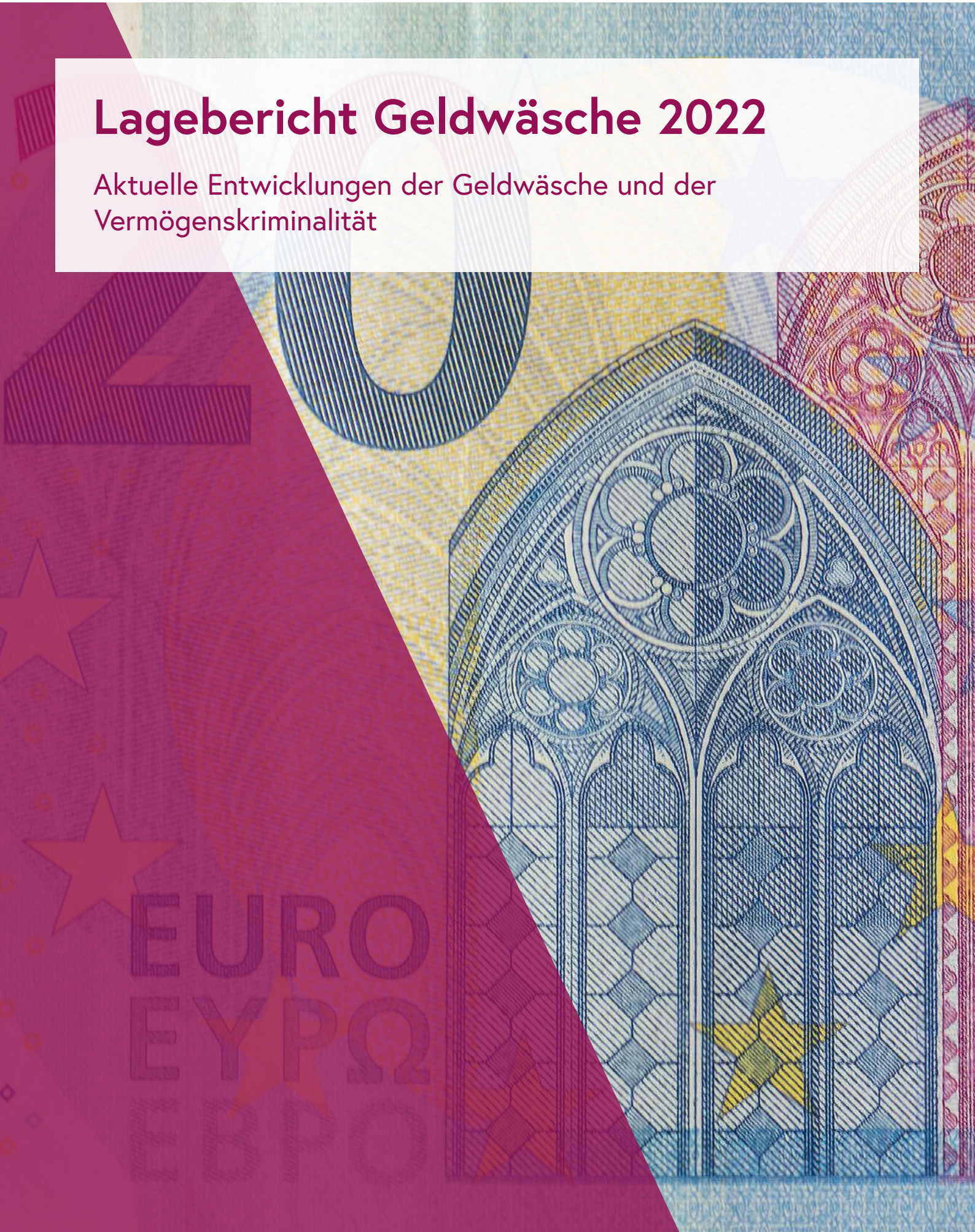
Bundesministerium
Inneres

Bundeskriminalamt

Lagebericht Geldwäsche 2022

Aktuelle Entwicklungen der Geldwäsche und der Vermögenskriminalität



Lagebericht Geldwäsche 2022

Aktuelle Entwicklungen der Geldwäsche und derVermögenskriminalität

Wien, im Oktober 2023

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres/Bundeskriminalamt
Josef-Holaubek-Platz 1, 1090 Wien
+43 1 24 836 985025
bundeskriminalamt.at
Autor: Rat Louis Verdier
Fotonachweis: Bundeskriminalamt/Armin Halm
Layout: Armin Halm
Druck: Digital-Print-Center des BMI, Herrengasse 7, 1010 Wien
Wien, im Oktober 2023

Vorwort

Liebe Interessierte!

Generaldirektor für die öffentliche Sicherheit Mag. Dr. Franz Ruf MA

Das Jahr 2022 hat die Geldwäschemeldestelle im Bundeskriminalamt (A-FIU) vor zahlreiche neue Herausforderungen gestellt. Zwar verschwanden die für die Vorjahre so prägenden Betrugsphänomene im Zusammenhang mit der Covid-19-Pandemie, doch drängte sich ab Februar 2022 ein ganz anderes Aufgabenfeld ins Zentrum. Der russische Angriffskrieg auf die Ukraine und die ihm nachfolgenden Sanktionspakete der Europäischen Union führten zu einem empfindlichen Anstieg an dazu gemeldeten Sachverhalten. Zur Umsetzung der Sanktionsmaßnahmen unterstützte das Bundeskriminalamt die zuständigen Behörden auch mit kriminalpolizeilicher Expertise und mit Daten, deren Koordinierung die Geldwäschemeldestelle übernahm.

Direktor des Bundeskriminalamtes General Mag. Andreas Holzer MA

Die Entwicklungen des Jahres 2022 zeigen, wie groß das Risiko ist, dass der Finanzplatz für die Wäsche und die Ausleitung von Betrugsgeldern missbraucht wird. Internettelefonie, Messengerdienste und Echtzeitüberweisungen haben unser Wirtschaftsleben derart beschleunigt und anonymisiert, dass sich das Betrugsgeschehen immer weiter in die Onlinewelt verlagert. Weil diese Kriminalitätsform immer häufiger der Geldwäsche vorangeht, werden das Bundeskriminalamt und die A-FIU künftig einen Schwerpunkt auf Prävention und Verfolgung der Betrugskriminalität legen.

Die Kooperationen der Geldwäschemeldestelle mit ihren Partnern aus der Privatwirtschaft und der Behördenwelt haben sich auch heuer weiter vertieft. Die in den Jahren der Corona-Pandemie rasant gewachsene Schwarzarbeit im Bausektor ist äußerst kapitalintensiv. Der enorme Bedarf an Bargeld zur Bezahlung der Schwarzarbeitenden machte einen verstärkten Informationsaustausch mit Banken nötig. Sie sollten dadurch Scheinunternehmen innerhalb ihrer Kundschaft rascher erkennen und melden können. In intensiver Kooperation mit der Bundesfinanzverwaltung ist es der Geldwäschemeldestelle gelungen, einige dieser Geldkreisläufe durch Sicherstellungen zu unterbrechen.

Wir möchten uns bei allen Mitarbeitenden der A-FIU und des Büros für Betrugskriminalität für ihren Einsatz bedanken. Sie haben es in einer Welt der sich ständig wandelnden Vermögenskriminalität und der dauernden technischen Weiterentwicklung geschafft, unermüdlich gegen Geldwäscherei und ihre Vortaten vorzugehen.

Ihr

Mag. Dr. Franz Ruf MA
Generaldirektor für die öffentliche Sicherheit

General Mag. Andreas Holzer MA, Direktor des Bundeskriminalamtes

Inhalt

1 Einleitung

Der vorliegende Jahresbericht bietet einen umfassenden Überblick über die Geldwäschemeldestelle im Bundeskriminalamt (Internationale Bezeichnung: Austrian Financial Intelligence Unit – A-FIU), sowie über ihre Aufgaben, Leistungen und Erfolge im Jahr 2022.

Die Analysen der Geldwäschemeldestelle zeigen, dass Onlinebetrug, Sozialmissbrauch und Abgabenhinterziehung in Form von Scheinunternehmen immer häufiger als Vortaten zur Geldwäscherei auftreten. Dem risikobasierten Ansatz folgend, widmet sich der heurige Bericht diesen Delikten in einem eigenen Kapitel.

Das Phänomen Geldwäsche

Ausgangspunkt jeder Geldwäscherei ist der Besitz von illegal erworbenen Vermögenswerten, die durch Steuerhinterziehung, Betrug, Menschen- oder Drogenhandel, Korruption oder durch andere Straftaten erwirtschaftet wurden. Ziel der Geldwäsche ist es, diese gleichsam „schwarzen" Vermögenswerte dem Zugriff der Behörden zu entziehen. Zu diesem Zweck wird das Schwarzgeld durch eine Reihe möglichst unauffälliger und meist komplexer Transaktionen im Kreis geschickt. Das soll den Behörden erschweren, die illegale Herkunft der Vermögenswerte zu erkennen. Am Ende dieses Prozesses kann das „weißgewaschene" Vermögen wieder in den legalen Wirtschaftskreislauf überführt werden, ohne dabei die Aufmerksamkeit der Behörden auf sich zu ziehen.

Das Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC) unterscheidet drei Phasen des Geldwäscheprozesses:

- Platzierung („Placement"),
- Schichtung („Layering") und
- Reintegration („Reintegration")

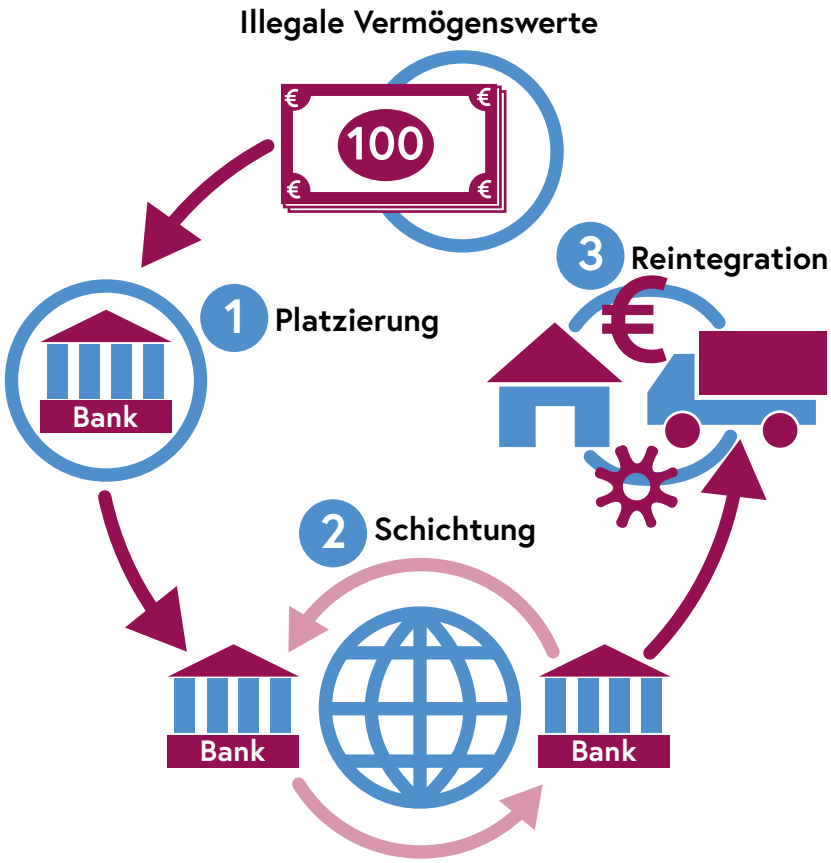
Der erste Schritt (Platzierung) dient dazu die illegalen Vermögenswerte in den legalen Finanzkreislauf einzuschleusen. Um möglichst keine Aufmerksamkeit zu erregen, erfolgt die Platzierung regelmäßig in kleineren Teilbeträgen, dem sogenannten „smurfing". Einzahlungen können direkt auf Bankkonten, bei Spielbanken, Wechselstuben oder bei anderen Wirtschaftsteilnehmern erfolgen. Die Platzierung bildet die riskanteste Phase des Geldwäscheprozesses, denn sie birgt das größte Risiko der Enttarnung.

Im zweiten Schritt (Schichtung) wird das Schwarzgeld in einer Reihe von Transaktionen im Kreis geschickt, sodass seine illegale Herkunft immer schwerer nachzuvollziehen ist: Mit jeder Transaktion, also mit jedem weiteren Waschgang, wird das Schwarzgeld ein bisschen „weißer" und die Verschleierung erfolgreicher. Beliebte Mittel zur Durchführung der Transaktionen sind Offshore-Banken, Scheingeschäfte, Briefkastengesellschaften, Strohleute und immer öfter Kryptowährungen.

Ist das inkriminierte Vermögen einmal „weißgewaschen“ und der Anschein eines legalen Ursprungs erweckt, folgt die letzte Phase (Reintegration): Das Vermögen wird im legalen Wirtschaftskreislauf ausgegeben und beispielweise für den Kauf von Luxusgütern oder Unternehmensanteilen verwendet.

Welcher Anteil der Wirtschaftsleistung aus illegalen Quellen stammt, ist schwer zu beziffern. UNODC schätzt, dass zwei bis fünf Prozent des Weltbruttoinlandproduktes aus Geldwäschehandlungen stammen, was einer Summe zwischen 715 Milliarden und 1,87 Billionen Euro pro Jahr entspricht.

Grafische Darstellung eines typischen Geldwäscheprozesses



2 Kampf gegen die Geldwäsche

Zur Bekämpfung der Geldwäsche verfolgt der Gesetzgeber einen mehrdimensionalen Ansatz: Im Sinne der Prävention sind Berufsgruppen, die besonders geldwäschegeneigte Geschäfte abwickeln (sogenannte „Verpflichtete“ oder „meldepflichtige Berufsgruppen“), zur Einhaltung bestimmter Sorgfalts- und Meldepflichten angehalten. Gleichzeitig setzt der Gesetzgeber auf Repression und kriminalisiert unter dem Titel der Geldwäscherei (§165 Strafgesetzbuch – StGB) das Verbergen oder Verschleiern von Vermögensbestandteilen, die aus bestimmten Straftaten herrühren.

Sorgfaltspflichten der Verpflichteten

Als besonders risikobehaftete Berufsgruppen gelten etwa Banken und andere Dienstleister am Finanzmarkt, Wirtschaftstreuhand-, Bilanzbuchhaltungs- und rechtsberatende Berufe, Immobilienmaklerinnen und Immobilienmakler sowie Dienstleistende in Bezug auf virtuelle Währungen, umgangssprachlich auch „Exchanger“ genannt. Sie haben unüblichen Transaktionen und Transaktionsmustern ohne erkennbaren wirtschaftlichen oder rechtmäßigen Zweck sowie risikobehafteter Kundschaft besondere Aufmerksamkeit zu widmen.

Das Finanzmarkt-Geldwäschegesetz (FM-GwG) enthält zahlreiche Bestimmungen zur Verhinderung und Bekämpfung von Geldwäscherei und Terrorismusfinanzierung für die Berufsgruppe der Kredit- und Finanzdienstleister sowie Exchanger. Dieses Gesetz dient regelmäßig als Vorbild für die Sorgfaltspflichten der anderen Berufsgruppen. Deren Sorgfaltspflichten sind teilweise gleichlautend in der Rechtsanwaltsordnung, der Gewerbeordnung oder dem Wirtschaftstreuhandberufsgesetz verankert.

Die wesentlichsten Sorgfaltspflichten der meldepflichtigen Berufe umfassen:

Unternehmensbezogene Risikoanalyse

- Diese dient dazu, das Risiko für das Unternehmen einschätzen zu können, von Dritten für Geldwäscherei oder Terrorismusfinanzierung missbraucht zu werden.

