Bundesministerium
Inneres

Bundeskriminalamt

Lagebericht Geldwäsche 2023

Aktuelle Entwicklungen der Geldwäsche und der Vermögenskriminalität

Lagebericht Geldwäsche 2023

Aktuelle Entwicklungen der Geldwäsche und der Vermögenskriminalität

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres, Bundeskriminalamt
Josef-Holaubek-Platz 1, 1090 Wien
+43 1 24836 985025 (SPOC)
bundeskriminalamt.at
Layout: BMI-I/C/10/a - Strategische Kommunikation und Kreation
Druck: Digitalprintcenter des Bundesministeriums für Inneres
Wien, 2024

Vorwort

Liebe Interessierte!

Generaldirektor für die öffentliche Sicherheit Franz Ruf

Das Jahr 2023 hat die Geldwäschemeldestelle im Bundeskriminalamt (A-FIU) vor neue Herausforderungen gestellt und gezeigt, dass auch altbekannte Betrugsformen und Geldwäschephänomene noch nicht verschwunden sind.

Die Entwicklungen des Jahres 2023 bestätigen erneut, wie groß das Risiko ist, dass der Finanzplatz für die Wäsche und die Ausleitung von Betrugsgeldern missbraucht wird. Internet-Telefonie, 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 einen besonderen Fokus auf die Prävention und Verfolgung der Betrugskriminalität setzen.

Um diesen Herausforderungen zu begegnen, intensivierte die A-FIU einerseits die Zusammenarbeit mit ihren Partnerbehörden, die die Einhaltung der Sorgfaltspflichten überprüfen. Andererseits suchte die Geldwäschemeldestelle – noch mehr als in den Vorjahren – den Kontakt zu ihren Informationsgeberinnen und -gebern in den meldeverpflichteten Berufsgruppen. Mit der grundlegenden Neukonzeption der strategischen Analyse und mit der neuen Kommunikationsstrategie der A-FIU ging eine deutliche Intensivierung des öffentlich-privaten Informationsaustauschs einher. Das Vertrauen und Verständnis für die Belange des jeweiligen Gegenübers konnte in zahlreichen Treffen im Rahmen des Financial Intelligence Networks Austria und bei anderen Treffen weiter ausgebaut werden.

Direktor des Bundeskriminalamts Andreas Holzer

Das Jahr 2023 stand ferner im Zeichen der Vorbereitung der fünften Überprüfungsrunde des österreichischen Systems zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung durch die Financial Action Task Force (FATF). Viele der 40 Empfehlungen, die die FATF ihren Mitgliedstaaten im Kampf gegen Geldwäsche und Terrorismusfinanzierung macht, betreffen das Bundesministerium für Inneres. Die anstehende Überprüfung ist in Umfang und Strenge beispiellos und ihr Ausgang ist für den Wirtschaftsstandort von großer Bedeutung. Das Bundeskriminalamt, die Direktion Staatsschutz und Nachrichtendienst, das Bundesamt für Korruptionsprävention und Korruptionsbekämpfung arbeiteten Hand in Hand, um ein möglichst gutes Prüfungsergebnis für Österreich sicherzustellen.

Wir möchten uns bei allen Mitarbeitenden der A-FIU und des Büros für Betrugskriminalität für ihren Einsatz bedanken. Sie haben in einer Welt der sich ständig wandelnden Vermögenskriminalität und der dauernden technischen Weiterentwicklung unermüdlich gegen Geldwäscherei und ihre Vortaten gekämpft. Ebenso möchten wir uns bei den behördlichen und privaten Kooperationspartnern bedanken, die uns auch 2023 wieder dabei unterstützten, Trends und Typologien zu erkennen.

Ihr

Franz Ruf

Generaldirektor für die öffentliche Sicherheit

Andreas Holzer

Direktor des Bundeskriminalamts

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 2023.

Die Analysen der Geldwäschemeldestelle zeigen, dass Onlinebetrug, Sozialmissbrauch und Abgabenhinterziehung in Form von Scheinunternehmen besonders häufig als Vortaten zur Geldwäscherei auftreten. Der sogenannte 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. Diesem Prinzip folgend, widmet sich der heurige Bericht diesen Delikten im Kapitel Vortaten zur Geldwäscherei.

Das Phänomen Geldwäsche

Ausgangspunkt jeder Geldwäsche 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. Sie sollen es 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, beim Glücksspiel, in Wechselstuben oder

bei anderen Unternehmen 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.

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 Geldwäsche 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 Geldwäsche 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 Geldwäsche oder von Terrorismusfinanzierung erforderlich scheinen.

Die Melde- und Auskunftsverpflichtungen gegenüber der A-FIU bilden den 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

§ 165 StGB stellt die Geldwäscherei unter Strafe. Die vorgesehenen Kombinationen der verschiedenen Tathandlungen und ihrer jeweils zugehörigen Vorsatzstufen sind äußerst komplex, 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 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. Ein weiteres Beispiel ist ein Finanzagent, der Gelder, die aus Betrugshandlungen stammen und auf seinem Konto eingelangt sind, 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 Geldwäsche-meldestelle

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.

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 im Kampf gegen 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 der Vogelperspektive. Ihm obliegt die fallübergreifende (und nicht auf den Einzelfall beschränkte) Darstellung von Mustern und Trends, das Erkennen von Typologien zur Verhütung und Bekämpfung von Geldwäsche oder Terrorismusfinanzierung sowie die Darstellung aktueller Phänomene. Diese Erkenntnisse leitet die A-FIU den Meldeverpflichteten weiter. Sie dienen der Bewusstseinsbildung bei den meldepflichtigen Berufsgruppen sowie der frühzeitigen Erkennung von strafrechtlich relevanten Sachverhalten.

Dem Referat Operative Finanzstromanalyse obliegen 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.

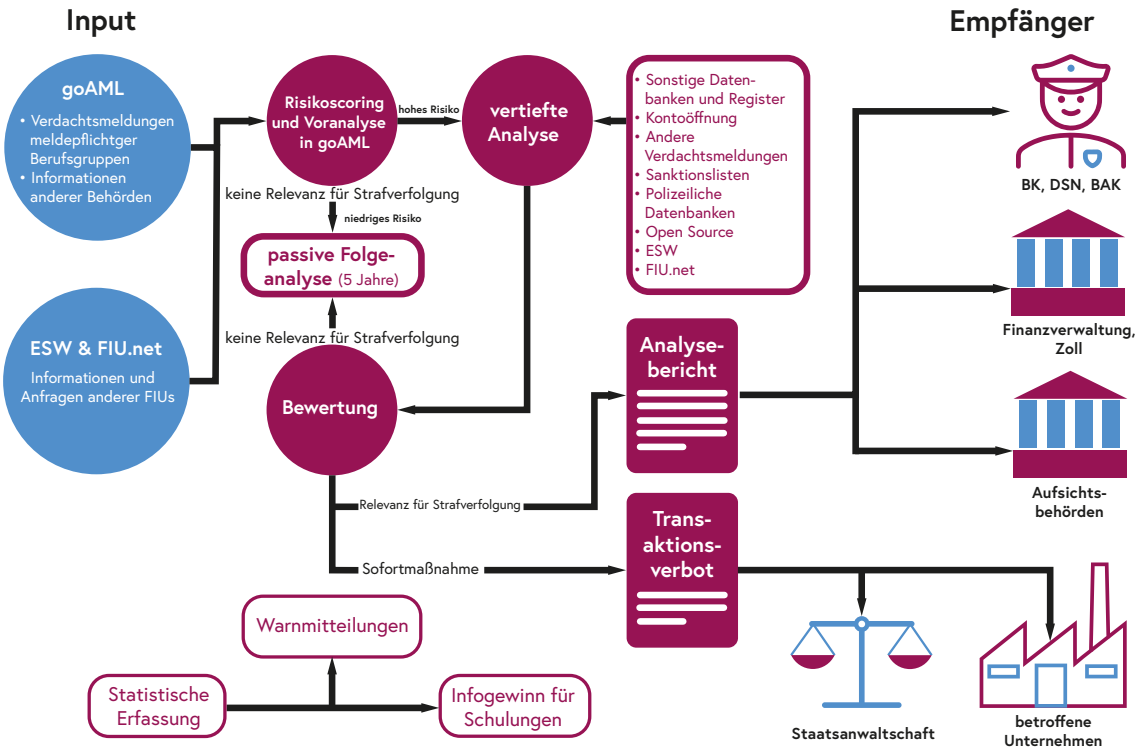
Im Berichtsjahr waren durchschnittlich 25 Mitarbeitende in der A-FIU beschäftigt.

