Orders, Decisions und Indictments	22
9	Foreign Involvement in Suspicious Transactions	26
10	Number of Suspicious Transactions by Country of Origin	27
11	Number of Suspicious Transactions by Country of Destination	28
12	Key Risk Areas of the FIU	30
13	Received Suspicious Transaction Reports with Reference to COVID-19	32
14	Case Study – Billing Fraud with Corona Testing Centres	34
15	Case Study – Real Estate	40
16	Total Number of Reports and Notifications in the Key Risk Area of Serious (Tax) Criminal Acts	42
17	Simplified Representation of a VAT Carousel	43
18	Case Study – Carousel Fraud	45
19	Suspicious Transaction Reports with the Reason for Suspicion Being “Abnormalities in Connection with Virtual Currencies“	47
20	Case Study – Financial Agent Activity in Connection with Virtual Assets	48
21	Case Study – Suspicious Use of Intermediary Payment Instruments	50
22	Means of Transport as Percentage of Cash Discoveries	55
23	National Partner Authorities – An Overview	58
24	FIU LO	60
25	Case Study – Art Deals	63
26	Percentage of Disseminated Reports on Actions to Involved Groups of Supervisory Authorities in accordance with Section 50 AMLA	64
27	Incoming Domestic Requests	66
28	Breakdown of Domestic Requests by Sender	66
29	Case Study – Requests from Domestic Authorities	67
30	Domestic Requests related to Terrorist Financing and State Security	69
31	Breakdown of Domestic Requests related to Terrorist Financing and State Security by Sender	69
32	Membership Structure of the AFCA in 2021	73
33	Structure of the AFCA	74
34	Cases of International Cooperation in a Year-on-Year Comparison	77
35	Request and Spontaneous Information in Year-on-Year Comparison	78
36	Incoming Cases of International Cooperation by Country of Origin	80
37	Outgoing Cases of International Cooperation by Country of Destination	81
38	Case Study – International Requests	83
39	Cross-border Information Exchange with connection to Terrorist Financing or State Security	85
40	International Committees	87

List of Tables

Table	Title	Page
1	Number of STRs according to Subgroups of Reporting Entities	17
2	Number of Active Reporting Entities	19
3	Share of Disseminated STRs	20
4	Number of Incoming and Outgoing Requests Broken down by Countries	82
5	Number of Incoming and Outgoing Spontaneous Information Cases Broken down by Countries	82
6	Number of Incoming and Outgoing Requests with Connection to Terrorist Financing or State Security, Broken down by Countries	86
7	Number of Incoming and Outgoing Spontaneous Information Cases with Connection to Terrorist Financing or State Security, Broken down by Countries	86

List of Abbreviations

Abbreviation	Explanation
AFCA	Anti Financial Crime Alliance
AMLA	Anti-Money Laundering Authority
AO	German Tax Code, valid in the version dated 1 October 2002, as last amended by Article 33 of this Act on 5 October 2021
BaFin	Federal Financial Supervisory Authority
BfV	Federal Office for the Protection of the Constitution
BGBL	Federal Law Gazette
BKA	Federal Criminal Police Office
BMF	Federal Ministry of Finance
BND	Federal Intelligence Service
CSM	Coordination and Support Mechanism
DeFi	Decentralised Finance, decentralised financial services
EFIPPP	Europol Financial Intelligence Public Private Partnership
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit / Central Agency for Financial Transaction Investigation
GW	Money Laundering
GwG	Money Laundering Act of 23 June 2017, as last amended by Article 92 of the Act of 10 August 2021
GwG-MeldV-Immobilien	Ordinance on Matters in the Real Estate Sector Subject to Reporting under the Anti-Money Laundering Act of 20 August 2020
GZD	Central Customs Authority
IEWG	Information Exchange Working Group
IIF	Institute of International Finance
ITZBund	Federal Information Technology Centre
LEA	Law Enforcement Authority
LKA/LKÄ	State Office(s) of Criminal Investigation
MAD	Military Counter-Intelligence Service
MSCWG	Membership, Support and Compliance Working Group
NFT	Non-Fungible Token
NGO	Non Governmental Organisation
NPO	Non Profit Organisation
NPS	New psychoactive substances
PPP	Public Private Partnership
PPWG	Policy and Procedures Working Group
RBA	Risk-based approach

Abbreviation	Explanation
SNRA	Supranational Risk Analysis
StGB	Criminal Code in the version promulgated on 13 November 1998, as last amended by Article 2 of the Act of 22 November 2021
StPO	Code of Criminal Procedure in the version promulgated on 7 April 1987, last amended by Article 2 of the Act of 25 March 2022
TATWG	Technical Assistance and Training Working Group
TF	Terrorist Financing
UstG	Value Added Tax Act in the version of the announcement of 21 February 2005, last amended by Article 1 of the Act of 21 December 2021
FIU LO	Liaison Officers of the FIU
ZollVG	Customs Administration Act of 21 December 1992, as last amended by Article 6 (6) of the Act of 5 July 2021

■ LEGAL NOTICE:

Published by:

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

Edited by:

Central Customs Authority (GZD)

Design and creation:

Central Customs Authority (GZD), Training and Science Centre of the Federal Revenue Administration

Registration number:

90 SAB 272

www.zoll.de

Cologne, January 2023

www.fiu.bund.de