Know-your-Customer-Prinzip (KYC)

- Geldwäscherinnen und Geldwäscher sollen möglichst keine Anonymität genießen. Die KYC-Regeln verpflichten daher dazu, Kundinnen und Kunden möglichst gut zu kennen, um so rasch Änderungen ihrer Verhaltensmuster erkennen zu können. Im Rahmen des KYC hat beispielsweise eine Identitätsprüfung der Kundschaft, die Feststellung des Zwecks der Geschäftsbeziehung oder einer Transaktion zu erfolgen.
- Die verpflichtende Überprüfung der Mittelherkunft, indem etwa Nachweise und Urkunden über deren Ursprung verlangt werden, dient dazu, den Eintritt von Schwarzgeld in den legalen Finanzkreislauf möglichst zu erschweren.

- Das KYC-Prinzip dient als Grundbaustein aller Sorgfaltspflichten, auf dem auch die verpflichtende kundenbezogene Risikoanalyse basiert.

Meldepflicht

- Entsteht bei den meldepflichtigen Berufsgruppen der berechtigte Grund zur Annahme, dass ein Geschäft in Zusammenhang mit Geldwäscherei oder mit Terrorismusfinanzierung steht, sind sie zur Erstattung einer Verdachtsmeldung an die A-FIU verpflichtet. Steht der konkrete Geschäftsfall oder die Transaktion noch bevor, kann von der A-FIU eine Entscheidung darüber verlangt werden, ob gegen die unverzügliche Durchführung Bedenken bestehen. Äußert sich die A-FIU nicht bis zum Ablauf des folgenden Bankarbeits- oder Werktags, darf das Geschäft nicht abgewickelt werden.

Auskunftsverpflichtung gegenüber der A-FIU

- Alle Verpflichteten haben mit der Geldwäschemeldestelle zusammenzuarbeiten und ihr auf Verlangen – ungeachtet einer zuvor erstatteten Verdachtsmeldung – alle erforderlichen Auskünfte zu erteilen, die ihr zur Verhinderung oder zur Verfolgung von Geldwäscherei oder von Terrorismusfinanzierung erforderlich scheinen.

Die Melde- und Auskunftsverpflichtung gegenüber der A-FIU bilden den zentralen Ausgangspunkt für die Aufgabenerfüllung der Geldwäschemeldestelle. Die Überprüfung der Einhaltung der beschriebenen Sorgfaltspflichten hingegen obliegt den jeweiligen Aufsichtsbehörden. Im Finanzdienstleistungssektor übernimmt diese Aufgabe die Finanzmarktaufsicht (FMA), für Angehörige der rechtsberatenden Berufe und Wirtschaftstreuhandberufe deren jeweilige Kammern. Handelsgewerbetreibende, Unternehmensberatende sowie Immobilienmaklerinnen und Immobilienmakler werden von den Gewerbebehörden beaufsichtigt.

Das Delikt Geldwäscherei – § 165 Strafgesetzbuch

Im Jahr 2021 erfolgte eine Novellierung des Geldwäscherei-Tatbestands in § 165 StGB. Diese erfolgte in Umsetzung der EU-Richtlinie 2018/1673 über die strafrechtliche Bekämpfung der Geldwäsche, die die Harmonisierung der europäischen Geldwäscherei-Tatbestände vorantreibt, indem sie zum Beispiel strengere Freiheitsstrafen vorsieht. Die neuformulierten Kombinationen der verschiedenen Tathandlungen und ihrer jeweils zugehörigen Vorsatzstufen sind durch diese Novelle in ihrer Komplexität noch einmal gestiegen, weshalb sie hier nur verkürzt dargestellt werden.

Gemäß § 165 Absatz 1 StGB ist mit Freiheitsstrafe von bis zu fünf Jahren zu bestrafen,

- wer Vermögensbestandteile, die aus bestimmten schweren Straftaten stammen, entweder umwandelt oder einem überträgt, und zwar um den illegalen Ursprung des Vermögens zu verschleiern oder um den Täter dabei zu unterstützen sich der Strafverfolgung zu entziehen, oder
- wer die wahre Natur, Herkunft oder Lage von Vermögensbestandteilen, die aus bestimmten schweren Straftaten stammen, verheimlicht oder verschleiert.

Beispiel für die erste Form der Tatbegehung ist eine Frau, die mit den Erträgen eines Drogengeschäfts ins Casino geht und das Geld über ein paar risikolose Roulettespiele in vermeintlich sauberes Geld umwandelt. Oder ein Finanzagent (Money Mule), der Gelder, die aus Betrugshandlungen stammen und auf seinem Konto eingelangt sind, wiederum an andere Money Mules weitertransferiert. Die zweite Form der Tatbegehung liegt beispielsweise vor, wenn eine gewerbsmäßige Kfz-Diebesbande ihre gestohlenen Autos umlackiert und falsche Kennzeichen montiert, um die wahre Natur und Herkunft des Diebesguts zu verschleiern.

Nach § 165 Absatz 2 StGB macht sich strafbar, wer Vermögensbestandteile bloß erwirbt, besitzt, umwandelt oder einem anderen überträgt, von denen er weiß, dass sie aus bestimmten schweren Straftaten stammen.

Alle diese Formen der Geldwäscherei stellen darauf ab, dass die zu waschenden Vermögensbestandteile aus bestimmten schweren Straftaten stammen. Nicht jeder Vermögensbestandteil ist also geldwäschetauglich. Nur wenn der betreffende Vermögensbestandteil aus gerichtlich strafbaren Handlungen stammt, die mit mehr als einjähriger Freiheitsstrafe bedroht sind oder aus den §§ 223, 229, 289, 293, 295 StGB oder §§ 27 oder 30 Suchtmittelgesetz stammt, ist Geldwäscherei überhaupt möglich. Diese Vorbedingung macht die Geldwäscherei zu einem sogenannten „Anschlussdelikt".

Für die Strafbarkeit nach Absatz 1 ist es irrelevant, ob die Geldwäsche durch dieselben Täter begangen wird, wie das vorgelagerte Delikt (sogenannte Eigengeldwäsche) oder ob sie durch Dritte erfolgt (sogenannte Fremdgeldwäsche). Auch wer versucht, den illegalen Ursprung seiner eigenen Schwarzgelder durch komplexe Transaktionen über die eigenen Konten zu verschleiern, kann sich der Geldwäscherei strafbar machen.

Zuletzt macht sich gemäß § 165 Absatz 3 StGB auch strafbar, wer wissentlich Vermögensbestandteile an sich bringt, verwahrt, anlegt oder verwaltet, die der Verfügungsmacht einer kriminellen Organisation oder einer terroristischen Vereinigung unterliegen. Wegen der hohen kriminellen Energie derartiger Gruppierungen und der von ihr ausgehenden Gefahren kommt es bei dieser Begehungsform auf das Vorliegen einer geldwäschereitauglichen Vortat nicht an.

3 Die Geldwäschemeldestelle

Wie nahezu alle Staaten dieser Welt besitzt auch Österreich eine zentrale Stelle für die Entgegennahme und Analyse von Sachverhalten im Zusammenhang mit Geldwäscherei, ihren Vortaten oder mit Terrorismusfinanzierung. Die Geldwäschemeldestelle (A-FIU) ist im Bundeskriminalamt angesiedelt. Sie bildet in ihrer Zentralstellenfunktion die einzige Ansprechstelle für meldepflichtige Berufsgruppen bei den Sicherheitsbehörden in Sachen Geldwäsche.

Funktionen der A-FIU

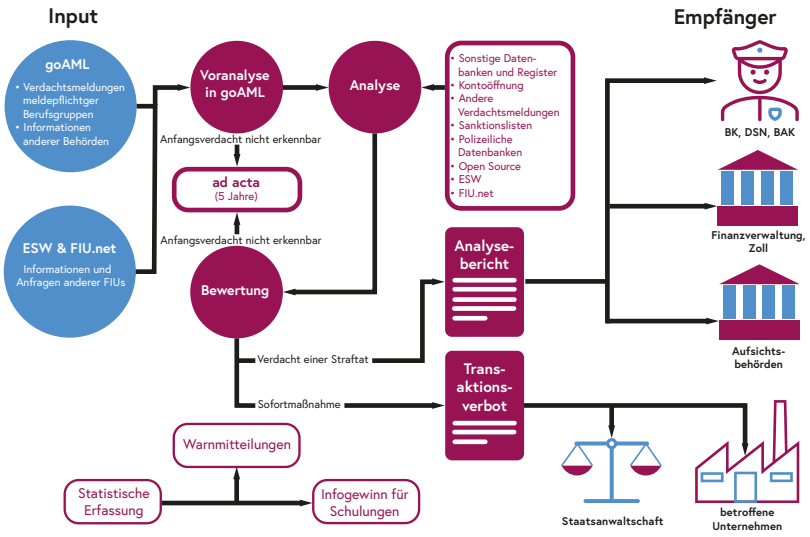
Filterfunktion

Eine Kernfunktion der A-FIU liegt in ihrer – den Strafverfolgungsbehörden vorgelagerten – Filtertätigkeit: Nicht jede der zahlreichen einlangenden Informationen ist geeignet, an die Strafverfolgungsbehörden übermittelt zu werden. Der Grund dafür liegt darin, dass eine Verdachtsmeldung an die A-FIU schon dann zu erstatten ist, wenn der „berechtigte Grund zur Annahme" besteht, dass ein Geschäft oder eine Transaktion im Zusammenhang mit Geldwäscherei oder Terrorismusfinanzierung steht. Diese Meldeschwelle ist vergleichsweise niedrig, denn ein Ermittlungsverfahren nach den Regeln der Strafprozessordnung beginnt erst bei Vorliegen eines konkreteren „Anfangsverdachts".

Logo der österreichischen Geldwäschemeldestelle A-FIU

Die niedrige Schwelle der Meldepflicht führt zu einem hohen Informationsaufkommen aufseiten der A-FIU. Die Geldwäschemeldestelle muss daher aus den zahlreichen übermittelten Verdachtsmeldungen jene erkennen, denen mit hoher Wahrscheinlichkeit ein strafbarer Sachverhalt zugrunde liegt. Die einlangenden Informationen durchlaufen ein besonderes Analyseverfahren. Dieser Vorgang dient unter anderem dazu, die Strafverfolgungsbehörden zu entlasten, indem diesen nur solche Sachverhalte übermittelt werden, deren strafrechtliche Verfolgung aufgrund eines vorliegenden Anfangsverdachts gerechtfertigt ist.

Grafische Darstellung des Analyseprozesses



In einem ersten Schritt nimmt die A-FIU Meldungen von Verpflichteten über verdächtige Transaktionen und sonstige Informationen entgegen und überprüft sie auf ihre Relevanz in Hinblick auf Geldwäscherei, ihre Vortaten oder Terrorismusfinanzierung (Zulässigkeitsprüfung). Die Datenübermittlung erfolgt über die verschlüsselte Web-Applikation goAML.

Analyseverfahren

Bestätigt sich der Verdacht, dass eine Straftat begangen wurde oder weist der gemeldete Sachverhalt Verbindungen zu bereits bekannten Fällen auf, beginnt die zweite Kernaufgabe der A-FIU: Die Verdachtsmeldung wird vertieft analysiert.

Im Rahmen dieses Analyseverfahrens wertet die Geldwäschemeldestelle die übermittelten Informationen aus und zerlegt sie in ihre Bestandteile (Transaktionen, Transaktionsmuster, Mittelzufluss, Mittelabgang, Senderin oder Sender, Empfängerin oder Empfänger, Plausibilität und so weiter). Die übermittelten Informationen werden verifiziert und mit vorhandenen Datenbeständen abgeglichen. Die A-FIU überprüft ferner, ob weitere polizeiliche Erkenntnisse oder sonstige finanznachrichtendienstliche Informationen bekannt sind, die den gemeldeten Verdachtsfall verdichten. Ist es zur Verhinderung oder zur Verfolgung von Geldwäscherei oder Terrorismusfinanzierung erforderlich, holt die A-FIU ergänzende Auskünfte von den meldepflichtigen Berufsgruppen ein oder leitet einen internationalen Schriftverkehr mit ausländischen Partnerdiensten ein.

Die A-FIU ist jedoch nicht im Dienste der Strafrechtspflege tätig. Ermittlungshandlungen im Sinne der Strafprozessordnung stehen ihr nicht zu: Erhärtet sich aufgrund des Analyseverfahrens der Verdacht, dass eine Straftat begangen worden ist, leitet die Geldwäschemeldestelle ihr Analyseergebnis sowie zusätzliche relevante Informationen an die für Strafverfolgung zuständigen Stellen weiter. In Fällen vermuteter Terrorismusfinanzierung leitet die A-FIU ihr Analyseergebnis an die Direktion Staatsschutz und Nachrichtendienst (DSN) weiter, bei Verdacht auf Korruptionsdelikte an das Bundesamt für Korruptionsprävention und Korruptionsbekämpfung (BAK). Besteht der Verdacht der Geldwäscherei oder ihrer Vortaten, ist aber kein Zusammenhang mit besonderen Tatbeständen wie Sanktionsbrüchen, Steuerhinterziehung, Zollvergehen, Korruptionstatbeständen und dergleichen erkennbar, leitet die A-FIU das Analyseergebnis an die zuständigen Stellen im Bundeskriminalamt oder an die Landeskriminalämter (LKAs) weiter.

Quellenschutz wird bei der Informationsweitergabe großgeschrieben: Im Sinne des „No-Tipping-Off“ geht aus der weitergeleiteten Analyse nicht hervor, ob die verdachtsauslösende Information von einer meldepflichtigen Berufsgruppe übermittelt oder durch die A-FIU selbst erkannt wurde.

Erhärtet sich im Rahmen des Analyseverfahrens kein Verdacht einer strafbaren Handlung, legt die A-FIU die erhaltene Verdachtsmeldung für künftige Analysen ad acta. Nach längstens fünf Jahren sind die so ermittelten Daten zu löschen.

Den für ihre Aufgabenerfüllung notwendigen internationalen Informationsaustausch mit Partnerdiensten (ausländische FIUs) nimmt in Österreich ausschließlich die A-FIU wahr.

Befugnisse der A-FIU

Zur ordnungsgemäßen Erfüllung ihres Auftrags steht der Geldwäschemeldestelle eine Reihe von Befugnissen zur Verfügung, die wichtigsten sind Folgende:

Erheben, Verarbeiten, Übermitteln

Die A-FIU kann von den meldepflichtigen Berufsgruppen alle Auskünfte verlangen, die ihr zur Verhinderung oder zur Verfolgung von Geldwäscherei oder Terrorismusfinanzierung erforderlich scheinen. In diesem Zusammenhang gilt das Bankgeheimnis nicht. Die Auskunftspflicht besteht ungeachtet einer zuvor erstatteten Verdachtsmeldung.

Die Geldwäschemeldestelle ist befugt, alle erforderlichen Daten von natürlichen und juristischen Personen sowie von sonstigen Einrichtungen mit Rechtspersönlichkeit zu erheben und gemeinsam mit Daten operativ oder strategisch zu analysieren, die sie als Teil der Sicherheitsbehörden in Vollziehung von Bundes- oder Landesgesetzen bereits verarbeitet hat oder verarbeiten darf.

Zur Analyse bedient sich die A-FIU des speziellen Analysetools goAML, das von UNODC für den weltweiten Einsatz durch FIUs und speziell für die Analyse im Bereich der Geldwäsche entwickelt wurde. Neben der Analysefunktion bietet goAML den meldepflichtigen Berufsgruppen den Vorteil, Verdachtsmeldungen vereinfacht an die A-FIU zu übermitteln. Die Daten der Verdachtsmeldungen gelangen über goAML bereits strukturiert in die Datenverarbeitungssysteme der A-FIU, was die Manipulation der Informationen vereinfacht. Die Anschaffung und der Betrieb von goAML wird durch den Fonds für die innere Sicherheit der Europäischen Union kofinanziert.

Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert.