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.

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 Sachverhalt im Zusammenhang mit Geldwäscherei, ihren Vortaten oder mit Terrorismus 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 oder die für ihre Arbeit sonst von Relevanz scheinen.



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

Der sogenannte 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. Diesem Prinzip folgend hat die A-FIU ein teilautomatisiertes Risikoscoring entwickelt, das einlangende Verdachtsmeldungen danach ordnet, wie groß ihre Wahrscheinlichkeit für Geldwäsche und Terrorismusfinanzierung ist. Das Risikoscoring orientiert sich an der Nationalen Risikoanalyse, damit möglichst jene Fälle einer vertieften Analyse unterzogen werden, die im nationalen Kontext als besonders geldwäschegeneigt betrachtet werden.

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 weiteren 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, Korruptions-

tatbeständen und dergleichen erkennbar, leitet die A-FIU das Analyseergebnis an die zuständigen Stellen im Bundeskriminalamt oder an die Landeskriminalämter (LKA) weiter.

Quellenschutz wird bei der Informationsweitergabe großgeschrieben: Im Sinne des „No-Tipping-Off" geht aus der erzeugten 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 ausreichender Verdacht einer strafbaren Handlung, behält die A-FIU die erhaltene Verdachtsmeldung für künftige Analysen auf. 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.

Um die Datenqualität weiter zu steigern, nimmt die Geldwäschemeldestelle seit diesem Berichtsjahr die Datenanlieferung von Verpflichteten nach dem FM-GwG nur noch nach einem bestimmten Standard (XML) entgegen. Die Herausforderungen für die Meldeverpflichteten, die mit dieser technischen Umstellung verbunden waren, sind nicht zu unterschätzen. Daher ging der verpflichtenden Datenanlieferung im XML-Format eine Umstellungs- und Erklärungsphase von einem Jahr voraus, in der die A-FIU den Meldeverpflichteten umfangreichen technischen Support lieferte. Die Anschaffung und der Betrieb von goAML wird durch den Fonds für die innere Sicherheit der Europäischen Union kofinanziert.

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 Beschlagnahme 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.

4
Europäische und internationale Kooperationen

Durch die Globalisierung der Wirtschaft ist die A-FIU 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 2023 in den verschiedenen internationalen Gremien, denen auch die A-FIU angehört, die Frage diskutiert, wie man mit dem Organisationsmitglied Russland umgehen solle. Sowohl die Egmont-Gruppe als auch die FATF haben im Berichtsjahr sehr deutlich Stellung dazu bezogen.

Egmont-Gruppe

Die Egmont-Gruppe ist ein weltweiter Zusammenschluss von 174 nationalen FIUs mit Hauptsitz in Toronto. Egmont hat sich 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. ESW erhielt im Berichtsjahr ein umfassendes Upgrade. Die von der Egmont-Gruppe angestrebte Vereinfachung des Systems und Beibehaltung der bisherigen Sicherheitsstandards sollte es auch technisch weniger entwickelten Ländern erlauben, am internationalen Informationsaustausch teilzunehmen.

Der mit dem Angriffskrieg gegen die Ukraine begangene Völkerrechtsverstoß und der damit verbundene Vertrauensbruch führte dazu, dass die Egmont-Gruppe im Berichtsjahr Russlands Mitgliedschaft in der Gruppe und in der Kommunikationsplattform ESW suspendiert hat.

Egmont organisiert sich 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 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, 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 2023 fand in Abu Dhabi das Plenartreffen der Egmont-Gruppe statt, bei dem die österreichische FIU wieder 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 40 Mitglieder. Die FATF ist vor allem auf politischer Ebene aktiv und erarbeitete Empfehlungen und Standards für die effektive Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Diese dienen häufig auch als Grundlage für nationale und europäische Gesetzgebungen.

Zusätzlich führt die FATF Länderprüfungen durch, um die Umsetzung ihrer Empfehlungen zu kontrollieren. Ergebnisse solcher Evaluierungen können hohen Druck erzeugen, da sich eine schlechte Länderbewertung äußerst negativ auf den Finanzsektor dieses Landes auswirkt. Österreichs letzte Überprüfung fand 2015/2016 statt. Die damals festgestellten Defizite des österreichischen Systems zur Geldwäschebekämpfung wurden in den darauffolgenden Jahren schrittweise beseitigt. Der sogenannte Enhanced Follow-up-Prozess, der der nachfolgenden Überprüfung dieser Anpassungen dient, ist abgeschlossen.

Ab 2024 beginnt die nächste Evaluierung Österreichs. Die meisten behandelten Themen sind sogenannte Querschnittsmaterien. Zu ihrer Behandlung sind allein im Bereich des Innenministeriums neben der A-FIU auch andere Dienststellen wie die DSN oder das BAK berufen. Die Abwicklung der Länderevaluierung bedarf daher auch im Innenressort einer umfassenden Koordinierung, mit der die A-FIU im Berichtsjahr begonnen hat.

Nähere Ausführungen zu der ab kommendem Jahr stattfindenden FATF-Länderevaluierung finden sich im Ausblick.

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.

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. Die A-FIU widmete sich in der Untergruppe „Ressourcen“ insbesondere dem Thema der Übersicht über vorhandene Informationsquellen der teilnehmenden FIUs mit dem Ziel, einer anfragenden FIU noch vor ihrem ersten Informationsersuchen einen Überblick darüber zu verschaffen, welche Informationen sie erwarten darf und welche nicht.

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 übernahm die Betreuung des Systems.

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 (AMLA)
- Verordnung zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung
- Sechste Richtlinie zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, sie 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 zusammen, die im Kampf gegen Geldwäscherei und Terrorismusfinanzierung beteiligt sind 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 Geldwäsche und der Terrorismusfinanzierung auch weiterhin gewährleistet bleiben.

Das Legislativpaket einschließlich der Wahl des Standorts der neuen EU-Anti-Geldwäschebehörde waren im Berichtsjahr noch nicht beschlossen. Nähere Ausführungen zu den Entwicklungen und dem Verhandlungsstand dieses Legislativpakets finden sich im Ausblick.

5
Das Jahr 2023 in Zahlen

Entsteht bei den meldeverpflichteten Berufsgruppen der berechtigte Grund zur Annahme, dass ein Geschäft in Zusammenhang mit Geldwäscherei oder der Terrorismusfinanzierung steht, müssen sie eine Verdachtsmeldung an die Geldwäschemeldestelle (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. Ebenso sind auch Behörden zur Informationsweitergabe an die A-FIU verpflichtet, wenn ihnen Sachverhalte vorliegen, die in Zusammenhang mit Geldwäscherei oder Terrorismusfinanzierung stehen könnten. Das folgende Kapitel liefert einen statistischen Überblick über die im Berichtsjahr 2023 eingelangten Verdachtsmeldungen und ihre Herkunft, über den Akteneingang im Allgemeinen und über den weiteren Umgang mit Sachverhalten, deren Analyse weitergehende kriminalpolizeiliche Ermittlungen erforderten.

Art und Herkunft der Akteneingänge

Im Jahr 2023 verzeichnete die Geldwäschemeldestelle insgesamt 8.242 Akteneingänge. Mit einer erneuten Steigerung von rund 19 Prozent im Vergleich zum Vorjahr wird der Trend der vergangenen Jahre fortgesetzt. Nicht mitgezählt sind Meldungen, die die A-FIU wegen Nichterfüllung der Mindesterfordernisse zur Verbesserung zurückstellte. Den größten Teil der Eingänge bildeten, wie in den vergangenen Jahren, die Gruppe der Verdachtsmeldungen (7.603), gefolgt von 512 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 29 Meldungen. Die unter „andere Behörden“ erfassten 90 Eingänge stammten von inländischen Dienststellen, zum Beispiel von LKA, der DSN oder vom BAK.

Herkunft der Akteneingänge	Anzahl	Anteil
Verdachtsmeldungen von meldeverpflichteten Berufsgruppen	7.603	92%
FMA	4	0%
Zollamt	9	0%
BMF und Finanzämter	15	0%
Gerichte	1	0%

Herkunft der Akteneingänge	Anzahl	Anteil
andere Behörde	90	1%
Internationaler Eingang	512	6%
Sonstige (z.B. Privateingaben)	8	0%
Summe	**8.242**	**100%**

Mit 6.482 Verdachtsmeldungen steht erneut der Bankensektor an der Spitze, gefolgt von den Dienstleistern in Bezug auf virtuelle Währungen (VASP oder Kryptoexchanger), die im Berichtsjahr 1.021 Verdachtsmeldungen erstattet haben. Das ist ein Rückgang von rund 25 Prozent im Vergleich zum Vorjahr. Diese Entwicklung dürfte auf die schlechten Kursentwicklungen der meisten Kryptowährungen im Jahr 2023 zurückzuführen sein. Die geringere Nachfrage hat zu weniger Verdachtsfällen bei den Exchangern geführt. Durch die bevorstehende Umsetzung der Verordnung über Märkte für Kryptowerte (MiCAR – Markets in Crypto Assets Regulation) ist in Zukunft aber ein Anstieg der Verdachtsmeldungen von Krypto-Exchangern zu erwarten (siehe auch Kapitel Kryptowährungen).