Logos von gAML und Fonds für die innere Sicherheit der Europäischen (ISF)

Ferner ist die A-FIU befugt, ihre Analyseergebnisse und jede andere relevante Information – unter Wahrung des Quellenschutzes – an inländische und ausländische Behörden oder Stellen weiterzuleiten, soweit dies zur Bekämpfung der Geldwäscherei, ihrer Vortaten oder von Terrorismusfinanzierung erforderlich ist.

Vorläufiges Unterbinden oder Aufschieben von Transaktionen

Im Falle der Erstattung einer Verdachtsmeldung zu einer laufenden oder unmittelbar bevorstehenden Transaktion haben die Verpflichteten bis zum Ende des nächstfolgenden Bank- oder Werktags mit der Abwicklung der Transaktion oder des Geschäfts zu warten. Ergänzend haben sie das Recht von der A-FIU eine Entscheidung dahingehend zu verlangen, ob gegen die unverzügliche Durchführung des Geschäfts Bedenken bestehen.

Kommt die A-FIU aufgrund ihrer Analyse zum Ergebnis, dass gegen die Abwicklung des Geschäfts oder der Transaktion Bedenken bestehen, so ist sie ermächtigt, diese mittels Anordnung vorläufig zu unterbinden. Darüber hinaus kann die A-FIU anordnen, dass Aufträge der Kundschaft über Geldausgänge nur mehr mit ihrer Zustimmung durchgeführt werden dürfen. Über eine derartige Anordnung ist die Staatsanwaltschaft ohne unnötigen Aufschub zu verständigen. Sie entscheidet dann, ob die Voraussetzungen für eine Beschlagnahme nach den strafprozessualen Vorschriften vorliegen und beantragt diese gegebenenfalls bei Gericht. Liegen die Voraussetzungen nicht vor, hat die A-FIU ihr Transaktionsverbot wieder aufzuheben. Mit der Entscheidung eines Gerichts über den Antrag auf Beschlagnahme beziehungsweise nach längstens sechs Monaten tritt die Anordnung der Geldwäschemeldestelle automatisch außer Kraft.

In der Praxis jedoch steht die A-FIU als Teil der Sicherheitsbehörden in direktem Kontakt mit den Staatsanwaltschaften, die über die dauerhafte Beschlagnahmung der bedenklichen Vermögenswerte zu entscheiden haben. Wenn die Geldwäschemeldestelle eine Transaktionssperre für notwendig erachtet, regt sie diese daher direkt bei der Staatsanwaltschaft an. Die Staatsanwaltschaft kann so von Beginn an über die dauerhafte Sicherstellung entscheiden und zwar ohne Dazwischentreten eines verwaltungsrechtlichen Transaktionsverbots der A-FIU. Die Vorgangsweise beschleunigt die Sicherstellung verdächtiger Vermögenswerte und vereinfacht den Rechtschutz für die Betroffenen.

Organisationsaufbau

Die Geldwäschemeldestelle ist in die Abteilung 7 (Wirtschaftskriminalität) des Bundeskriminalamts eingebettet und gliedert sich in drei Referate:

- Referat 7.3.1 – Internationale Angelegenheiten
- Referat 7.3.2 – Strategische Finanzstromanalyse
- Referat 7.3.3 – Operative Finanzstromanalyse

Das Referat Internationale Angelegenheiten ist für die international-strategische Zusammenarbeit auf dem Gebiet der Bekämpfung und Analyse von Geldwäsche und Terrorismusfinanzierung zuständig. Zu den Aufgaben des Referats zählen der internationale Austausch, die ständige Weiterentwicklung und die laufende Optimierung von technischen und rechtlichen Kooperations- und Kommunikationsmethoden zwischen der A-FIU und ihren weltweiten Partnerbehörden.

Das Referat Strategische Finanzstromanalyse betrachtet Meldungen und sonstige Informationen aus strategischer Sicht. Ihm obliegt die fallübergreifende (und nicht auf den Einzelfall beschränkte) Darstellung von Mustern und Trends, das Erkennen von Typologien zur Verhinderung und Bekämpfung von Geldwäscherei oder Terrorismusfinanzierung sowie

die Darstellung aktueller Phänomene im Bereich der Geldwäsche. Diese Erkenntnisse werden den Meldeverpflichteten regelmäßig weitergeleitet und dienen der Bewusstseinsbildung bei den meldepflichtigen Berufsgruppen sowie der frühzeitigen Erkennung von strafrechtlich relevanten Sachverhalten.

Dem Referat Operative Finanzstromanalyse obliegt die Entgegennahme der Verdachtsmeldung und die Durchführung des Analyseverfahrens. Es wertet die übermittelten Informationen aus, zerlegt sie in ihre Bestandteile und gleicht gewonnene Informationen mit den vorhandenen Datenbeständen ab. Anschließend überprüft das Referat Operative Finanzstromanalyse, ob weitere polizeiliche Erkenntnisse oder sonstige finanznachrichtendienstliche Informationen bekannt sind, die den gemeldeten Verdachtsfall verdichten. Im Berichtsjahr waren durchschnittlich 25 Mitarbeitende in der A-FIU beschäftigt.

4 Europäische und internationale Kooperationen

Durch die Globalisierung der Wirtschaft ist die A-FIU vielfach mit grenzüberschreitenden Straftaten konfrontiert, deren erfolgreiche Bekämpfung eine enge internationale Kooperation erfordert. Eine vertrauensvolle Zusammenarbeit mit ausländischen FIUs und Organisationen ist daher wesentlich. Die A-FIU nützt unterschiedliche Foren, um die Kontakte zu ihren internationalen Partnern aufzubauen und zu vertiefen.

Besonders intensiv wurde 2022 in den verschiedenen internationalen Gremien, denen auch die A-FIU angehört, die Frage diskutiert, wie man mit dem Organisationsmitglied Russland umgehen solle. Angesichts seines flagranten Völkerrechts- und damit verbundenen Vertrauensbruchs ist für viele Staaten fraglich, ob Russland noch in gleicher Weise in den internationalen Informationsaustausch eingebunden sein kann.

European Financial Intelligence Public-Private Partnership (EFIPPP)

Logo European Financial Intelligence Public-Private Partnership (EFIPPP)

Im Kampf gegen die Geldwäsche spielen sogenannte Public-Private-Partnerships (PPPs) eine immer wichtigere Rolle. Bei vertraulichen und regelmäßigen Treffen zwischen öffentlichem und privatem Sektor sollen Informationen ausgetauscht werden, die beiden Seiten das Erkennen von bestimmten Trends und Mustern der Geldwäsche erleichtern sollen. PPPs finden sowohl auf internationaler als auch auf nationaler Ebene statt.

2017 initiierte Europol die European Financial Intelligence Public-Private Partnership (EFIPPP). Sie bringt auf europäischer Ebene Interessensvertretende aus den unterschiedlichsten Bereichen zusammen. In diesem Forum sind 79 Institutionen wie FIUs und Banken aus 18 EU- und Nicht-EU-Ländern vertreten. EFIPPP dient zum einen dem Austausch aktueller strategischer Informationen auf multilateraler Ebene und bietet zum anderen aber auch die Möglichkeit zu persönlichen Treffen mit Expertinnen und Experten. Die A-FIU war auch 2022 bei EFIPPP-Treffen in Den Haag vertreten.

Egmont-Gruppe

Logo Egmont-Gruppe

Die Egmont-Gruppe ist ein weltweiter Zusammenschluss von 166 nationalen FIUs mit Hauptsitz in Toronto. Egmont hat sich insbesondere den operativen Herausforderungen der FIUs verschrieben und bietet ihnen das sogenannte Egmont Secure Web (ESW) an. Das System ermöglicht es allen teilnehmenden FIUs Informationen gesichert auszutauschen. Zusätzlich organisiert sich Egmont in verschiedenen Arbeitsgruppen und fördert dadurch ein einheitliches globales Verständnis davon, wie man effektiv Geldwäsche und Terrorismusfinanzierung bekämpfen kann. Die Arbeitsgruppen widmen sich folgenden Themen:

Information Exchange on Money Laundering/Terrorist Financing Working Group (IEWG)

- Diese Arbeitsgruppe dient dazu, den Informationsaustausch zwischen den FIUs zu verbessern. Das geschieht in Form von Projektgruppen, an denen verschiedene Expertinnen und Experten teilnehmen und die ihre Erfahrungen im operativen und technischen Bereich teilen. Die Ergebnisse werden präsentiert und anschließend den Mitgliedern zur Verfügung gestellt.

Membership, Support and Compliance Working Group (MSCWG)

- Diese Arbeitsgruppe beschäftigt sich mit der Neuaufnahme, der bestehenden Mitgliedschaft, mit den Verfehlungen und der Unterstützung von FIUs innerhalb der Egmont-Gruppe.

Policy and Procedures Working Group (PPWG)

- Diese Arbeitsgruppe ist für die Bearbeitung und Weiterentwicklung von operativen, regulatorischen und strategischen Aufgaben verantwortlich.

Technical Assistance and Training Working Group (TATWG)

- Sie ist für die Identifizierung, Entwicklung und Umsetzung technischer Möglichkeiten und für Trainings verantwortlich, die sich bei Egmont-Mitgliedern im Zusammenhang mit der Einhaltung der Egmont-Standards und der für FIUs relevanten Empfehlungen von internationalen Organisationen ergeben.

Im Juli 2022 fand in Riga das erste persönliche Treffen der Egmont-Gruppe seit dem Ausbruch der Covid-19-Pandemie statt, bei der die österreichische FIU vertreten war.

Financial Action Task Force (FATF)

Die FATF ist ein 1989 durch die G7-Staaten gegründetes Gremium mit Sitz bei der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung in Paris und hat 39 Mitglieder. Die FATF ist vor allem auf politischer Ebene relevant und hat Empfehlungen und Standards für die effektive Bekämpfung von Geldwäsche und Terrorismusfinanzierung erarbeitet. Diese dienen häufig auch als Grundlage für nationale und europäische Gesetzgebungen.

Logo Financial Action Task Force (FATF)

Zusätzlich führt die FATF Länderprüfungen durch, um die Umsetzung ihrer Empfehlungen zu kontrollieren. Ergebnisse solcher Evaluierungen können durchaus hohen Druck erzeugen, da sich eine schlechte Länderbewertung äußerst negativ auf den Finanzsektor dieses Landes auswirken kann. Österreichs letzte Überprüfung fand 2015/2016 statt. Die damals festgestellten Defizite des österreichischen Systems zur Geldwäschebekämpfung wurden in den darauffolgenden Jahren schrittweise beseitigt. Der sogenannten

Enhanced Follow-up-Prozess, der der nachfolgenden Überprüfung dieser Anpassungen dient, ist inzwischen abgeschlossen. Der Start der nächsten Überprüfung Österreichs wird mit Ende 2024 erwartet.

Financial Intelligence Unit Plattform

Die Financial Intelligence Unit Plattform wurde von der Europäischen Kommission im Jahr 2006 als informelle Gruppe ins Leben gerufen und 2014 als offizielle Expertengruppe der Kommission etabliert. Sie besteht aus allen europäischen FIUs und berät sich in regelmäßigen Treffen über die Möglichkeiten noch engerer Kooperation und wie man den operativen Informationsaustausch über den europäischen Austauschkanal FIU.net weiterentwickeln kann.

Logo der Europäischen Kommission

Advisory Group

Die A-FIU ist auch Mitglied der Advisory Group. Die Gruppe, die aus neun bis elf Delegierten europäischer FIUs besteht, ist ein Beratungsgremium, das von der Financial Intelligence Unit Plattform eingerichtet wurde. Ihre Hauptaufgabe ist die Weiterentwicklung von FIU.net, dem Kommunikationssystem europäischer FIUs. Die Advisory Group soll mit ihrer Arbeit den europäischen Informationsaustausch im Bereich Geldwäscherei und Terrorismusfinanzierung noch effizienter machen. Dabei berät sie sich mit der Europäischen Kommission über technische Lösungsansätze in FIU.net und ist im ständigen Austausch mit der Financial Intelligence Unit Plattform, der sie über die Entwicklungen berichtet.

Logo des FIU.net

FIU.net

Bei FIU.net handelt es sich um ein dezentralisiertes System, das von den 27 FIUs der Union gemeinschaftlich verwendet wird. Über dieses System werden Informationen zu Geldwäsche und Terrorismusfinanzierung gesichert ausgetauscht, die einen Bezug zu einem anderen europäischen Mitgliedsstaat aufweisen. Das Grundprinzip von FIU.net ist, dass jede FIU ihre Informationen in ihrer eigenen lokalen Datenbank speichert und diese mit anderen europäischen FIUs mithilfe des lokalen FIU.net-Applikationsservers austauscht. Bis 2021 wurde FIU.net von Europol betreut und gewartet. Im Zuge einer Weiterentwicklung des Systems hat der europäische Datenschutzbeauftragte zum Jahresende 2019 ausgesprochen, dass die technische Betreuung von FIU.net durch Europol nicht mehr zulässig sei und dessen Transfer zu einer anderen EU-Institution gefordert. 2020 wurde daher der Transfer des Systems zur Europäischen Kommission vorbereitet und die zugrundeliegende Vereinbarung ausgearbeitet. Der Prozess wurde im September 2021 abgeschlossen und die Europäische Kommission hat die Betreuung des Systems übernommen.

Legislativpaket der Europäischen Kommission

Im Juli 2021 hat die europäische Kommission einen Vorschlag für ein neues Legislativpaket zur Bekämpfung von Geldwäscherei und Terrorismusbekämpfung vorgelegt, das aus vier verschiedenen Rechtsakten besteht:

- Verordnung zur Schaffung einer neuen EU-Behörde für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung
- Verordnung zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung
- Sechste Richtlinie zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (ersetzt die fünfte Geldwäsche-Richtlinie)
- Überarbeitung der Geldtransfer-Verordnung von 2015

Für die Koordinierung einer gesamtösterreichischen Stellungnahme zu den Legislativvorschlägen ist das Bundesministerium für Finanzen (BMF) zuständig. Das BMF arbeitet in enger Abstimmung mit den anderen Behörden, die im Kampf gegen Geldwäscherei und Terrorismusfinanzierung beteiligt sind, zusammen und vertritt die österreichischen Standpunkte bei den Verhandlungen auf europäischer Ebene.

Große Bereiche des Legislativpakets betreffen die Geldwäschemeldestelle im Bundeskriminalamt. Angefangen bei der Reichweite der Meldepflichten, über die Schaffung einer neuen supranationalen Geldwäschebehörde bis hin zur Neukonzeption der Befugnisse der europäischen FIUs, die A-FIU ist intensiv in die Verhandlungen eingebunden und bringt ihre Standpunkte ein. So soll eine nachhaltige und zielgerichtete Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung auch weiterhin gewährleistet bleiben.

5 Das Jahr 2022 in Zahlen

Entsteht bei den meldeverpflichteten Berufsgruppen der Grund zur Annahme, dass ein Geschäft in Zusammenhang mit Geldwäscherei oder der Terrorismusfinanzierung steht, müssen sie eine Verdachtsmeldung an die A-FIU erstatten. Ferner haben alle Verpflichteten mit der Geldwäschemeldestelle zusammenzuarbeiten und ihr auf Verlangen alle erforderlichen Auskünfte zu erteilen, die ihr zur Verhinderung oder zur Verfolgung von Geldwäscherei oder von Terrorismusfinanzierung erforderlich scheinen. Diese Melde- und Auskunftsverpflichtungen gegenüber der A-FIU bilden den Ausgangspunkt für ihre Aufgabenerfüllung. Aber auch Behörden sind zur Informationsweitergabe an die A-FIU verpflichtet, wenn ihnen Sachverhalte unterkommen, die in Zusammenhang mit Geldwäscherei oder Terrorismusfinanzierung stehen könnten.

Das folgende Kapitel liefert einen statistischen Überblick über die im Berichtsjahr eingelangten Verdachtsmeldungen und ihre Herkunft, über den Akteneingang im Allgemeinen und über den weiteren Umgang mit Sachverhalten, deren Analyse durch die A-FIU tiefergehende kriminalpolizeiliche Ermittlungen erforderten.

Art und Herkunft der Akteneingänge

Im Jahr 2022 verzeichnete die Geldwäschemeldestelle insgesamt 6.903 Akteneingänge. Mit einer Steigerung um rund 16 Prozent im Vergleich zum Vorjahr wird der Trend der letzten Jahre damit fortgesetzt. Nicht mitgezählt sind Meldungen, die die A-FIU wegen Nichterfüllung der Mindesterfordernisse zur Verbesserung zurückgewiesen hat.

Den größten Teil der Eingänge bildeten, wie in den vergangenen Jahren, die Gruppe der Verdachtsmeldungen (6.053), gefolgt von 716 Anfragen und Informationen an die A-FIU im Wege der internationalen Kanäle (Egmont Secure Web – ESW und FIU.net). Von Behörden und Gerichten erhielt die A-FIU im Berichtsjahr insgesamt 132 Meldungen. Die unter „andere Behörden“ erfassten 92 Eingänge stammten von inländischen Dienststellen, zum Beispiel von LKAs, der DSN oder vom Bundesamt für Korruptionsprävention und Korruptionsbekämpfung (BAK).

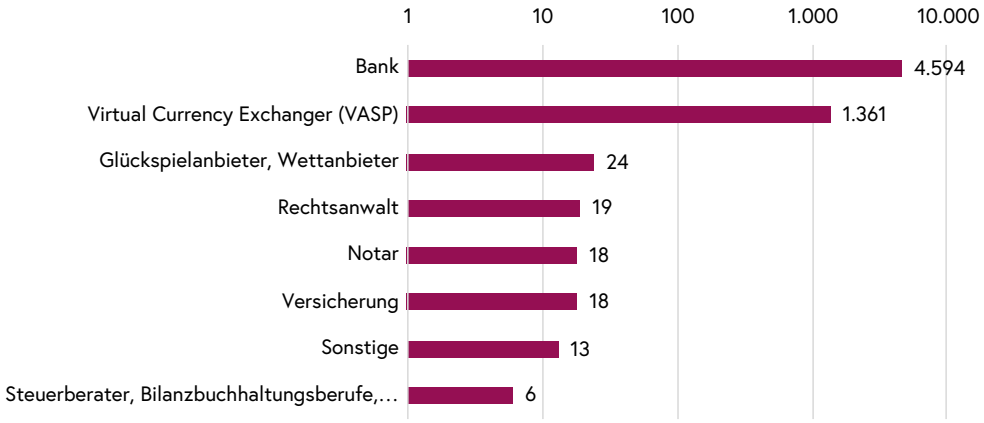
Herkunft der Akteneingänge im Jahr 2022

Herkunft der Akteneingänge	Anzahl	Anteil
Verdachtsmeldungen von meldeverpflichteten Berufsgruppen	6.053	88 %
Behörden und Gerichte	132	2 %
FMA	11	
Abgabenbehörden des Bundes	27	
Zollamt	10	
BMF und Finanzämter	17	
Gerichte	2	
andere Behörde	92	
Internationaler Eingang	716	10 %
Sonstige (zum Beispiel Privateingaben)	2	
Gesamt	6.903	100,00%

An der Spitze steht mit 4.594 Verdachtsmeldungen, wie auch in den Vorjahren, der Bankensektor, gefolgt von den Dienstleistern in Bezug auf virtuelle Währungen (VASP oder Krypotexchanger), die im Berichtsjahr 1.361 Verdachtsmeldungen erstattet haben. Das ist eine neuerliche Steigerung von mehr als 500 Prozent im Vergleich zum Vorjahr. Dieser enorme Anstieg bei Meldungen der VASPs ist darauf zurückzuführen, dass sich die Exchanger nach ihrer Gleichstellung mit dem Kredit- und Finanzsektor vor drei Jahren inzwischen an das Sorgfaltsniveau der Banken angenähert haben und ihre Kunden mit speziellen und treffsichereren Instrumenten monitoren. Bleibt das Meldeverhalten im kommenden Jahr konstant, werden die Kryptoexchanger 2023 erstmals mehr Verdachtsmeldungen erstatten, als die klassische Bankenwirtschaft.

Bei den Verdachtsmeldungen der übrigen meldepflichtigen Berufsgruppen sind, auch aufgrund der niedrigen Meldungszahlen, nur unwesentliche Veränderungen festzustellen.

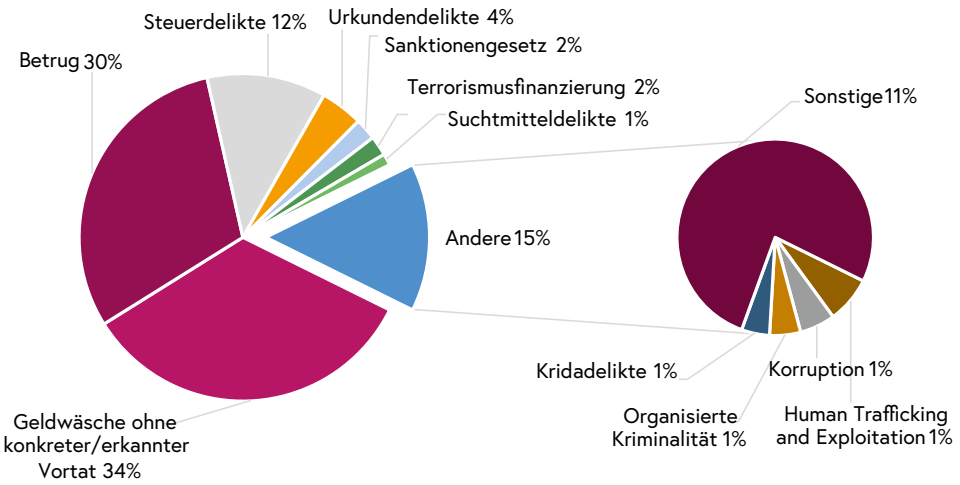
Verdachtsmeldungen gruppiert nach Sektoren im Jahr 2022



Deliktsbereiche der Verdachtsmeldungen

Die Analyse der Geldwäschemeldestelle erlaubt es, die meisten Verdachtsmeldungen bestimmten Deliktsbereichen zuzuordnen. In 34 Prozent der Fälle ließ sich trotz Analyse der A-FIU keine Vortat ausmachen, die der gemeldeten Geldwäscherei vorausgegangen sein könnte.

Dort, wo eine Zuordnung zu bestimmten Delikten möglich war, dominieren wie in den Vorjahren Betrugshandlungen (30 Prozent). Bei zwölf Prozent der Verdachtsmeldungen erkannte die A-FIU, dass die gemeldeten Sachverhalte in Zusammenhang mit Steuerdelikten stehen könnten. In vier Prozent der Fälle lag der Verdacht eines Urkundendelikts nahe und jeweils zwei Prozent der Verdachtsmeldungen berichteten über terrorismusbezogene Verdachtsmomente beziehungsweise über mögliche Sanktionsverstöße. Die übrigen Meldungen verteilen sich in etwa gleich auf Suchtmitteldelikte, Kridadelikte, organisierte Kriminalität, Korruption sowie Menschenhandel. Elf Prozent der Meldungen konnten anderen Straftaten zugeordnet werden.



Verdachtsmeldungen nach Deliktsbereichen im Jahr 2022

Sparbuchlegitimationen

Unabhängig von bestimmten Verdachtslagen müssen Kreditinstitute gemäß § 16 Absatz 3 Finanzmarkt-Geldwäschegesetz (FM-GwG) die A-FIU über die Auszahlung bestimmter Spareinlagen informieren und zwar, wenn es sich noch um anonyme Sparguthaben handelt, deren Guthaben 15.000 Euro oder mehr betragen. Die 112 im Berichtsjahr eingelangten Meldungen über Sparbuchlegitimierung dienen dazu, die letzten noch verbleibenden anonymen Spareinlagen ihren wirtschaftlichen Berechtigten zuzuordnen, um so die Geldwäscherei zu erschweren.

Korrespondenz mit anderen Behörden

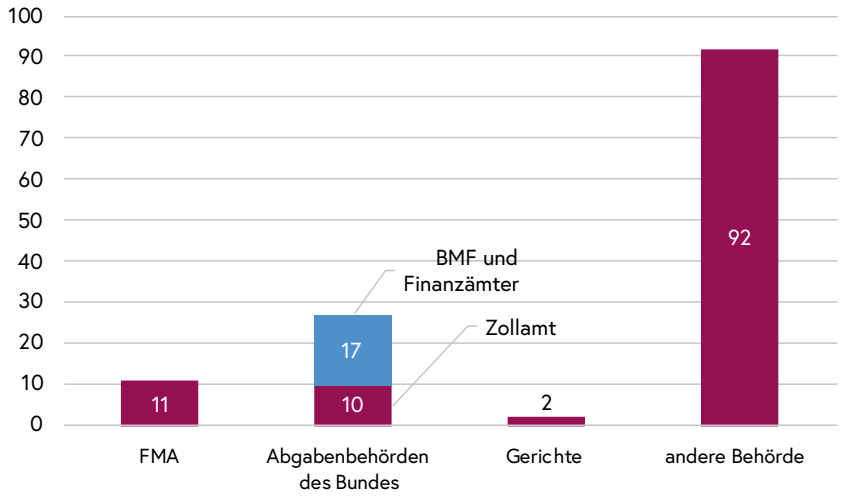
Neben der Privatwirtschaft müssen auch Behörden der Geldwäschemeldestelle Sachverhalte melden, wenn im Rahmen ihrer Aufgabenerfüllung der Verdacht strafbarer Handlungen im Zusammenhang mit Geldwäscherei oder Terrorismusfinanzierung entsteht.

Das Finanzamt Österreich und das BMF haben bei der Wahrnehmung ihrer Aufgaben im Berichtsjahr 2022 in 17 Fällen Hinweise auf Geldwäscherei beziehungsweise Terrorismusfinanzierung gefunden und diese – entsprechend ihrer Verpflichtung nach § 18 FM-GwG – der A-FIU berichtet. Ergänzend ist das Zollamt Österreich gemäß § 17b Zollrechts-Durchführungsgesetz im Zusammenhang mit der Durchführung von Bargeldkontrollen angehalten, Meldungen an die A-FIU zu erstatten. Diese Meldungen erfolgen, wenn die Vermutung besteht, dass Bargeld oder gleichgestellte Zahlungsmittel (zum Beispiel Gold- oder Silbermünzen) zum Zweck der Geldwäscherei oder Terrorismusfinanzierung verbracht werden. In diesem Zusammenhang erhielt die A-FIU zehn Meldungen.

Auch die Finanzmarktaufsicht (FMA) und die Oesterreichische Nationalbank (OeNB) sind gemäß § 18 FM-GwG verpflichtet die A-FIU zu verständigen, wenn ihnen bei der Ausübung ihrer Aufsichtstätigkeit mit Geldwäscherei oder Terrorismusfinanzierung in Zusammenhang stehende Transaktionen auffallen. Von diesen Behörden erhielt die Geldwäschemeldestelle im Berichtsjahr elf Meldungen.

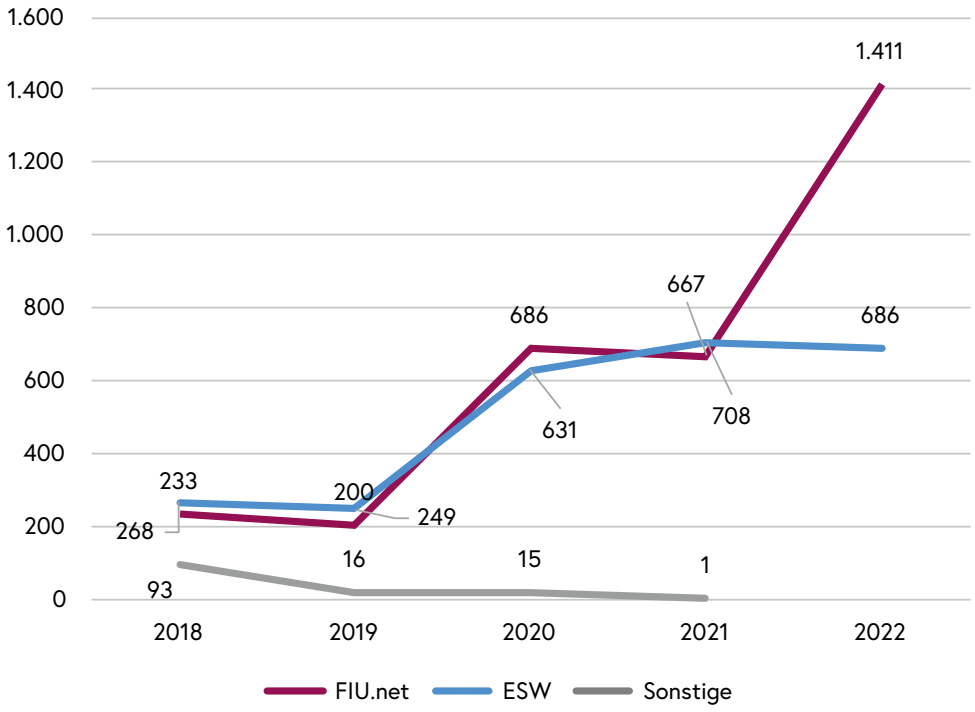
Die Geldwäschemeldestelle übermittelt ihre Analysen an die Strafverfolgungsbehörden grundsätzlich aus Eigenem. Manchmal benötigen diese aber auch weiterführende Hilfe. Die Behörden erhalten diese Hilfe bei der A-FIU in Form von weiteren Finanzinformationen oder -analysen. Im Berichtsjahr erhielt die Geldwäschemeldestelle 92 Ersuchen und Informationen von sonstigen Behörden, wie beispielsweise den LKAs oder anderer polizeilicher Dienststellen.

Mitteilungen über geldwäscherelevante Sachverhalte durch inländische Behörden und Stellen im Jahr 2022



Die Herkunft der Mitteilungen über geldwäscherelevante Sachverhalte durch inländische Behörden und Stellen sowie deren Ersuchen sind der folgenden Abbildung zu entnehmen.

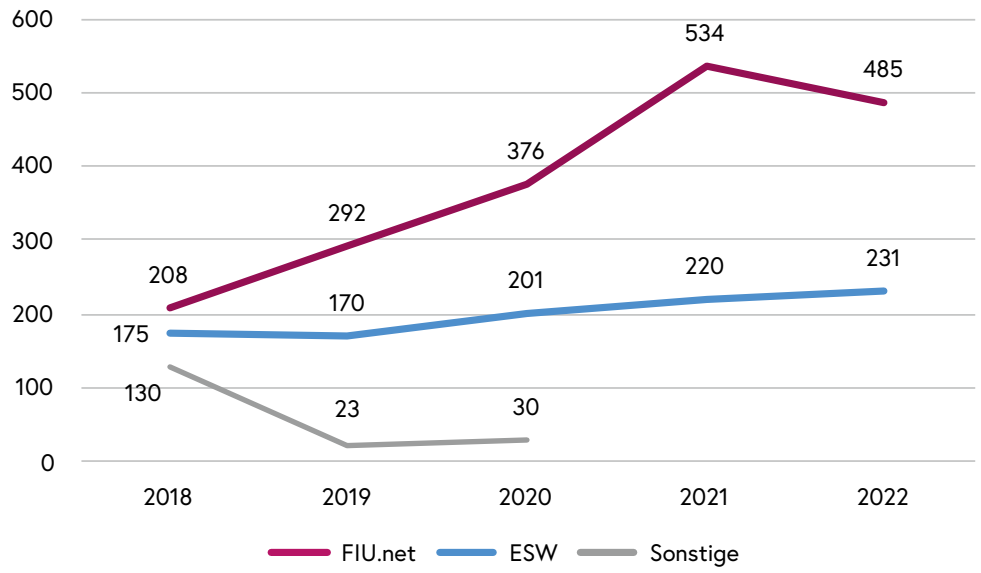
Die A-FIU leitete in 2.097 Fällen einen internationalen Schriftverkehr ein, um nähere Informationen zu den analysierten Sachverhalten einzuholen beziehungsweise die Partnerdienste über eigene Erkenntnisse zu informieren. Dabei wurde in diesem Berichtsjahr am häufigsten FIU.net (1.411 Fälle) verwendet, gefolgt von Egmont Secure Web (686 Fälle). Die Verdoppelung des Schriftverkehrs, der über FIU.net abgewickelt wird, ist auf eine bestimmte Berufsgruppe zurückzuführen: Einige österreichische Kryptoexchanger verfügen über einen großen ausländischen Kundenstamm. Verdachtsmeldungen zu solchen Kunden haben – außer dem Sitz des meldenden Unternehmens – keine weiteren Anknüpfungspunkte zu Österreich. Solche Meldungen übermittelt die A-FIU daher den betroffenen Partnerdiensten, allen voran der FIU Deutschland.