Die Zahlen der Verdachtsmeldungen der übrigen Berufsgruppen haben sich nicht wesentlich verändert. Qualität der Verdachtsmeldungen

Verdachtsmeldungen gruppiert nach Sektoren

Qualität der Verdachtsmeldungen

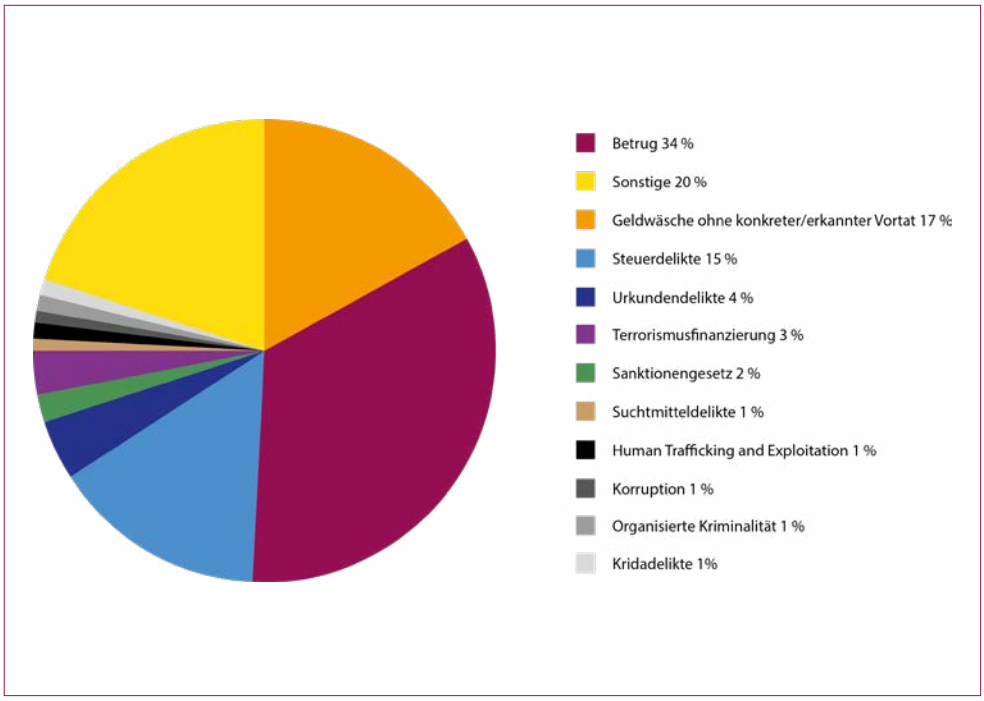
Das Analyseergebnis der A-FIU hängt stark von der Qualität der erstatteten Verdachtsmeldungen ab. Um die gemeldeten Personen und Sachverhaltselemente verlässlich in Datenbanken finden zu können, müssen die eingehenden Informationen richtig, strukturiert und vollständig übermittelt werden. Für das Verständnis der meist komplexen wirtschaftlichen Sachverhalte ist eine fundierte Erklärung der Verdachtsmomente durch die Meldeverpflichteten ebenso unerlässlich. Aus diesem Grund wird jede einlangende Verdachtsmeldung auf ihre Vollständigkeit und Richtigkeit geprüft. Genügt die Verdachtsmeldung diesen Anforderungen nicht, etwa weil sie unverständlich ist oder notwendige Beilagen fehlen oder Anhänge nicht ins Deutsche oder Englische übersetzt wurden, stellt die A-FIU die Verdachtsmeldung zur Verbesserung zurück. Die A-FIU orientiert sich dabei an den Standards, die die Aufsichtsbehörden in Rundschreiben veröffentlichen.

Die Qualität der Verdachtsmeldungen ist in den vergangenen Jahren deutlich gestiegen. Heute stellt die A-FIU nur noch sieben Prozent der erstmals einlangenden Verdachtsmeldungen zur Verbesserung zurück. In diesen Fällen erfolgt die Verbesserung meist zeitnah und verlässlich. Die deutlich sinkende Trendlinie der Zurückstellungen zeigt, wie sehr diese Maßnahme zur Qualitätsverbesserung beiträgt. Das verschafft der A-FIU auch einen wertvollen Zeitvorteil für Sicherstellungen.

Deliktsbereiche der Verdachtsmeldungen

Die Analyse der Geldwäschemeldestelle erlaubt es, die meisten Verdachtsmeldungen bestimmten Deliktsbereichen zuzuordnen. Mit 34 Prozent der Verdachtsmeldungen dominierten erstmals Betrugshandlungen die festgestellten Vortaten. Während im Vorjahr bei den meisten Fällen keine bestimmte Vortat identifiziert werden konnte, beläuft sich die Gruppe „Geldwäsche ohne konkreter/erkannter Vortat" auf nur mehr 17 Prozent.

Bei 15 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 drei Prozent der Verdachtsmeldungen berichteten über terrorismusbezogene Verdachtsmomente. Mögliche Sanktionsverstöße konnten in zwei Prozent der Verdachtsmeldungen als mögliche Vortat festgestellt werden. 24 Prozent der Meldungen konnten anderen Straftaten zugeordnet werden. Sie verteilen sich auf Suchtmitteldelikte, Kridadelikte, organisierte Kriminalität, Korruption sowie Menschenhandel.



Verdachtsmeldungen nach Deliktsbereichen

Korrespondenz mit anderen Behörden

Nationale Kooperation

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

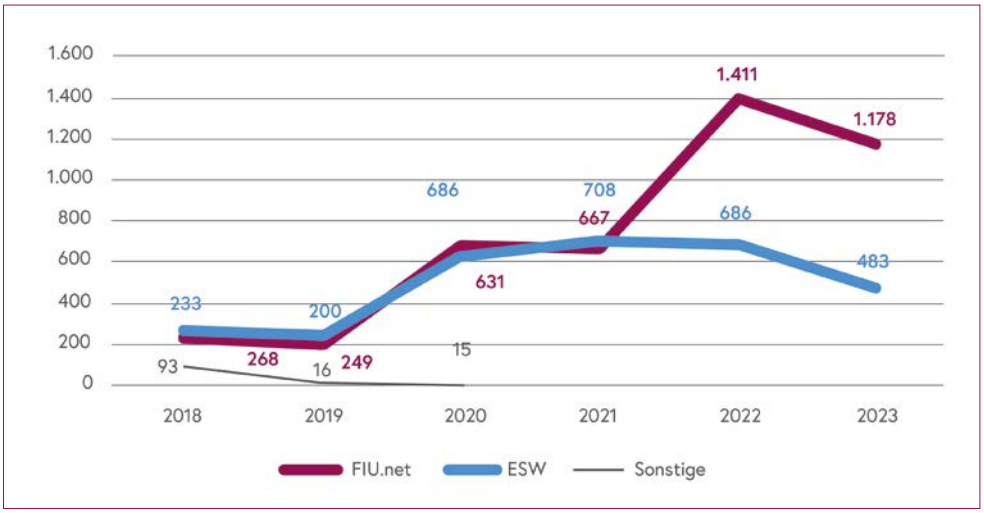
Das Finanzamt Österreich und das BMF haben bei der Wahrnehmung ihrer Aufgaben im Berichtsjahr 2023 in 15 Fällen Hinweise auf Geldwäscherei beziehungsweise Terrorismusfinanzierung gefunden und diese – entsprechend ihrer Verpflichtung nach § 18 FM-GwG – der A-FIU berichtet. Ergänzend ist das Zollamt Österreich 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 neun 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 vier 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 Jahr 2023 erhielt die Geldwäschemeldestelle 90 Ersuchen und Informationen von sonstigen Behörden, wie beispielsweise den LKA oder anderen polizeilicher Dienststellen.

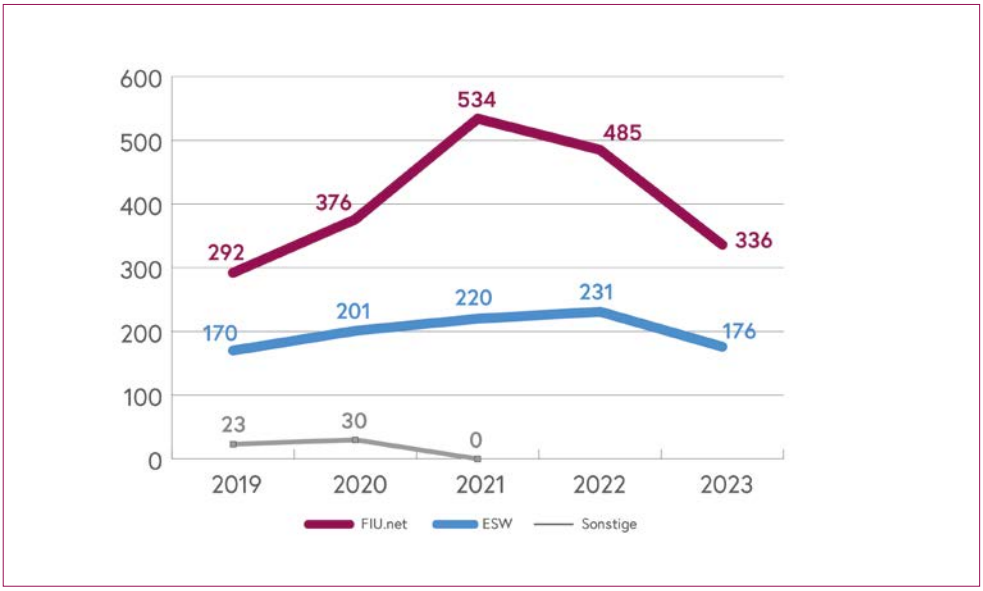
Internationale Kooperation

Die A-FIU leitete in 1.661 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 (1.178 Fälle) verwendet, gefolgt von Egmont Secure Web (483 Fälle). 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. Die 740 Meldungen übermittelte die A-FIU daher den betroffenen Partnerdiensten über FIU.net, allen voran der FIU Deutschland.



Anzahl des ausgehenden Schriftverkehrs nach Kanal: Internationaler Ausgang

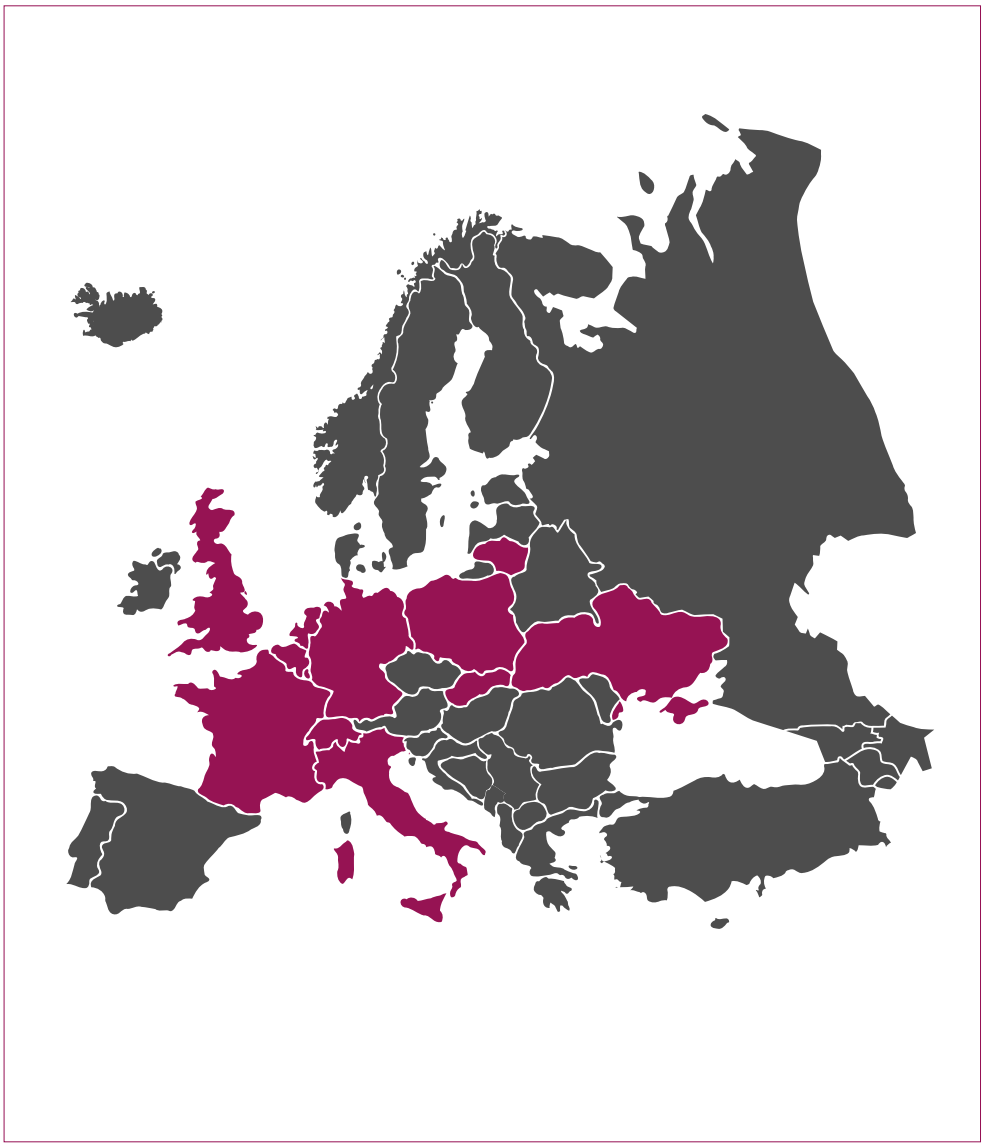
Im Berichtsjahr empfing die A-FIU 512 Informationsersuchen und Spontaninformationen ausländischer FIUs und Behörden. Dabei ist eine verstärkte Nutzung des Kommunikationskanals FIU.net feststellbar. 2023 wurde dieser in 336 Fällen genutzt. Die Kategorie „Sonstige" enthielt andere Kommunikationskanäle wie zum Beispiel 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: Internationaler Eingang

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

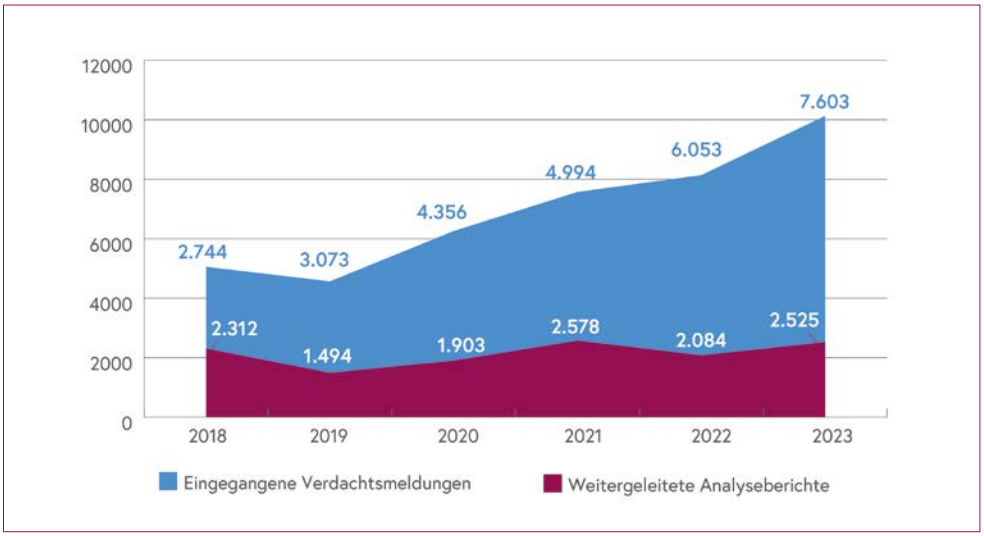
Internationaler Schriftverkehr nach Ländern



Weiterleitung von Analyseberichten

Wenn die A-FIU aufgrund ihres Analyseverfahrens zur Überzeugung gelangt, dass eine Straftat begangen worden ist oder die Informationen sonst von Relevanz für andere Behörden sind, leitet sie ihre Erkenntnisse in Form eines Analyseberichts an die Strafverfolgungsbehörden weiter.