Anzahl des ausgehenden Schriftverkehrs nach Kanal von 2018 bis 2022

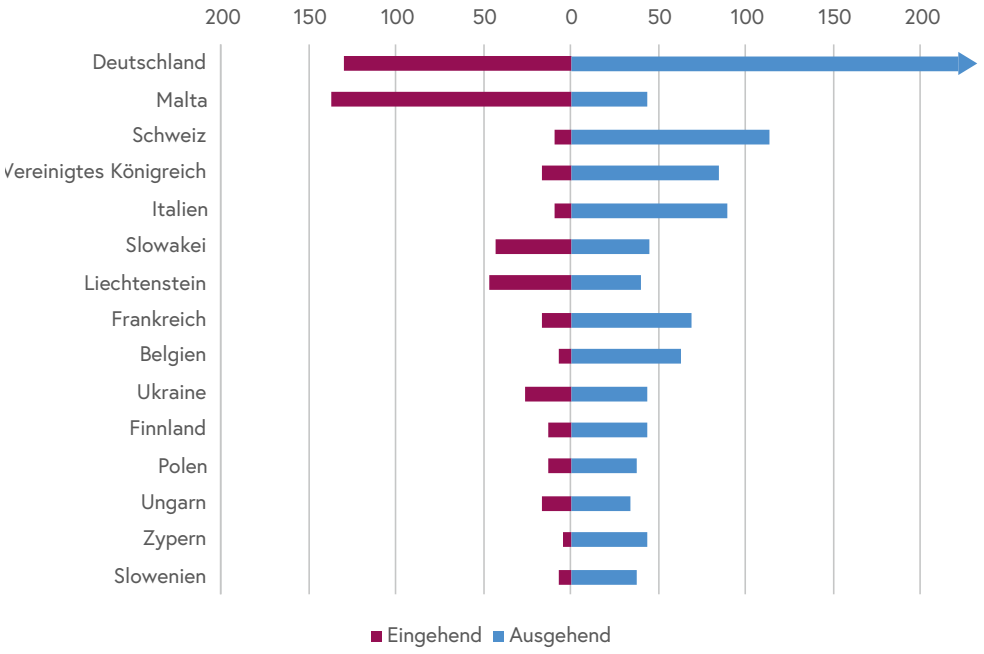
Im Berichtsjahr nahm die A-FIU 716 Informationsersuchen und Spontaninformationen ausländischer FIUs und Behörden entgegen. Dabei ist eine verstärkte Nutzung des Kommunikationskanals FIU.net feststellbar. 2022 wurde dieser in 485 Fällen genutzt. Die Kategorie „Sonstige“ enthielt andere Kommunikationskanäle, wie beispielsweise Verbindungsbeamte, Interpol oder Sirene, den Kommunikationskanal zum Schengener Informationssystem. Ein Schriftverkehr im Wege sonstiger Kommunikationskanäle fand im Berichtsjahr aufgrund der Reorganisation der A-FIU im Dezember 2018 nicht mehr statt.

Anzahl des eingehenden Schriftverkehrs nach Kanal von 2018 bis 2022



Die Staaten, mit denen am häufigsten Informationen ausgetauscht wurden, sind in der folgenden Abbildung ersichtlich.

Internationaler Schriftverkehr nach Ländern im Jahr 2022

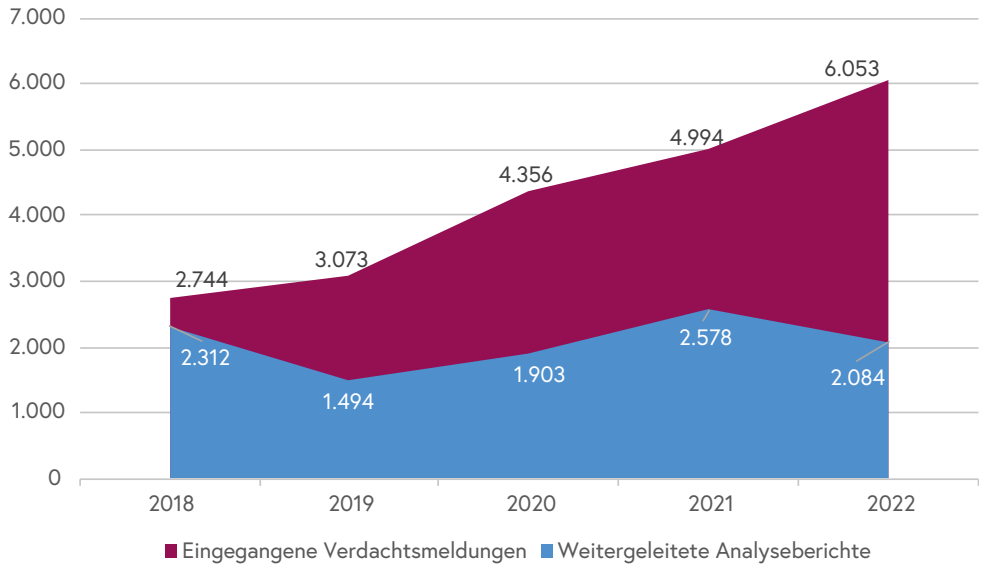


Weiterleitung von Analyseberichten

Wenn die A-FIU aufgrund ihres Analyseverfahrens zur Überzeugung gelangt, dass eine Straftat begangen worden ist oder zumindest ein dahingehender Verdacht besteht,

leitet sie ihre Erkenntnisse in Form eines Analyseberichts an die für Strafverfolgung zuständigen Stellen weiter.

Von den insgesamt 6.053 im Berichtsjahr erhaltenen Verdachtsmeldungen gingen nach Durchführung des Analyseverfahrens 2.084 in Form von Analyseberichten an die Strafverfolgungsbehörden zur weiterführenden Ermittlung weiter. Das entspricht einem Anteil von 34 Prozent der eingelangten Verdachtsmeldungen. Demgegenüber steht die Differenz von 3.969 Fällen, die die A-FIU mangels Anfangsverdachts oder weiterer Analyseansätze ad acta legte.



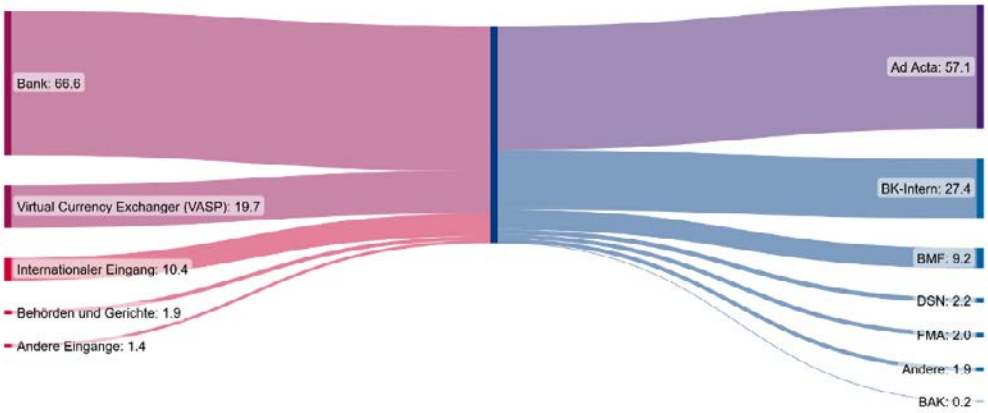
Eingegangene Verdachtsmeldungen und weitergeleitete Analyseberichte von 2018 bis 2022

Insbesondere die komplexen Fälle von vermuteter Geldwäscherei erfordern weiterführende Sachverhaltsklärungen im Rahmen eines Ermittlungsverfahrens. Besteht der Verdacht der Geldwäscherei oder ihrer Vortaten, ist aber kein Zusammenhang mit besonderen Tatbeständen, wie Steuer- oder Zollvergehen, Terrorismus- oder Korruptionstatbeständen erkennbar, leitet die A-FIU ihr Analyseergebnis an die zuständigen Stellen im Bundeskriminalamt weiter. Wie auch in den Vorjahren, wurden die meisten Analyseberichte (27,4 Prozent) an die Fachabteilungen und Büros im Bundeskriminalamt gesandt. Rund neun Prozent der Analyseberichte gingen wegen vermuteter Steuer- oder Zollvergehen an die Abgabenbehörden des Bundes und rund zwei Prozent an die Direktion Staatsschutz und Nachrichtendienst weiter.

Nur in dringenden Fällen oder in Fällen, in denen bereits ein einschlägiges Strafverfahren anhängig war, erfolgte eine direkte Abtretung an die zuständigen ermittelnden LKAs. 2022 war das bei rund zwei Prozent der Analyseberichte der Fall.

Fälle vermuteter Verletzungen der Vorschriften des Finanzmarkts gehen an die Finanzmarktaufsicht und Sachverhalte im Zusammenhang mit Korruptionsdelikten an das Bundesamt für Korruptionsprävention und –bekämpfung.

Ursprünge des Akteneingangs und Ziele der Analyseberichte



Auskunftsersuchen

Alle Verpflichteten haben mit der Geldwäschemeldestelle zusammenzuarbeiten und ihr auf Verlangen – ungeachtet einer zuvor erstatteten Verdachtsmeldung – alle erforderlichen Auskünfte zu erteilen, die ihr zur Verhinderung oder zur Verfolgung von Geldwäscherei oder von Terrorismusfinanzierung erforderlich scheinen. Von ihrem Recht derartige Auskünfte von den meldeverpflichteten Berufsgruppen zu verlangen, machte die A-FIU im Berichtsjahr 242-mal Gebrauch. Die A-FIU forderte unter anderem Unterlagen über die Plausibilität der Mittelherkunft, über Kontobewegungen oder Legitimationspapiere an.

Mitteilungen und Warnmeldungen

Symbol für Warnmeldungen der Geldwäschemeldestelle

Die Fallanalysen der Geldwäschemeldestelle bilden die Basis für eine fallübergreifende Darstellung von Mustern und Trends sowie für die Identifikation und die Darstellung aktueller Phänomene im Bereich der Geldwäscherei. Entsprechend ihrem gesetzlichen Auftrag teilt die A-FIU ihr so gewonnenes Wissen mit den Meldeverpflichteten.

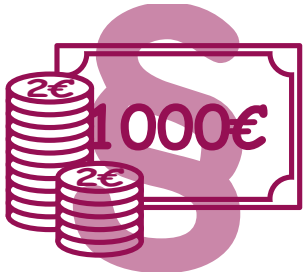
Die regelmäßig veröffentlichten allgemeinen Mitteilungen und Warnmeldungen der A-FIU erlauben es den meldeverpflichteten Berufsgruppen ihr Transaktionsmonitoring zu schärfen, indem sie die darin enthaltenen Indikatoren in ihre Analysen miteinfließen lassen. Dadurch werden meldepflichtige Sachverhalte rascher und verlässlicher identifiziert.

Die allgemeinen Mitteilungen der Geldwäschemeldestelle beinhalten fallübergreifende neu entdeckte Methoden und Phänomene der Geldwäscherei sowie aktuelle Informationen aus diesem Bereich.

Mit Warnmeldungen hingegen macht die A-FIU auf ganz konkrete Anhaltspunkte aufmerksam, anhand derer sich verdächtige Transaktionen erkennen lassen. Seit März 2021 kann die A-FIU im Wege von Warnmeldungen auch Informationen übermitteln, die dem Bankgeheimnis unterliegen, solange dies zur Verhinderung von Geldwäscherei oder Terrorismusfinanzierung erforderlich ist. Diese Warnmeldungen informieren beispielsweise über bestimmte im Umlauf befindliche falsche Urkunden oder über verdächtige internationale Bankkontonummern.

Die A-FIU hat im Berichtsjahr 13 Mitteilungen und Warnmeldungen über den gesicherten Kommunikationskanal goAML mit den meldepflichtigen Berufsgruppen geteilt. Einige Beispiele für diese Warnmeldungen sind im Kapitel über Typologien genauer beschrieben.

Sicherstellungen



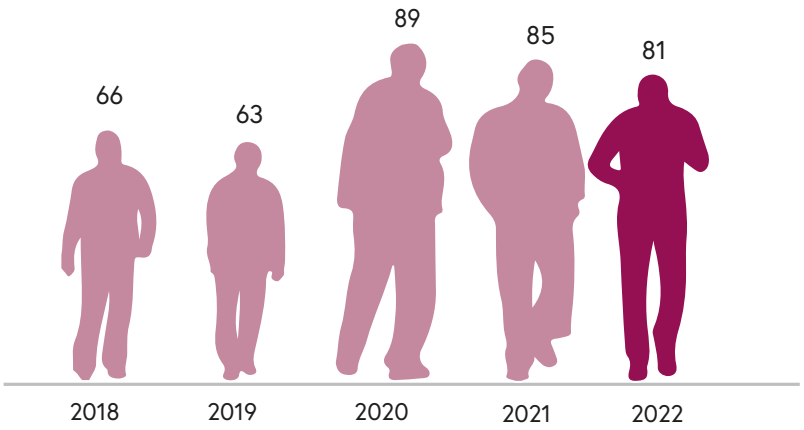
2022 hat die Geldwäschemeldestelle in 69 Fällen eine vermögensrechtliche Anordnung zur Sicherstellung von verdächtigen Vermögenswerten angeregt. Der Gesamtwert dieser Vermögenswerte belief sich auf 2,2 Millionen Euro. Die im Berichtsjahr stark ausgebaute Zusammenarbeit zwischen A-FIU, Kriminalpolizei und Staatsanwaltschaften in Sicherstellungsangelegenheiten führte dazu, dass in fast allen Fällen eine rasche Entscheidung durch die Justizbehörden erwirkt werden konnte.

Verurteilungsstatistik

Der an die zuständigen Stellen übermittelte Analysebericht der A-FIU, der Informationen über die zugrundeliegende Verdachtsmeldung, über kriminalpolizeiliche Daten, Finanzdaten und Ergebnisse des internationalen Informationsaustauschs beinhaltet, löst das kriminalpolizeiliche Ermittlungsverfahren oft erst aus. Dieses beschränkt sich nicht bloß auf Geldwäscherei oder Terrorismusfinanzierung. So sind die Analyseberichte häufig ausschlaggebend für Verurteilungen anderer strafbarer Handlungen, wie etwa den Vortaten.

2022 gab es 81 rechtskräftige Verurteilungen wegen Geldwäscherei zu verzeichnen, das entspricht einem Rückgang von fünf Prozent im Vergleich zum Vorjahr.

Bei den bekanntgewordenen und für die Verurteilung der Geldwäscherei notwendigen Vortaten waren Verstöße gegen das Suchtmittelgesetz, Betrügereien, Diebstähle, Veruntreuung, Urkunden- und Kridadelikte führend.