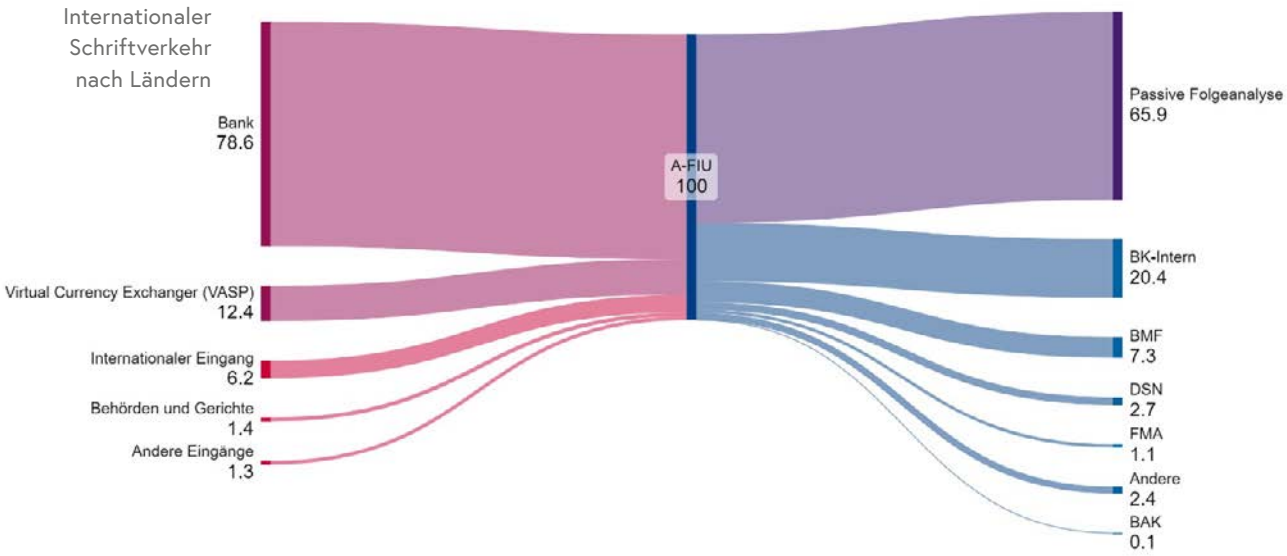
Von den insgesamt 7.603 im Berichtsjahr erhaltenen Verdachtsmeldungen gingen nach Durchführung des Analyseverfahrens 2.525 in Form von Analyseberichten an die Strafverfolgungsbehörden zur weiterführenden Ermittlung weiter. Das entspricht einem Anteil von 33 Prozent der eingelangten Verdachtsmeldungen. Demgegenüber steht die Differenz von 5.078 Fällen, die die A-FIU mangels Anfangsverdachts oder weiterer Analyseansätze zur passiven Folgeanalyse bei sich behielt.



Insbesondere die komplexen Fälle von vermuteter Geldwäsche erfordern weiterführende Sachverhaltsklärungen im Rahmen eines Ermittlungsverfahrens. Besteht der Verdacht der Geldwäsche 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 (20 Prozent) an die Fachabteilungen und Büros des Bundeskriminalamts gesandt. Rund sieben Prozent der Analyseberichte gingen wegen vermuteter Steuer- oder Zollvergehen an die Abgabenbehörden des Bundes und rund drei Prozent an die DSN weiter.

Nur in dringenden Fällen oder wenn bereits ein einschlägiges Strafverfahren anhängig war, erfolgte eine direkte Abtretung an die zuständigen ermittelnden LKA, im Berichtsjahr 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 BAK.



Auskunftsersuchen

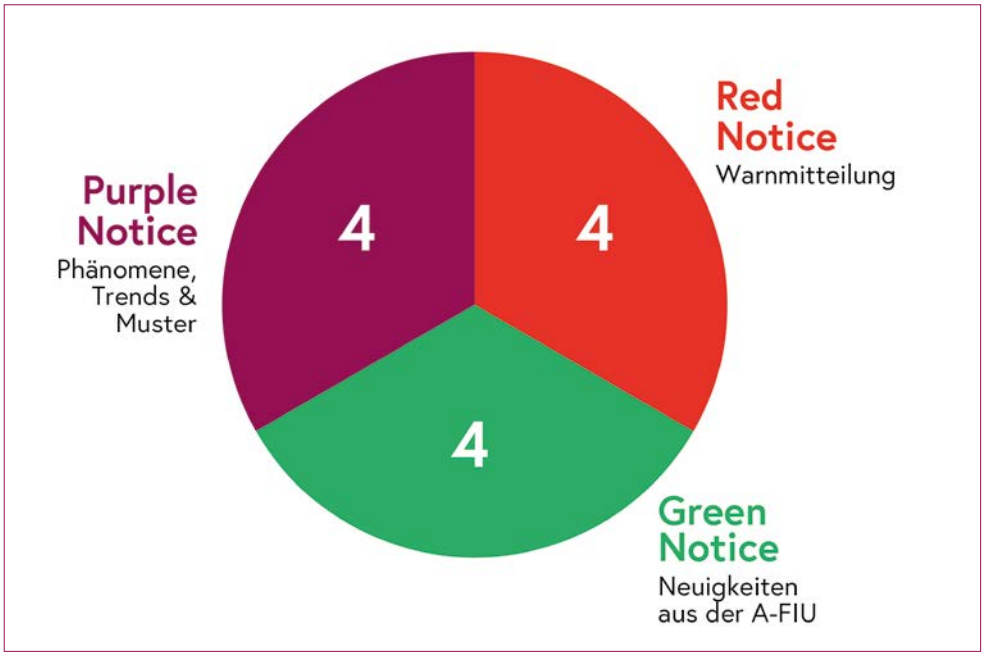
Alle Verpflichteten haben mit der Geldwäschemeldestelle zusammenzuarbeiten und ihr auf Verlangen – ungeachtet einer zuvor erstatteten Verdachtsmeldung – alle erforderlichen Auskünfte zu erteilen, die ihr zur Verhinderung oder zur Verfolgung von Geldwäscherei oder von Terrorismusfinanzierung erforderlich scheinen. Von ihrem Recht, derartige Auskünfte von den meldeverpflichteten Berufsgruppen zu verlangen, machte die A-FIU im Berichtsjahr 226 Mal Gebrauch. Die A-FIU forderte unter anderem Unterlagen über die Plausibilität der Mittelherkunft, über Kontobewegungen oder Legitimationspapiere an.

Mitteilungen und Warnmeldungen

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 Geldwäsche. 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.

Im Berichtsjahr etablierte die A-FIU ein neues Informationssystem für den Privatsektor, das drei Kategorien von Mitteilungen und Warnungen unterscheidet, die unterschiedliche

Zwecke verfolgen und farblich gekennzeichnet sind. Einzelheiten sind im Kapitel Neues Informationssystem beschrieben. Vor der Umstellung auf das neue Informationssystem



im August hat die A-FIU vier Warnmitteilungen zu konkreten verdächtigen Transaktionen und Geschäftspraktiken veröffentlicht. Ab August 2023 teilte die A-FIU zwölf Notices über den gesicherten Kommunikationskanal goAML mit den meldepflichtigen Berufsgruppen. In Reaktion auf diese Informationen der A-FIU erstatteten die meldeverpflichteten Berufsgruppen im Berichtsjahr 125 Verdachtsmeldungen.

6 Transaktionsverbote, Sicherstellungen und Verurteilungen

Transaktionsverbote und Sicherstellungen

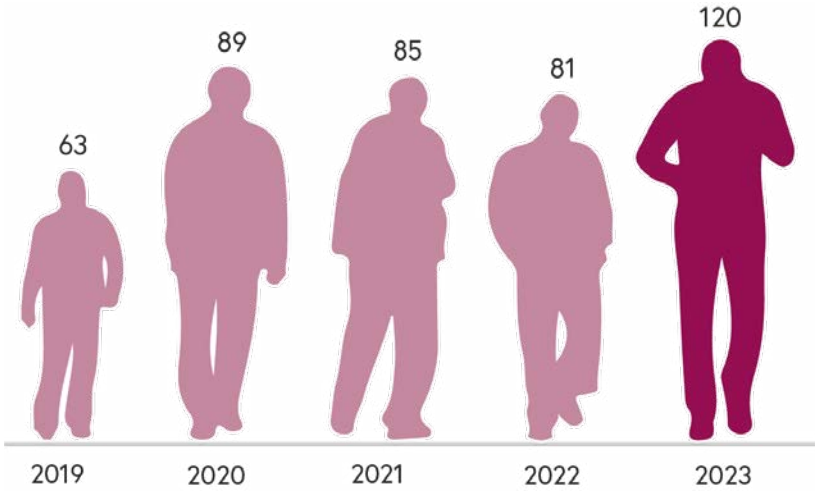
Kommt die A-FIU aufgrund ihrer Analyse zum Ergebnis, dass gegen die Abwicklung des Geschäfts oder der Transaktion Bedenken bestehen, so ist sie ermächtigt, diese mittels Anordnung vorläufig zu unterbinden. Darüber hinaus kann die A-FIU anordnen, dass Aufträge der Kundschaft über Geldausgänge nur mehr mit ihrer Zustimmung durchgeführt werden dürfen.