Verurteilungen von 2018 bis 2022 im Vergleich

7 Aktuelle Methoden der Geldwäscherei

Das Jahr 2022 hat die Geldwäschemeldestelle vor zahlreiche neue Herausforderungen gestellt. Zwar verschwanden die für die Vorjahre so prägenden Betrugsphänomene im Zusammenhang mit der Covid-19-Pandemie, doch drängte sich ab Februar 2022 ein ganz anderes Aufgabenfeld ins Zentrum.

Der russische Angriffskrieg auf die Ukraine und die ihm nachfolgenden Sanktionspakete der Europäischen Union führten zu einem empfindlichen Anstieg der dazu gemeldeten Sachverhalte. Im Rahmen der Umsetzung der Sanktionsmaßnahmen unterstützte das Bundeskriminalamt die zuständigen Behörden nicht nur mit kriminalpolizeilicher Expertise und mit Daten, sondern auch bei deren Koordinierung, die die A-FIU übernahm.

Die im Berichtsjahr festgestellten häufigsten Methoden der Geldwäscherei, zu denen die A-FIU auch zahlreiche Warnmeldungen mit den meldepflichtigen Berufsgruppen teilte, sind im Folgenden beschrieben.

Finanzagenten & Money Mules

Money Mules beziehungsweise Finanzagenten sind ein bekanntes Phänomen, das die A-FIU seit Jahren beschäftigt. Aufgrund der niederschwelligen Möglichkeit, über diesen Weg Geld zu waschen und der Leichtgläubigkeit vieler, die bedenkenlos anderen ihr Konto zur Verfügung stellen, erreichten die A-FIU auch 2022 wieder zahlreiche Verdachtsmeldungen, die von Finanzagenten berichteten.

Finanzagenten sind Personen, die von Kriminellen angeworben werden, um ihr Konto zur Verfügung zu stellen, damit über dieses Geld transferiert werden kann, über dessen illegale Herkunft die Kontoinhabenden nichts wissen (wollen). Das Geld, das auf ihren Konten einlangt, stammt durchwegs aus Online-Betrugshandlungen und fließt meist aus dem Ausland zu. Gemäß den Anweisungen des professionellen Geldwäscherings sollen die Money Mules die Gelder dann ans Ausland weiterleiten. Die wegen des Verdachts der Geldwäscherei einvernommenen Money Mules geben meist an, nichts von der kriminellen Vorgeschichte der bei ihnen eingelangten Gelder gewusst zu haben.

In vielen Fällen handeln Money Mules in Unwissenheit über die illegale Herkunft der Gelder. Aus rechtlicher Sicht fehlt daher häufig der nötige Vorsatz, um sie nach § 165 StGB – Geldwäscherei zu belangen. Ist die Wissentlichkeit nicht nachweisbar, drohen jedenfalls Verwaltungsstrafen bis zu 60.000 Euro wegen gewerblicher Zahlungsdienstleistung ohne Konzession oder wegen Nichtoffenlegung von Treuhandbeziehungen.

Kryptowährungen

Trotz der beachtlichen Kursschwankungen sind Kryptowährungen weiterhin ein bewährtes Mittel der Geldwäsche und Terrorismusfinanzierung. Gerade nach erfolgten Online-Betrugshandlungen sind Kryptowährungen häufig das Mittel der Wahl, um die Gelder schnell vom Opfer wegzutransferieren und dem Zugriff der Behörden zu entziehen.

Mixing und Chain-hopping

Wie auch bei den klassischen Mitteln der Geldwäsche, zielen Kriminelle bei der Geldwäsche mit Kryptowährungen darauf ab, die Herkunft des inkriminierten Vermögens zu verschleiern. Die Analysen der Geldflüsse in der Blockchain werden dabei immer herausfordernder, weil die Kriminellen günstige Mixing-Dienste verwenden und immer häufiger auch sogenanntes „Chain-hopping“ betreiben.

Mixing-Dienste sind Plattformen, die potentiell identifizierbare Kryptowerte unterschiedlichster Kundinnen und Kunden miteinander vermischen und sodann zeitlich und wertmäßig gestaffelt, ganz nach den Anforderungen der Kundschaft, wieder auszahlen. Trotz der Transparenz der Blockchain ist somit nicht nachvollziehbar, wer die tatsächlich wirtschaftlich Berechtigten an den Kryptowerten sind.

Mit der Weiterentwicklung der Decentralised-Finance-Technologien stellte die A-FIU im Berichtsjahr vermehrt Chain-hopping fest, also den raschen Wechsel von Kryptowerten in andere Kryptowährungen. Dazu bedient man sich sogenannter „Smart Contracts“, die als Programmcodes auf den Blockchains automatisiert Transaktionen nach festgelegten Bedingungen abwickeln. Sie sind dabei nicht an eine einzige Kryptowährung gebunden und erlauben daher den raschen und automatisierten Tausch von Kryptowerten in unterschiedliche Währungen.

Der Einsatz dieser technisch sehr aufwendigen aber – auf den ersten Blick – günstigen Methoden dient immer demselben Zweck: Am Ende des Geldwäscheprozesses soll das „Cash-out“, also die Auszahlung in Fiatgeld wie Euro, möglichst keine Aufmerksamkeit bei den Dienstleistenden am Finanzmarkt wecken.

Die Strafverfolgung wird besonders dadurch erschwert, dass das Cash-Out bei Exchangern mit Sitz in schwach regulierten Märkten mit geringen Anforderungen an die kundenbezogenen Sorgfaltspflichten erfolgt. Die Tatsache, dass in solchen Destinationen wichtige Zahlungsinformationen nur in unzureichendem Maße erhoben werden, erscheint angesichts der mangelnden Kooperationswilligkeit oder –fähigkeit dieser Länder nur nebensächlich.

Geldwäsche durch Krypto-Ladebons

Der Lagebericht 2021 berichtete von einer Betrugswelle mithilfe von Krypto-Ladebons. Die Opfer der Betrugsmasche wurden von den Kriminellen kontaktiert und dazu verleitet, bei einem vermeintlichen europäischen Lotteriespiel mitzumachen. Zum Teil wurden sie auch davon überzeugt einen monatlichen Beitrag zu leisten, um regelmäßig an einer Auslosung teilnehmen zu können. Einige Zeit später nahmen die Täter erneut Kontakt auf und behaupteten, die Opfer hätten einen Geldpreis gewonnen. Um jedoch den Gewinn ausbezahlt zu bekommen, müssten sie eine Gebühr für Transport- und Notarkosten entrichten.

Die Gebühr sollte mittels Gutscheinen für Kryptowährungen beglichen werden. Daraufhin kauften die Opfer diese Gutscheine und gaben den Code zum Einlösen des Betrags an die Kriminellen weiter. Meist übermittelten die Betrogenen auch gleich ihre Ausweisdokumente und persönlichen Informationen, mit denen die Täter wiederum Konten auf den Handelsplattformen eröffneten. Das Geld wurde dann über ein weit verzweigtes Netzwerk an Wallets weitergeleitet, um seine kriminelle Herkunft zu verschleiern. Der bisher bekannte Schaden liegt bei rund 600.000 Euro. Zudem weist alleine eines der im Waschvorgang involvierten Krypto-Wallets einen Umsatz von rund 20 Millionen Euro auf.

Nach einigen Treffen mit österreichischen Krypto-Exchangern, bei denen die A-FIU auf die erhebliche Gefahr hinwies, dass diese Gutscheine sowohl für Betrügereien als auch für die anschließende Geldwäsche missbraucht werden, stellten namhafte Exchanger dieses Geschäftsmodell ein.

Geldwäsche im Zusammenhang mit dem Ukrainekonflikt

Im Zuge des russischen Angriffskriegs auf die Ukraine erhöhte die Geldwäschemeldestelle ihre Aufmerksamkeit betreffend den Bargeldverkehr von der Ukraine in die Europäische Union. Die Einfuhr von Barmitteln, Gold, Inhaberpapieren und dergleichen in Höhe von 10.000 Euro oder mehr in die Union ist meldepflichtig. Der so erhobene offizielle Bargeldverkehr in die und aus der Europäischen Union sowie alle Fälle behördlicher Aufgriffe von nicht korrekt gemeldeten Bargeldtransporten werden in einer europaweiten Zolldatenbank verarbeitet. In die ZIS-Cash-Datenbank (Zollinformationssystem) haben auch die europäischen FIUs Einsicht.

Seit März 2022 sind vermehrt Einfuhren von großen Bargeldmengen aus der Ukraine in die Union festzustellen. Wenngleich diese Importe auch mit der berechtigten Angst zu erklären sind, dass die russische Besatzungsmacht lokale Vermögenswerte in der Ukraine einziehen könnte, so eignet sich die politische Situation durchaus auch zur Geldwäsche. Aufgrund der Kriegswirren lässt sich überzeugend behaupten, dass die Nachweise über die legale Herkunft der eingeführten Vermögenswerte verschollen sind. Es ist daher

davon auszugehen, dass große Mengen an inkriminierten Geldern in die Europäische Union eingeführt wurden. Das beschriebene Anmeldeverfahren liefert darüber hinaus eine Bescheinigung der Zollbehörden, die oftmals auch als Herkunftsnachweis missverstanden wird.

8 Vortaten zur Geldwäscherei

Geldwäsche ist ein sogenanntes Anschlussdelikt. Das bedeutet, dass die zu waschenden Vermögensbestandteile aus bestimmten, schweren Straftaten stammen müssen. Nicht jeder Vermögensbestandteil ist also geldwäschetauglich. Nur, wenn der betreffende Vermögensbestandteil aus gerichtlich strafbaren Handlungen stammt, die mit mehr als einjähriger Freiheitsstrafe bedroht sind oder aus den §§ 223, 229, 289, 293, 295 StGB oder §§ 27 oder 30 Suchtmittelgesetz stammen, ist Geldwäscherei überhaupt möglich.

Erstmals beleuchtet der Jahresbericht auch das Feld ebendieser Vortaten und beschreibt jene Delikte und Tathandlungen, die die A-FIU im Berichtsjahr am häufigsten identifiziert hat oder die sie inhaltlich besonders gefordert haben.

Der risikobasierte Ansatz, ein Prinzip, das die Grundlage der internationalen Geldwäschebekämpfung bildet, verpflichtet Behörden und Privatwirtschaft dazu, ihre – freilich begrenzten – Ressourcen in jene Bereiche zu stecken, die ein besonders hohes Risiko der Geldwäsche aufweisen. Die im folgenden beschriebenen Deliktsbereiche und Fallbeispiele zeigen die Risikolandschaft, in der sich Österreich befindet. Sie können dem Bundeskriminalamt und der A-FIU im Besonderen als Wegweiser dienen, auf welche Deliktsformen ein besonderes Augenmerk gelegt werden sollte.

Mögliche Sanktionsumgehung durch Weißrussland

Im Februar 2022 stellte die A-FIU erhöhte Finanzströme von Weißrussland in den Euro-Raum und wieder retour nach Weißrussland fest. Die Analysen ergaben, dass Personen offenbar einen günstigen Wechselkurs nutzten, um weißrussische Rubel zunächst in Euro und wieder zurück zu wechseln. Dabei erfolgten zahlreiche Barbehebungen mit weißrussischen Bankomatkarten bei österreichischen Bankomaten in Euro, woraufhin das Bargeld auf Eurokonten eingezahlt und nach Weißrussland transferiert wurde. Dort behoben es die Beteiligten wiederum in weißrussischen Rubel.

Die Bereitschaft weißrussischer Banken für einlangende Euro derart günstige Wechselkurse anzubieten, dass sogar die Wechselgebühren im Euro-Raum damit kompensiert wurden, war wohl auf die geltenden EU-Sanktionen gegen Weißrussland zurückzuführen. Neben einem Barverkehrsverbot mit weißrussischen Unternehmen besteht auf europarechtlicher Ebene auch ein generelles Transaktionsverbot mit der weißrussischen Zentralbank oder von ihr kontrollierte Unternehmen. Diese Maßnahmen dürften zu einem erhöhten Bedarf an Devisen in Weißrussland geführt haben, woraus sich die ungewöhnlich günstigen Wechselkurse erklärten.

Die Vermutung war zunächst, dass die Beteiligten versucht hatten, das durch die EU-Sanktionen eingeführte Transaktionsverbot mit der weißrussischen Zentralbank zu umgehen, um ihren Bedarf an Devisen zu befriedigen. Letztlich ließ sich der Verdacht

einer vorsätzlichen Sanktionsumgehung durch die Beteiligten nicht bestätigen. Allerdings führte eine Warnmeldung der A-FIU zur möglichen Sanktionsumgehung zum sofortigen Verschwinden dieses Geschäftsmodells.

Abgabenhinterziehung und Scheinunternehmen

Die im Vorbericht erläuterte Problematik der Scheinunternehmen hat sich 2022 weiter verschärft. Der Trend zur Gründung von Scheinunternehmen hat sich vor allem im Baugewerbe weiter fortgesetzt. Sie werden eingesetzt, um Sozialabgaben im großen Stil vorzuenthalten und Steuern zu hinterziehen.

Vorrangiges Ziel der mehrstufigen Scheinunternehmen-Konstrukte ist es, gewinn- und damit steuermindernd Vermögen aus Unternehmen auszuschleusen, um damit im Anschluss Schwarzarbeitende bar bezahlen zu können – erneut ohne Einkommensteuern oder Sozialabgaben abzuliefern.

Zu diesem Zweck werden zahlreiche Gesellschaften mit beschränkter Haftung gegründet oder als Firmenmäntel übernommen. Als Geschäftsführende fungieren ausschließlich Strohleute, die mit dem tatsächlichen operativen Geschäft der Gesellschaft nichts zu tun haben, wodurch die tatsächlich wirtschaftlich Berechtigten im Dunkeln bleiben. Diese Scheinunternehmen werden in einer Kette hintereinandergeschaltet und stellen dem jeweiligen Vorunternehmen „Rechnungen“ für Leistungen, die sie tatsächlich niemals erbracht haben. So verfügt das Vorunternehmen über den notwendigen Beleg, um den gewinnmindernden Zahlungsausgang in die Buchhaltung aufnehmen zu können. Je weiter unten sich ein Scheinunternehmen in der Kette befindet, desto kurzlebiger ist es und desto weniger Verantwortungsträger lassen sich noch finden. Am Ende der Kette kommt es dann zur Barbehebung der überwiesenen Gelder, die dann mittels Kick-Back an die obersten Unternehmen übergeben werden, die damit die Schwarzlöhne bezahlen.

Ein gemeinsamer Schwerpunkt des Amts für Betrugsbekämpfung und der A-FIU ist die Aufdeckung und Bekämpfung von Scheinunternehmen mithilfe der meldeverpflichteten Berufsgruppen, insbesondere der Banken. Mit der Veröffentlichung des Szenarios zur Geldwäsche durch Scheinunternehmen im Jahr 2021 und durch die daraufhin erstatteten zahlreichen Verdachtsmeldungen der Banken wurden die enormen Dimensionen der vorenthaltenen Sozialleistungen und hinterzogenen Abgaben sichtbar: Alleine in den vergangenen zwei Jahren behoben Scheinunternehmen über 600 Millionen Euro in bar von ihren Bankkonten. Geld, das meist für die Bezahlung von Schwarzarbeitenden verwendet wird, und für das die Beteiligten weder Sozialabgaben noch Steuern leisten.

Die Verdachtsmeldungen lassen auf eine hohe Dunkelziffer schließen. Es ist daher von einem tatsächlichen Volumen an Barbehebungen von rund einer Milliarde Euro auszu

gehen, die eine Hinterziehung von Lohnabgaben, Sozialversicherungsabgaben, Ertragsteuren und teils Umsatzsteuer in gleicher Höhe nach sich ziehen.