Über eine derartige Anordnung ist die Staatsanwaltschaft unverzüglich 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 aufzuheben. Mit der Entscheidung eines Gerichts über den Antrag auf Beschlagnahme beziehungsweise nach längstens sechs Monaten tritt die Anordnung der A-FIU 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 Beschlagnahme der bedenklichen Vermögenswerte zu entscheiden haben. Wenn die Geldwäschemeldestelle eine Transaktionssperre für notwendig erachtet, regt sie diese daher direkt bei der Staatsanwaltschaft oder bei der Kriminalpolizei 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. In Fällen vermuteter Abgabenhinterziehung regt die Geldwäschemeldestelle Sicherungsmaßnahmen bei den Abgabenbehörden des Bundes an.

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.



2023 gab es 120 rechtskräftige Verurteilungen wegen Geldwäscherei zu verzeichnen, das entspricht einem Anstieg von rund 50 Prozent im Vergleich zum Vorjahr.

Bei den bekanntgewordenen und für die Verurteilung der Geldwäscherei notwendigen Vortaten waren Verstöße gegen das Suchtmittelgesetz, Diebstähle, Betrügereien, Hehlerei, Urkundendelikte und Veruntreuungen führend.

7 Phänomene, Muster und Trends

Nach wie vor beschäftigt der russische Angriffskrieg auf die Ukraine die A-FIU. Die Reflexwirkungen des Krieges, insbesondere die Sanktionspakete der Europäischen Union und die Flucht von verdächtigen Geldmitteln aus der Ukraine nach Österreich, prägten die Arbeit der Geldwäschemeldestelle.

Das Jahr 2023 stellte die Geldwäschemeldestelle aber auch vor zahlreiche neue Herausforderungen. Besonders die technologischen Entwicklungen und neue Produkte zum Geldtransfer haben sich im Berichtsjahr bemerkbar gemacht. Sie erleichtern es Kriminellen, inkriminierte Gelder schnell, anonym und kontaktlos zu transferieren und erschweren die Rückverfolgbarkeit des Geldflusses immer mehr.

Die folgenden Beispiele zeigen, wie die technologischen Weiterentwicklungen im Zahlungsverkehr genutzt werden, um inkriminierte Gelder zu waschen.

Unklare Mittelherkunft in Zusammenhang mit Grundstückserwerben

Die zahlreichen Analysen von beabsichtigten Immobilienkäufen im Berichtsjahr bestätigen, dass sich Grundstückserwerbe für die Geldwäsche großer Vermögenswerte besonders eignen. Teure Immobilien liefern eine gute Erklärung für den hohen Mitteleinsatz. Doch allzu oft wird auf die kritische Frage nach der Herkunft der eingesetzten Gelder vergessen. Die A-FIU muss wiederholt feststellen, dass die Berufsgruppen, die bei der Abwicklung solcher Geschäfte unterstützen, teilweise sogar sehr deutliche Hinweise darauf übersehen, dass die eingesetzten Mittel aus illegalen Quellen stammen könnten.

Der folgende – etwas vereinfacht dargestellte – Fall zeigt, welche Methoden in der Praxis anzufinden sind und welche Faktoren gerne übersehen werden, die auf inkriminierte Mittel hinweisen.

Ein osteuropäischer Kaufinteressent einer großen Immobilie in Westösterreich versuchte, die Herkunft des Kaufpreises von mehreren Millionen Euro für diese Immobilie mit unterschiedlichsten Dokumenten zu legitimieren. Neben schwer lesbaren und schlecht übersetzten ausländischen Unterlagen legte der Kaufinteressent seinem Rechtsanwalt auch Verkaufsverträge über Aktien vor. Dass diese Verträge von Käuferseite gar nicht unterzeichnet waren, dürfte dem Rechtsanwalt des Kaufinteressenten nicht aufgefallen sein. Die eingesetzten Gelder übertrug der Betroffene sodann mittels Schenkung an nahe Angehörige. Diese stellten ihm die Gelder wiederum mittels Kredites zu ungewöhnlich guten Konditionen zur Verfügung, um die Liegenschaftsanteile am Geschäftskomplex in Westösterreich zu erwerben.

Schon eine schnelle Internetrecherche hätte allen involvierten Berufsgruppen aufgezeigt, dass gegen die betroffene Person im Ausland wegen groß angelegter Untreuehandlungen und anderer Wirtschaftsstraftaten ermittelt wird und es sich bei ihr um eine „politisch exponierte Person" handelt, bei denen die Mittelherkunftsprüfungen besonders streng durchzuführen sind.

Zweifel an der objektiven Wahrnehmung der Sorgfaltspflichten durch die Rechtsvertreter des Betroffenen löste nicht zuletzt der Umstand aus, dass die zu verkaufenden Immobilien den Rechtsvertretern selbst gehörten und damit ein sogenanntes Insichgeschäft zu vermuten war.

Der Fall fiel einer aufmerksamen Bank auf, die die Abwicklung des Geschäfts aufgrund der negativen Presseberichte über den Kaufinteressenten verweigerte. Das hinderte die Beteiligten aber nicht daran, es noch einmal – über eine andere Bank – zu versuchen. Auch diese verweigerte die Transaktion und erstattete eine Verdachtsmeldung bei der A-FIU.

Die A-FIU äußerte gegenüber den involvierten Berufsgruppen erhebliche Bedenken gegen die Abwicklung des Geschäfts, das im Anschluss auch Gegenstand eines Ermittlungsverfahrens wurde. Zudem stellte die A-FIU ihre Erkenntnisse den jeweiligen Kammern und Aufsichtsbehörden der betroffenen Berufsgruppen zur Verfügung, die entsprechende aufsichtsrechtliche Erhebungen einleiteten.

Die meisten Fälle vermuteter Geldwäsche im Kontext von Immobilien- oder Unternehmenskäufen erhält die A-FIU nicht von Angehörigen der rechtsberatenden Berufe oder von Immobilienmaklerinnen und -maklern, sondern von Banken. Wie dieses Beispiel zeigt, stellt sich im Zuge der Analyse der A-FIU sehr oft heraus, dass die Risikoindikatoren schon bei den zuvor mit der Vertragsabwicklung befassten Berufsträgern hätten auffallen können und sollen.

Virtuelle IBAN

Technische Weiterentwicklungen im Zahlungsverkehr machen Kundinnen und Kunden den Geldtransfer immer einfacher, doch auch Kriminelle profitieren davon. Seit 2023 verbreitet sich eine neue Form der IBAN, die sogenannte virtuelle IBAN (vIBAN).

Unter vIBAN versteht man eine von einem Finanzinstitut ausgegebene Referenznummer, die nicht nur optisch, sondern auch funktional mit der herkömmlichen IBAN identisch ist. Die vIBAN besteht wie ihr herkömmliches Ebenbild aus bis zu 34 alphanumerischen Zeichen. Im Unterschied zur klassischen IBAN garantiert der vIBAN aber nicht, dass das physische Kundenkonto ebenfalls bei der ausgebenden Bank geführt wird. Die vIBAN dient als bloße Routinginformation, damit das Geld zu einer bestimmten Bank transferiert

werden kann. Ob das physische Bankkonto tatsächlich bei dieser ausgebenden Bank liegt, darüber sagt die vIBAN nichts aus. Insbesondere virtuelle Banken, also Banken, die ausschließlich online auftreten und denen oft die technische Infrastruktur für die Abwicklung des Zahlungsverkehrs fehlt, nutzen vIBAN und lagern die tatsächliche Kontoführung an klassische Banken aus. Das physische Konto führt dann eine andere (meist klassische) Bank, die vIBAN lässt aber fälschlicherweise vermuten, das Konto läge bei der ausgebenden Bank. Das physische Konto kann je nach angebotenem Modell auch im Ausland liegen. Diese Technik macht es zudem möglich, mehrere vIBAN mit einem Masterkonto zu verknüpfen.

In der technischen Komplexität und den vielen Anwendungsmöglichkeiten liegt auch das hohe Risiko, die vIBAN für betrügerische Zwecke sowie Geldwäsche zu missbrauchen. Denn sie ermöglicht es, Betrugsopfern eine bestimmte Kontoansässigkeit vorzutäuschen. Zudem können vIBAN unendlich oft von Bank zu Bank weitergegeben werden, sodass auch die erstausgebende Bank nicht weiß, bei welcher Bank die tatsächliche Kontoführung erfolgt.

Die vIBAN birgt große Herausforderung für Behörden. Denn vIBAN müssen derzeit nicht ins Kontenregister eingetragen werden. Das versetzt die Behörden wieder in die Zeit vor Einführung des Kontenregisters zurück. Ein Auskunftsverlangen über Kontobewegungen verwandelt sich immer öfter zu einem Fragenreigen, der die Ermittelnden von einer Bank zur nächsten führt, bis endlich jene gefunden ist, die das fragliche Konto tatsächlich führt und Auskunft erteilen kann. Die langwierigen Erhebungen verbrauchen wertvolle Zeit, die bei der anschließenden Sicherstellung oder bei Transaktionsverboten der A-FIU fehlen. So entsteht die Gefahr, dass inkriminierte Gelder abgeflossen sind, bis die kontoführende Bank gefunden ist. Österreich zählt bereits eine Vielzahl an Anbietern solcher virtuellen IBAN.

Gemeinsam mit anderen europäischen Behörden, die ebenfalls negative Erfahrungen bei Ermittlungen in Zusammenhang mit vIBAN gemacht haben, setzte sich die A-FIU im Berichtsjahr erfolgreich für eine Lösung des Problems ein: Mit der zwischenzeitlich fertigverhandelten sechsten Geldwäsche-Richtlinie wird die Aufnahme von vIBAN in die europäischen Kontenregister verpflichtend.

Lebensversicherungen

Auch Lebensversicherungen mit hohen Einmalzahlungen eignen sich gut für die Wäsche von Schwarzgeld und rücken national sowie international stärker in den Fokus der FIUs. Durch die Auflösung der Lebensversicherung – wenn auch zu einem unwirtschaftlichen Rückkaufwert – kommen die Versicherten nicht nur rasch an ihr Vermögen: Die Auszah-

lung durch ein Versicherungsunternehmen vermittelt auch den Anschein einer legitimen Mittelherkunft.

Gelingt es, eine Lebensversicherung abzuschließen, ohne dass beim Versicherungsunternehmen Zweifel an der Herkunft des Geldes aufkommen, erreichen Geldwäscherinnen und Geldwäscher aber noch weitere Vorteile: Zum einen ist das Schwarzgeld auf einen Schlag von der Bildfläche verschwunden. Je nach Geduld der Versicherten kann das Vermögen sogar bis zum Ablauf der strafrechtlichen Verjährung unauffällig geparkt bleiben. Ferner gibt es keinen umfassenden Überblick über abgeschlossene Lebensversicherungen. Die Identität der wirtschaftlichen Berechtigten ist nur dem Versicherungsunternehmen bekannt, denn Lebensversicherungen sind in keinem speziellen Register eingetragen. Die internationalen Erfahrungen zeigen auch, dass das Transaktionsmonitoring bei Lebensversicherungen mit Einmalprämien nur beschränkt wirksam ist, speziell wenn zum Zeitpunkt der Einzahlung keine Anhaltspunkte für eine kriminelle Herkunft der Vermögenswerte vorlagen. Eine erneute Prüfung der beteiligten Personen auf Anhaltspunkte für Geldwäsche und ihre Vortaten erfolgt in der Regel erst zum Zeitpunkt der Rückforderung eines Anspruchs.

Vielfach werden Lebensversicherungen für Zwecke der Geldwäsche auch in Kombination mit Kreditaufnahmen missbraucht. Die notwendige Besicherung des Kredits erfolgt dann mit einer Lebensversicherung. Das im Zuge der Kreditvergabe ausgezahlte Vermögen stammt von einer redlichen Quelle, die nicht weiter hinterfragt wird. Kommt es in der Folge zu einem – unbeabsichtigten oder beabsichtigten – Kreditausfall, wird die Gläubigerbank an einer strengen Prüfung der aushaftenden Lebensversicherung kein besonderes Interesse haben.

Kryptowährungen

Kryptowährungen sind aus dem Finanzalltag nicht mehr wegzudenken. Ihre große Komplexität und ihre extreme Entwicklungsdynamik (über-)fordern Nutzerinnen und Nutzer regelmäßig. Auch die weitverbreitete Vorstellung von völlig unrealistischen Renditemöglichkeiten machen Kryptowährungen zu einem beliebten Instrument für Betrügereien. Aufsichts- und Ermittlungsbehörden sind daher berufen, präventiv über die Risiken von Kryptowährungen zu informieren.

Der sogenannte Krypto-Winter der vergangenen zwei Jahre führte mit seinen großen Kurseinbrüchen auch zu einem leichten Rückgang der Verdachtsmeldungen von Krypto-Exchangern. Unverändert bleibt jedoch die Attraktivität von Kryptowährungen für Betrugshandlungen und Geldwäsche. Kriminelle nutzen dabei die hochkomplexe Technik und den geringen Sachverstand der Opfer gepaart mit der Möglichkeit, die Gelder rasch

dem Zugriff der Behörden zu entziehen. Auffallend oft verwenden die Kriminellen bei ihren Betrugsversuchen sogenannte Stablecoins.

Einen besonderen Fokus legte die A-FIU in diesem Berichtsjahr auf die Optimierung der übermittelten Verdachtsmeldungen im Zusammenhang mit virtuellen Währungen und deren Analyse.

Stablecoins

Unter Stablecoins versteht man virtuelle Währungen, deren Wert an einen Ankerwert gekoppelt ist, wie zum Beispiel einer Fiat-Währung, oft Euro oder US-Dollar. Das Ziel von Stablecoins ist, die typische hohe Volatilität zu vermeiden und dabei die Vorteile von Kryptowährungen beizubehalten. Für Betrugshandlungen sind Stablecoins aufgrund ihrer Stabilität besonders beliebt, weil das inkriminierte Vermögen dort nur einem geringen Kursrisiko unterliegt.

Ein populärer Stablecoin ist Tether (USDT). Er ist einer der weitverbreitetsten Coins und mittlerweile Teil der meisten Handelspaare. Anders als bei anderen Kryptowährungen ist es bei Tether in ganz speziellen Fällen sogar möglich, Vermögenswerte einzufrieren. Das ist dem Bundeskriminalamt im Berichtsjahr im Rahmen eines Ermittlungsverfahrens auch gelungen. Bei allen Erfolgen bleiben die Herausforderungen bei Kryptowährungen enorm: Zum Beispiel die aufwändige Nachverfolgung von Geldflüssen, die Nutzung von Mixing-Diensten oder die Auszahlung von Geldern durch unseriöse Exchanger mit Sitz in unkooperativen oder schwach regulierten Ländern.

Crypto-FINA

Die wachsende Zahl der verpflichteten Krypto-Exchanger und die ab 2024 geltende Verordnung über Märkte für Kryptowerte (MiCAR – Markets in Crypto Assets Regulation), gibt Anlass den Dialog zwischen A-FIU und der Privatwirtschaft zu intensivieren. Bereits im Berichtsjahr hat die A-FIU Krypto-Exchanger aktiv kontaktiert und die Zusammenarbeit intensiviert. Im Vordergrund stand die Qualität der Verdachtsmeldungen.

Wegen der großen Relevanz der Kryptowährungen für Zwecke der Geldwäsche und im Bereich der Finanzkriminalität plant die A-FIU, ihre Kooperation im kommenden Jahr sowohl mit den Ermittlungsbehörden als auch mit dem Privatsektor weiter auszubauen. Die „Crypto-FINA“, eine Ausweitung der bereits bestehenden Public Private Partnership Initiative der A-FIU, wird sich auf die Krypto-Exchanger fokussieren und ein vertrauensvolles Diskussionsforum bieten. Es wird darum gehen, das Meldetool goAML besser auf Kryptowährungen anzupassen, technische Entwicklungen zu diskutieren und ihre

Risiken zu verstehen sowie aufkeimende Betrugs- und Geldwäschephänomene rasch auszubremsen.