Gestützt auf ein Gutachten des Österreichischen Juristentags zum Sozialbetrug, das anhand von echten Fällen den Problemstand und den geltenden Rechtsrahmen erörtert, bemühten sich das Amt für Betrugsbekämpfung und die A-FIU, die Aufmerksamkeit aller beteiligten Akteure für die Problematik zu erhöhen. 2022 erfolgte ein intensiver Austausch zwischen Kriminalpolizei und Staatsanwaltschaften, um die Finanzströme der Scheinunternehmen zu kappen, bevor diese sich im Bargeldverkehr verlieren. Denn das Bargeld ist der Motor der organisierten Schwarzarbeit.

Die Vorgangsweise der Scheinunternehmen bleibt für die Strafverfolgung eine rechtliche Herausforderung: Einerseits muss die Vermögenssicherung äußerst rasch vonstattengehen, um zu verhindern, dass sich die Spur des Geldes im Barverkehr verliert. Bei aller Kenntnis der Behörden über die theoretische Vorgangsweise der Kriminellen, bedürfen behördliche Sicherstellungsmaßnahmen aber entsprechender Begründungen, die mit konkreten Tatsachen belegt sind. Diese lassen sich aber oft erst im Laufe langwieriger Ermittlungen erheben.

Betrug

Die Zahl der Verdachtsmeldungen, die über erfolgte Betrugshandlungen berichten, steigen kontinuierlich. Der überwiegende Teil dieser Meldungen betrifft Bankkundinnen und -kunden, die über das Internet betrogen worden sind. Dass das zu waschende Geld immer häufiger aus Onlinebetrug stammt, liegt an den immer einfacheren und rascheren Möglichkeiten zur Kontaktaufnahme mit potentiellen Opfern: Internettelefonie, Messengerdienste und Echtzeitüberweisungen haben unser Wirtschaftsleben derart beschleunigt und anonymisiert, dass sich Betrügereien sehr profitabel und mit viel geringerem Entdeckungsrisiko über das Internet durchführen lassen.

Betrugshandlungen in der Offline-Welt finden immer noch statt. Klassische Tank- oder Geldwechselbetrügereien finden nach wie vor Ihren Weg zur Strafverfolgung, aber meist über Anzeigen bei den Polizeiinspektionen und nicht über Verdachtsmeldungen an die A-FIU.

Angesichts des immer größeren Ausmaßes, das Betrugsdelikte bei den Vortaten zur Geldwäscherei erreichen, hat das Büro für Betrugsermittlungen im Bundeskriminalamt im vergangenen Jahr ein Lagebild zum Betrug aufgebaut. Dieses gibt tagesaktuell Auskunft über die österreichweite Betrugslage, über regionale Häufungen von Betrugsanzeigen und hat sich wiederholt als Frühwarnsystem, das neueste Betrugsmaschen sehr früh

zeitig aufdeckt, bewährt. Es bildet die Grundlage für Geldrückholungen bei großen Betrugssachverhalten und hilft bei der Steuerung bundesweiter Schwerpunktaktionen.

2022 veranlasste das Büro für Betrugsermittlungen aufgrund der Erkenntnisse aus dem Lagebild Internetbetrug 51 Geldrückholungen. Die Fälle betrafen einen Gesamtschaden von 3,4 Millionen Euro. Rund die Hälfte der veranlassten Geldrückholungen war erfolgreich, sodass rund 1,5 Euro gesichert und den Opfern wieder zur Verfügung gestellt werden konnten.

Anrufbetrug

Nach wie vor stellt der klassische Anrufbetrug eine große Herausforderung für die österreichische Polizei dar. Die Täter kontaktieren ihre Opfer telefonisch und bringen sie mit unterschiedlichsten Tricks dazu, in finanzielle Vorleistung zu gehen. Die Modi Operandi variieren je nach Tätergruppe.

Falsche Polizisten

Diese Art des Anrufbetrugs verursachte im Jahr 2022 mehr als 15 Millionen Euro Schaden. Weil diese Form des Betrugs nicht saisonabhängig ist, stellt das Phänomen eine ganzjährige Problematik dar. Zielgruppe sind betagte Menschen, die jedenfalls im pensionsfähigen Alter sind und häufig altmodisch klingende Namen tragen.

Die Täter rufen ihre Opfer an und geben sich als Polizeibedienstete aus. Häufig behaupten sie, dass Angehörige des Opfers in einen Verkehrsunfall verwickelt seien und sich nun in Haft befänden. Nur durch die Bezahlung einer Kaution im fünfstelligen Bereich könne eine Freilassung erwirkt werden.

In einer anderen Variante behaupten die falschen Polizisten, dass sich im Umfeld des Opfers Einbrüche oder Raubüberfälle ereignet hätten und die Polizei nun als Schutzmaßnahme Wertgegenstände und Geld vorübergehend übernehmen müsse. In einer weiteren Abwandlung dieses Modus schlüpfen die Täter in die Rolle von Bankangestellten. Mit der Begründung korrupte Bankmitarbeiter würden die Schließfächer der Kundschaft heimlich ausräumen, sähen sie Misstrauen gegenüber der Bank des Opfers.

Das Büro für Betrugsermittlung hat zur Vorbeugung dieser Betrugsformen ein Präventionsmodell entwickelt und dieses im Rahmen von „Gemeinsam.Sicher“ in Kooperation mit der Wirtschaftskammer Österreich, den österreichischen Banken sowie den Präsidenten des Seniorenrates im Mai 2022 vorgestellt.

Falsche englischsprachige Polizeibedienstete

Im Dezember 2021 trat der Anrufbetrug erstmals in einer englischsprachigen Version auf. Die Täter gaben sich als Bedienstete internationaler Polizeibehörden aus, meist von Interpol oder Europol oder als Mitarbeitende eines nicht näher genannten „Federal

Police Departements“. Die Kommunikation erfolgte ausschließlich auf Englisch. Um die Betrugsmasche zu beschleunigen, bedienten sich die Täter sogenannter Call-Bots. Diese automatisierten englischsprachigen Tonbandaufnahmen forderten die angerufenen Opfer auf, Taste 1 zu drücken und die Kommunikation mit den vermeintlichen Interpol- oder Europol-Bediensteten aufzunehmen. Dadurch erreichten die Täter zweierlei: Zum einen war sichergestellt, dass die kontaktierten Opfer auch verlässlich Englisch sprechen. Zum anderen filterten die Täter mit den Call-Bots all jene Menschen aus, die nicht auf die Taste 1 gedrückt hatten und eben nicht auf die Betrugsmasche reinfallen würden. Mittels IP-Telefonie und sogenanntem Rufnummern-Spoofing fälschten die Täter obendrein die auf dem Display der Opfer erscheinende Anrufnummer.

War die Sprechverbindung einmal aufgebaut, behaupteten die Täter, dass die Opfer in verschiedenste Straftaten verwickelt seien oder ihre DNA an vermeintlichen Tatorten aufgefunden worden sei. So sollten die Opfer verunsichert und zur Geldüberweisungen verleitet werden. In den meisten Fällen überwiesen die Opfer ihr Vermögen auf Konten von Finanzagenten, in anderen Fällen zahlten sie Bargeld bei Bitcoin-Automaten auf unbekannte Wallets ein.

In Zusammenarbeit mit einem international tätigen Hinweisgeber und Aktivisten konnte das Bundeskriminalamt ein betrügerisches Callcenter in Indien lokalisieren, das für dieses bundesweit auftretende Phänomen verantwortlich schien. Über Interpol strengte das Bundeskriminalamt eine Fallkooperation mit Indien und Deutschland an, im Zuge derer die Existenz des Callcenters nachgewiesen wurde. Die indischen Polizeibehörden führten eine Hausdurchsuchung durch, nahmen mehrere Täter in Haft und stellten Beweismaterial und Opfergelder sicher, was direkte Auswirkung auf Österreich hatte: Seit September 2022 ist das Phänomen des falschen englischsprachigen Polizisten in Österreich nicht mehr feststellbar.

Die falschen Bankbediensteten

Bei dieser Weiterentwicklung der bekannten Betrugsmasche mittels Phishing-SMS erhalten die Opfer zur Vorbereitung des Betrugs zumeist eine SMS im Namen einer vermeintlichen Bank. Die SMS informiert die Opfer darüber, dass angeblich widerrechtliche Abbuchungen von ihrem Konto erfolgt seien oder dass die Opfer die Legitimation für das Online-Banking verlängern müssten. Die Opfer werden dazu verleitet auf einen Link zu klicken.

Im Glauben auf die seriöse Website ihrer Bank weitergeleitet worden zu sein, geben die Opfer ihre Zugangsdaten bekannt. Im Anschluss ruft die Täterschaft mit gefälschten Telefonnummern an und angebliche Bankbedienstete melden sich und bauen Vertrauen auf. Die Opfer werden aufgefordert Überweisungen zu bestätigen beziehungsweise freizugeben. Da es sich vorranging um Echtzeitüberweisungen handelt, besteht nur

eine geringe Wahrscheinlichkeit die Geldbestände durch die Banken oder die Behörden wiederzuerlangen.

Bestellbetrug

Der „Bestellbetrug" bildet den Überbegriff verschiedener Varianten von Betrügereien im Onlinehandel. Man unterscheidet zwischen zwei unterschiedlichen Begehungsformen: Versandbetrug und Warenbetrug. Beim Versandbetrug bestellen die Täter Waren im Internet schon mit dem Vorsatz, diese nach Erhalt nicht zu bezahlen. Von Warenbetrug spricht man, wenn Täter Waren mit dem Ziel anbieten, Opfer zu einer Bezahlung zu bringen, ohne jedoch die versprochene Ware jemals liefern zu wollen oder zu können.

Bestellung auf fremden Namen

Diese Begehungsform definiert sich dadurch, dass die Täter tatsächlich existierende Identitäten benutzten und in deren Namen Waren bestellen. Zumeist werden mit den Daten der Geschädigten Einkaufs-Accounts im jeweiligen Onlineshop erstellt, Bestellungen aufgegeben und anschließend an eine abweichende Zustelladresse bestellt. Die Rechnungen und später die Mahnungen trudeln in den Briefkästen der unwissenden Opfer ein.

Angebote bei Kleinanzeigenplattformen

Immer beliebter werden Betrügereien durch Kleinanzeigen im Internet. Die Täter geben sich als Privatpersonen aus und bieten auf Kleinanzeigenplattformen Waren zum scheinbaren Verkauf an. Die Geschädigten überweisen den vereinbarten Kaufpreis ohne jemals eine Ware zu erhalten.

Bei einer weiteren Form des Bestellbetrugs auf den privaten Verkaufsplattformen nehmen die Täter aktiv mit den Opfern Kontakt auf. Sie geben sich als kaufwillige Interessenten aus und überreden die geschädigten Verkäuferinnen und Verkäufer, angebliche Transportkosten im Voraus zu übernehmen. Letztendlich werden die Opfer oft doppelt geschädigt. Einerseits durch den Verlust der versendeten Ware und andererseits durch die getätigten Vorauszahlungen.

Fakeshops

Die Opfer werden zufällig auf Werbung im Internet aufmerksam oder suchen gezielt nach einem bestimmten Produkt. Dadurch locken die Täter die Geschädigten auf Onlineshops von täuschend echt wirkenden Firmen. Sie bestellen dort das gewünschte Produkt und überweisen den Kaufbetrag im Vorhinein, allerdings warten die Geschädigten vergebens auf ihre Ware oder erhalten nur Pakete mit wertlosem Inhalt.

Phishing-Betrug

Unter dem Begriff „Phishing" versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner auszugeben.

Ziel der Kontaktaufnahme ist zunächst, an persönliche Daten eines zukünftigen Opfers zu gelangen. In der Regel handelt es sich hierbei um Online-Banking-Zugangsdaten. Im Anschluss daran missbrauchen die Täter selbst die erlangten persönlichen Daten für weitere Straftaten oder nehmen Kontakt mit den Opfern auf, um diese um ihr Geld zu bringen.

Tochter-Sohn-Modus

Nach wie vor sehr erfolgreich ist der sogenannte Tochter-Sohn-Betrug. Die Täter verschicken massenweise SMS oder WhatsApp-Nachrichten an zufällig gewählte Mobilnummern. Darin geben sie sich als angebliche Tochter oder Sohn der Empfängerinnen und Empfänger aus und erklären eine neue Telefonnummer zu haben. Kurz darauf geben die Täter – wieder per Textnachricht – vor, dringend Geld zu benötigen, meist wegen angeblicher Spontangebrechen oder wegen Notfällen. Zumeist geben sie als Zahlungsempfänger ausländische Konten an. Im Glauben der Tochter oder dem Sohn etwas Gutes zu tun, überweisend die Geschädigten und das zumeist mit Echtzeittransfer.

Phishing-Betrug auf Kleinanzeigenplattformen

Opfer eines Phishing-Betrugs werden auch Menschen, die private Gegenstände auf Kleinanzeigenplattformen verkaufen wollen. Die Täter stellen den Kontakt zu den Geschädigten her und bekunden ihr scheinbares Kaufinteresse. Um das Vertrauen der Opfer zu erlangen, werden Fragen über die Waren gestellt und Smalltalk betrieben. Die Täter wirken seriös und ernsthaft interessiert. Schließlich schlagen sie vor, die Zahlung und die Übergabe der Ware über einen Kurierdienst abzuwickeln.

Die Opfer erhalten dann einen Phishing-Link, der sie auf eine gefälschte Webseite weiterleitet. Diese vermittelt den Opfern den Eindruck, die verkaufte Ware sei bereits bezahlt. Die Opfer werden weiter aufgefordert ihre Kreditkartendaten einzugeben, damit der Betrag scheinbar überwiesen werden kann. Mit dem Bestätigen der Freigabe erhalten die Opfer jedoch kein Geld – im Gegenteil: In Wirklichkeit geben die Opfer eine Zahlung frei und überweisen damit Geld an die Täter.

Vorauszahlungsbetrug

Beim Vorauszahlungsbetrug werden Geschädigte dazu aufgefordert, finanzielle Vorleistungen zu tätigen, um später einen vermeintlichen Gewinn, ein Erbe, einen Kredit oder auch Wohnobjekte als Gegenleistung zu erhalten. Der bekannteste Vorauszahlungsbetrug ist wohl der Love- oder Romance-Scam.

Love- oder Romance-Scam

Die Love-Scam-Anbahnung erfolgt über Dating-Plattformen und in den sozialen Medien. Durch regelmäßigen Kontakt schaffen es die Täter, dass die Opfer eine emotionale Bindung zu ihnen aufbauen. Die Täter geben sich gerne als Ingenieurinnen und Ingenieure, Ärztinnen und Ärzte, Konstrukteure aus der Ölindustrie oder als US-Soldaten aus.

Beispielsweise werden den Opfern Geschichten präsentiert, wonach sich der Soldat im Auslandsaufenthalt befinde und derzeit nicht an sein privates Vermögen gelange. Die Täter bitten die verliebten Opfer um finanzielle Unterstützung, meist via Zahlungsdienstanbieter oder mittels Überweisung. Wiederholt versprechen die Täter bald nach Österreich zu kommen und das Geld zurückzuzahlen. Die Lügengeschichten werden leicht abgewandelt, wiederholen sich aber solange, wie die Opfer zahlungswillig sind. Diesem Delikt fallen durchschnittlich mehr Frauen als Männer zum Opfer.

Vorauszahlungsbetrug Kredite

Bei dieser Art des Vorauszahlungsbetrugs werden auf verschiedenen Internetplattformen Privatkredite angeboten. Die Täter geben jedoch vor, wegen Gebühren, Versicherungen oder Ähnlichem gewisse finanzielle Vorleistungen zu benötigen. Meist überweisen die Geschädigten dreistellige Beträge an das angegebene Bankkonto. Eine Kreditauszahlung sehen die Opfer jedoch nie.

Vorauszahlungsbetrug Miete

Wohnungssuchende laufen Gefahr, Opfer eines Mietbetrugs zu werden, wenn sie im Internet nach Miet- oder Airbnb-Wohnungen suchen. Dabei stoßen sie auf äußerst interessante Angebote, die vorwiegend in sozialen Medien und einschlägigen Vermieterplattformen geschaltet wurden. Nach Kontaktaufnahme – zumeist durch die Geschädigten selbst – wird eine Kaution in Vorauszahlung gefordert. Das Opfer erhält jedoch nie Zugang zum gewünschten Objekt.

Investmentbetrug

Opfer eines Investmentbetrugs, auch „Cyber Trading Fraud“ oder CTF genannt, werden meist Menschen, die selbst aktiv nach Investmentmöglichkeiten im Internet gesucht haben. Seltener erfolgt der Erstkontakt durch die Täter selbst.

Folgende Formen der Erstanbahnung werden unterschieden:

- Hochprofessionelle und echt wirkende Internetauftritte von Investitionsplattformen, auf die die Opfer nach eigener Suche stoßen
- Werbung auf Internetseiten und in Printmedien
- Ungefragte Anrufe von „Investmentspezialisten“
- Empfehlungen durch Dating-App-Kontakte
- Empfehlungen von Freunden, die noch nicht erkannt haben, dass sie selbst Opfer eines Betrugs wurden
- Folgeanruf nach bereits erfolgter Investition

Die Opfer erhalten meist Telefonanrufe, nachdem sie ihre Kontaktdaten bekanntgegeben haben. Die Täter eröffnen anschließend ein vermeintliches Tradingkonto für die Opfer, oftmals unter der Bedingung, dass ein verhältnismäßig niedriger Betrag als Erstinvestment

eingezahlt werden muss. Das Portfolio entwickelt sich zunächst prächtig und die Opfer erzielen scheinbar gute Gewinne. Teilweise werden diese sogar an die Opfer ausbezahlt, um ein Vertrauensverhältnis aufzubauen und zu Folgeinvestments zu animieren. Gelingt dies, zeigt das Tradingkonto erneut gute Gewinne an, doch das „investierte" Geld ist zu diesem Zeitpunkt schon lange weg. Solange die Opfer einzahlen, setzen die Täter die Geldforderungen fort. Verlangen die Geschädigten die Auszahlung der Gewinne, rasselt der vermeintliche Wert des Investmentportfolios meist in den Keller und der Kontakt mit den Tätern bricht ab.

Die Täter verwenden immer öfter eine Fernwartungs-Software, bevorzugt Anydesk, um selbst auf die Computer der Opfer zugreifen können.

CEO-Fraud und Business E-Mail Compromise

Beim CEO-Fraud handelt es sich um eine Form des Betrugs, bei der gefälschte E-Mails an Firmen verschickt werden. Diese stammen scheinbar von Mitgliedern der Geschäftsführung des Unternehmens. Im E-Mail fordern die vermeintlichen Geschäftsführenden von der Buchhaltung die dringliche Überweisung hoher Geldbeträge an angebliche Partnerfirmen mit ausländischen Bankverbindungen und ersuchen die Beteiligten um absolute Verschwiegenheit. Nach der ersten schriftlichen Kontaktaufnahme, rufen die Täter die ausführenden Mitarbeitenden in der Buchhaltung an und setzen sie unter Druck, die Zahlung möglichst rasch vorzunehmen.
Unter Business E-Mail Compromise (BEC) versteht man das Kompromittieren eines Unternehmens durch betrügerische Phishing E-Mails. Dabei treten zwei Firmen in Kontakt zueinander, mit der Absicht ein Geschäft abzuwickeln. Die Täter schalten sich unbemerkt in die E-Mail-Kommunikation ein und manipulieren den Schriftverkehr. Meist verändern sie die Kontodaten des Empfängers, sodass es zur Übermittlung einer falschen IBAN kommt und die Rechnungsbegleichung an die Täter geht.

9 Einhaltung der Sorgfalts-pflichten

Nicht nur Banken oder Handelsplattformen für Kryptowährungen werden für Geldwäscherei genutzt, auch Gewerbetreibende können Gefahr laufen von Kriminellen missbraucht zu werden. Insbesondere, wenn Kaufleute hohe Bartransaktionen akzeptieren oder wenn es um Immobilienvermittelnde, Auktionshäuser oder Kunsthandelnde geht, unterliegen sie strengen Sorgfaltspflichten in Bezug auf Geldwäscherei und Terrorismusfinanzierung.

Wirtschaftstreuhand- und Bilanzbuchhaltungsberufe

Große Verantwortung im Kampf gegen Geldwäscherei tragen auch Berufsberechtigte nach dem Wirtschaftstreuhandberufs- und dem Bilanzbuchhaltungsgesetz. Sie beraten unter anderem Kapitalgesellschaften in steuerlichen Angelegenheiten und haben dadurch einen guten Einblick in die Vorgeschichte und die Vermögensverhältnisse ihrer Klienten. Besonders im Hinblick auf die Problematik der Scheinunternehmen, meist GmbHs im Baugewerbe, die ausschließlich dazu gegründet werden, um gewinn- und steuermindernd Bargeld zur Bezahlung von Schwarzarbeitenden auszuleiten, kann diese Berufsgruppe einen wertvollen Beitrag leisten. Durch den tiefen Einblick in die Vorgeschichte und die Vermögensverhältnisse der GmbHs können Wirtschaftstreuhand- und Bilanzbuchhaltungsberufe als Frühwarnsystem bei der Erkennung von Scheinunternehmen fungieren. Aus diesem Grund hat die A-FIU im Berichtsjahr den Informationsaustausch mit den Aufsichtsbehörden der betroffenen Berufsgruppen intensiviert und sie mit Warnmeldungen zum Phänomenbereich der Scheinunternehmer versorgt. Vom Schulungsauftrag und der Aufsicht durch die Berufsvertretungen erhofft sich die Geldwäschemeldestelle einen Anstieg der Verdachtsmeldungen in diesem Bereich.

Know-your-Customer bei Kontoeröffnungen

Die A-FIU stellte im letzten Jahr hunderte Fälle von Onlinekonto-Eröffnungen fest, denen falsche Angaben und Daten der Kundschaft zugrunde lagen. Die mithilfe dieser Konten ausgeführten Straftaten (insbesondere Betrugshandlungen und Geldwäscherei) führten und führen zu erheblichen Schäden und das auch bei kontoeröffnenden Instituten. Die Geldwäschemeldestelle empfahl in diesem Zusammenhang einfache Maßnahmen beim Onboarding-Prozess, die einen großen Beitrag zur Verbrechensbekämpfung leisten und Schäden vorbeugen können.

Insbesondere, wenn es sich um Kontoeröffnungen mit falschen Wohnadressen der Kundinnen und Kunden handelt, kann die sorgfältige Überprüfung des angegebenen Wohnorts, zum Beispiel durch Prüfung des Meldezettels oder von Rechnungen und Gehaltszetteln, betrügerischen Kontoeröffnungen effektiv vorbeugen.

10 Strategische Entwicklungen

Um Geldwäscherei und Terrorismusfinanzierung nachhaltig zu bekämpfen, bedarf es eines strategischen Ansatzes, der – aufbauend auf den operativen Einzelfallanalysen der Verdachtsmeldungen – ein umfassendes Bild der aktuellen Entwicklungen zeichnet. Dieser Aufgabe widmet sich das Referat Strategische Finanzstromanalyse der A-FIU.

Financial Intelligence Network Austria (FINA)

Die Zusammenarbeit mit dem privaten Sektor ist für die A-FIU ein wichtiges Element bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Bei der größten Public-Private-Partnership im österreichischen System der Geldwäschebekämpfung ergaben sich in den vergangenen zwei Jahren wichtige Entwicklungen. Die im Herbst 2019 unter dem Namen „Arbeitsgruppe Finanzkriminalität" vom Bundesministerium für Finanzen ins Leben gerufene PPP wurde 2021 erweitert. Die A-FIU übernimmt seitdem abwechselnd mit dem BMF die Leitung dieser Arbeitsgruppe.

2022 kam es zu einer Neukonzeption der Arbeitsgemeinschaft. Unter dem Namen Financial Intelligence Network Austria (FINA) wurde der Teilnehmerkreis klarer definiert und die Themensetzung offener gestaltet. Die A-FIU und das BMF leiten die Sitzung weiterhin gemeinsam, doch die Schwerpunktsetzungen sollen alle Teilnehmenden aktiv mitgestalten. Die ersten Treffen im Herbst 2022 beschäftigten sich zum Beispiel mit den Möglichkeiten, wie der Datenaustausch im privaten Sektor selbst verbessert werden könnte. Neben dem Austausch von aktuellen Trends und Mustern sieht sich FINA als eine Diskussionsplattform zur vertrauensvollen Besprechung von Problemen und Herausforderungen der täglichen Arbeit und in der gemeinsam an Lösungen gefeilt wird.

PPP Glücksspiel und Sportwetten

Die Gesetzgebung im Bereich des kleinen Glücksspiels und des Wettwesens ist Ländersache. Daher besteht praktischer Bedarf an einer möglichst einheitlichen Interpretation der Sorgfalts- und Meldepflichten, denen Unternehmen in diesem Sektor unterliegen, sowie an einer Harmonisierung der aufsichtsbehördlichen Kontrollmaßnahmen. Denn Unternehmen in diesem Sektor sind meist länderübergreifend tätig und daher mit einer Vielzahl unterschiedlicher landesgesetzlicher Regelungen konfrontiert.

Gemeinsam mit der AML-Compliance e.U. hat die Geldwäschemeldestelle 2022 eine spartenspezifische Public Private Partnership für die Sektoren der Sportwetten und des Glücksspiels ins Leben gerufen. Neben den neun Landesregierungen waren Interessensvertretungen des Glücksspiel- und Sportwettensektors beteiligt. Im Oktober 2022 erging das gemeinsame Rundschreiben, das als Orientierung für Verpflichtete und Behörden bei der praktischen Anwendung der gesetzlichen Vorschriften dient.

Geldwäschetagung

Am 30. und 31. Mai 2022 fand in Salzburg zum siebenten Mal die Geldwäschetagung statt. Diese widmete sich besonders dem größten Legislativvorschlag, den die Europäische Kommission in der Geldwäschebekämpfung je erarbeitet hat: Das EU-Single-Rule-Book plant weitreichende Änderungen der Geldwäscheregeln über alle Branchen hinweg und bringt neue Möglichkeiten, aber auch Herausforderungen für FIUs.

Die Tagung bot dabei eine gute Gelegenheit die Auswirkungen des Paktes auf Österreich zu diskutieren. Es gab Vorträge und Workshops von und mit Vertreterinnen und Vertretern der Wirtschaftskammer Österreich, den betroffenen Bundesministerien, der Finanzmarktaufsicht, der Österreichischen Nationalbank, der Notariatskammer, des österreichischen Rechtsanwaltskammertags und der Kammer der Steuerberater und Wirtschaftsprüfer.

Schulungen und Vorträge

Neben ihrem repressiven Auftrag Geldwäscherei und Terrorismusfinanzierung aktiv zu bekämpfen, hat die A-FIU auch die präventive Aufgabe, den beteiligten Akteuren aktuelle Informationen über Methoden der Geldwäscherei und der Terrorismusfinanzierung und über Anhaltspunkte zu verschaffen, anhand derer sich verdächtige Transaktionen erkennen lassen. Zu diesem Zweck hielt die Geldwäschemeldestelle im Berichtsjahr 23 Schulungen ab und trug bei unterschiedlichsten Fachveranstaltungen vor, um unter anderem das Bewusstsein für die Meldeverpflichtungen zu schärfen.

Daneben war die A-FIU bei 15 Schulungen für Landeskriminalämter (für angehende dienstführende Polizeibedienstete) und Staatsanwaltschaften aktiv, um auch in diesen Bereichen mehr Verständnis für das Thema Geldwäscherei und Terrorismusfinanzierung zu schaffen.

Auch die technischen Aspekte bei der Geldwäschebekämpfung wurden thematisiert. Bei insgesamt zehn Schulungen bei Verpflichteten und Ministerien bildete die A-FIU die Teilnehmenden über das Meldesystems goAML weiter und warb für die Verwendung des strukturierten Datenformats XML bei der Einbringung von Verdachtsmeldungen.

Die Erfahrungen der A-FIU waren auch international gefragt: So präsentierte die A-FIU Fallstudien bei Expertentreffen der UNODC und im Rahmen eines CEPOL-Trainings für europäische Polizeibedienstete zu Hawala. Auch bei zahlreichen UNODC-Workshops konnte die A-FIU ihren internationalen Partnern aktuelle Muster und Trends präsentieren.

Task Force Sanktionen

Nach dem russischen Angriffskrieg auf die Ukraine und den darauffolgende EU-Sanktionen richtete Österreich eine interministerielle Task Force zum Thema der Sanktionsdurchsetzung ein. Unter der Leitung der Direktion Staatsschutz und Nachrichtendienst war die A-FIU auf Seiten des Innenministeriums eine weitere zentrale Vertretung. Wichtige Themen der Task Force waren der Informationsaustausch mit der EU, aber auch die Steuerung und Koordination der Maßnahmen innerhalb der beteiligten Ressorts in Österreich.

Nationales Koordinierungsgremium

Das nationale Koordinierungsgremium ist ein gesetzlich eingerichtetes Forum, dass sich der Entwicklung von Maßnahmen und Strategien zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung widmet. Es findet unter dem Vorsitz des Bundesministeriums für Finanzen statt. Neben der A-FIU nehmen Delegierte des Justizministeriums, der Direktion Staatsschutz und Nachrichtendienst, des Wirtschaftsministeriums, des Außenministeriums, der Finanzmarktaufsicht und der Österreichischen Nationalbank an den Sitzungen teil.

11 Ausblick

Auch das Jahr 2023 wird für die A-FIU große Herausforderungen bereithalten:

Einen besonderen Fokus wird die Geldwäschemeldestelle auf die Verhandlungen über den Entwurf eines neuen Geldwäschepakets der Europäischen Kommission (COM(2021) 420 final) legen. Dieser als „Single Rule Book" bezeichnete Legislativentwurf harmonisiert das europäische Geldwäscherecht und besteht aus vier verschiedenen Verordnungen und Richtlinien, die ins österreichische Recht umgesetzt werden müssen. Der Entwurf betrifft unter anderem auch die Kernaufgaben der europäischen FIUs, weshalb sich die A-FIU aktiv in die Verhandlungen einbringen wird, um ihre Standpunkte und Rechtsansichten durchzusetzen. Der Entwurf wird voraussichtlich 2024 beschlossen, sodass die A-FIU noch im selben Jahr mit den Vorbereitungen zur Umsetzung beginnen wird.

Voraussichtlich beginnt im Jahr 2024 die Überprüfung des österreichischen Systems der Bekämpfung von Geldwäsche und Terrorismusfinanzierung durch die Financial Action Task Force, einem internationalen Gremium mit Sitz bei der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung in Paris. Die Überprüfung, die sich allen praktischen und rechtlichen Aspekten der Geldwäschebekämpfung widmet, ist äußerst ressourcenintensiv und erfordert umfassende Vorbereitungen. Unter der Leitung des Bundesministeriums für Finanzen und in Kooperation mit der Direktion Staatsschutz und Nachrichtendienst wird sich die A-FIU im kommenden Jahr intensiv auf den Prüfprozess vorbereiten.

Das Rückgrat des Informationsaustauschs zwischen Geldwäschemeldestelle der A-FIU und der Privatwirtschaft ist nach wie vor goAML. Die Finanzierung erfolgte in der Vergangenheit zu großen Teilen aus Mitteln der Europäischen Union, und zwar dem Fonds für die innere Sicherheit (ISF). Das entsprechende Projekt ist im Berichtsjahr zu Ende gegangen. Die A-FIU plant ab 2023 wieder ein ISF-Projekt zu starten, um goAML zukunftsfit zu halten und mit den zahlreichen weiteren Datenbanken der Sicherheitsbehörden interoperabel zu machen.