8 Gefahren im Zusammenhang mit künstlicher Intelligenz

Die technische Weiterentwicklung und die breiten Anwendungsmöglichkeiten von Künstlicher Intelligenz (KI) bieten eine Fülle von Vorteilen, sowohl privat als auch beruflich. Doch auch Kriminelle erkennen die Einsatzmöglichkeiten künstlicher Intelligenz für ihre Zwecke. Die Technik tritt daher vermehrt in den Fokus der FIUs und ist auch international im Alltag der Ermittlungsbehörden angekommen. Insbesondere die Deepfake-Technologie, die Maschinenlernen zusammen mit KI nutzt, wird zur Herstellung von Fälschungen aller Art genutzt. Solche Fälschungen zu erkennen ist ohne technische Expertise oft nicht mehr möglich, weil die Qualität der so generierten Fälschungen sehr hoch ist.

Internationale Partner-FIUs haben die Geldwäschemeldestelle im Berichtsjahr vermehrt auf erfolgreiche Betrugshandlungen mittels KI nach dem CEO-Fraud-Phänomen aufmerksam gemacht. Dabei wurden durch täuschend echt aussehende Video- und Audiosequenzen von Geschäftsführenden eines Unternehmens Mitarbeitende und Bankangestellte dazu verleitet, Transaktionen durchzuführen. Bereits drei Sekunden Tonaufnahme genügen, um damit jede Wortfolge einer Person in einem täuschend echt klingenden Originalton nachzuahmen. In Zeiten von sozialen Medien und den häufig unbedachten Veröffentlichungen von Alltäglichem ist es keine große Herausforderung mehr, an Stimmbeispiele vieler Menschen zu gelangen. Gerade in großen Unternehmen, in denen wegen der langen Hierarchieketten eine gewisse Anonymität herrscht, können Kriminelle so erhebliche Schäden anrichten.

Risiken für Video-Ident-Verfahren

Ein großes Anwendungsfeld für den Einsatz von KI zu illegalen Zwecken stellt die Onlineeröffnung von Bankkonten mittels Video-Ident-Verfahren dar. Diese Verfahren bieten eine große Angriffsfläche für KI-Technologie. Ein großer Vorteil für Kriminelle besteht dann, wenn diese bereits im Besitz gestohlener Identitätsnachweise sind, die der KI zugeführt werden können, um Videosequenzen der Ausweisinhabenden zu fingieren. Neben Bankgeschäften können so auch Mobiltelefonverträge abgeschlossen werden.

Je nach Qualität der eingesetzten Indentifizierungsdienstleister ist das Online-Ident-Verfahren mittels KI leichter oder schwerer zu überlisten. Bisherige Fälle zeigen jedoch, dass die Kriminellen die Bankkonten, die sie durch KI mit Falschidentität eröffnen, zum Empfang und Weitertransfer von betrügerisch erlangten Geldern verwenden. Die Problematik verschärft sich noch weiter, da mit den einmal „identifizierten“ Bankkonten mittels sogenannter SEPA-Verifizierung (1-Cent-Überweisung) unkompliziert weitere Konten bei anderen Banken eröffnet werden können.

Ein erhebliches Problem steht den Ermittlungsbehörden jedoch noch bevor: In Kürze tritt die europaweite kostenlose Sofortüberweisung in Kraft. In Kombination mit den vielen Bankkonten, die (zu) einfach auf falsche Namen eröffnet werden, werden in Zukunft

inkriminierten Gelder lang außer Reichweite der Opfer und der Ermittlungsbehörden sein, bevor die Falschidentitäten überhaupt erkannt sind.

9
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 Geldwäsche überhaupt möglich.

Die folgenden Fallbeispiele beschreiben die aufsehenerregendsten Vortaten, die im Verlauf des Berichtsjahrs aufgetreten sind und zeigen die Risikolandschaft, in der sich Österreich befindet. Ihre Analysen und Erkenntnisse gibt A-FIU zur Prävention und Bekämpfung von Geldwäsche und Terrorismusfinanzierung den Aufsichtsbehörden und erforderlichenfalls den Strafverfolgungsbehörden weiter.

Abgabenhinterziehung und Scheinunternehmen

Die im Vorbericht erläuterte Problematik der Scheinunternehmen hat sich 2023 nicht entschärft. 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, somit bleiben die tatsächlich wirtschaftlich Berechtigten im Dunkeln. 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: Allein 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 auszugehen, 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. Seit 2022 erfolgt ein intensiver Austausch mit Kriminalpolizei und Staatsanwaltschaften, um die Finanzströme der Scheinunternehmen zu kappen, noch bevor diese sich im Bargeldverkehr verlieren. Denn das Bargeld ist der Motor der organisierten Schwarzarbeit.

Nice Tech GmbH

Im Juli 2023 stieß die A-FIU auf eine Reihe von Verdachtsmeldungen unterschiedlicher Banken, die einem gemeinsamen Sachverhalt zuzuordnen waren und die den Verdacht auf ein illegales Pyramidensystem begründeten. Die Kundinnen und Kunden der Bankinstitute hatten Überweisungen durchgeführt, die im Zusammenhang mit der Firma „Nice Tech GmbH“ standen.

Das angebliche Geschäftsmodell dieses Unternehmens zielte darauf ab, Kundinnen und Kunden zu akquirieren, die durch bloße Klicks auf Produkte bekannter Marken in einem speziellen Onlineshop Geld verdienen könnten. Durch die Klicks sollten die Bewertungen dieser Produkte auf großen Onlineplattformen verbessert werden. Um an diesem Geschäftsmodell teilnehmen zu können, mussten die Interessenten im Voraus Geld bezahlen. Durch höhere Beiträge wurden höhere monatliche Einkommen in Aussicht gestellt, basierend auf Hierarchiestufen und erwarteten Leistungen. Zudem versprachen die Kriminellen Prämien für die Anwerbung neuer Mitglieder.

Bei der A-FIU gingen über 100 Verdachtsmeldungen zu diesem Thema ein, aus denen rund 600 Schadensfälle mit einem Gesamtschadensvolumen von über 1,4 Millionen Euro hervorgingen. Durch die rasche Zusammenarbeit zwischen den Meldeverpflichteten,

den Ermittlungsbehörden und der A-FIU konnte die Ausbreitung dieses Pyramidenspiels eingedämmt und Beträge von knapp 800.000 Euro sichergestellt werden.

Phishing-Phänomen „FinLink“

Im Frühjahr 2023 wurden das Bundeskriminalamt und die Ermittlungsbehörden auf ein Phishing-Betrugsphänomen aufmerksam. Die Täter versandten gefälschte SMS-Nachrichten im Namen des Finanzamts und behaupteten, es bestehe ein Rückzahlungsanspruch über einen dreistelligen Euro-Betrag. Für die Auszahlung dieses Betrags sei die Verifizierung über einen in der SMS enthaltenen Link erforderlich. Tatsächlich führte der Link auf eine gefälschte FinanzOnline-Website, wo die Eingabe von Bankdaten verlangt wurde. Im laufenden Ermittlungsverfahren in der Causa „FinLink“ führte das rasche und koordinierte Vorgehen der A-FIU und der Ermittlungsbehörden bereits in der Erstphase zur Sperrung von über 20 Konten, etwa 1.700 Opfer wurden identifiziert und rund 250.000 Euro gesichert. So verloren die Kriminellen den Zugriff auf einen großen Teil der lukrierten Gelder, zahlreiche Opfer wurden entschädigt und das Phänomen war kurz nach Entstehung wieder beendet.

Bei der Tatbegehungsform „Phishing“, die einen von mehr als 50 Modi Operandi im Bereich der Betrugsphänomene darstellt, handelt es sich um den Diebstahl von persönlichen Daten, der der Vorbereitung für spätere Betrugshandlungen oder andere Straftaten dient. Konkret spähen die Kriminellen Zugangsdaten wie Bank- oder Kreditkartendaten aus, um in der Folge illegale Auszahlungen zu veranlassen. Eine Besonderheit dieses Betrugsphänomens ist, dass die meist professionell gestalteten und täuschend echt aussehenden betrügerischen Websites nur sehr kurz aufrufbar sind, bevor sie zu einer anderen Domain wechseln.

Die Auswahl der Opfer erfolgt sowohl gezielt als auch nach dem Zufallsprinzip. So werden beispielsweise ältere, vermeintlich internet- und technikunerfahrene Personen kontaktiert und für kriminelle Handlungen missbraucht. Schätzungen zufolge belief sich der Schaden allein durch Betrugsdelikte in Österreich im Jahr 2022 auf rund 700 Millionen Euro, wobei von einer sehr hohen Dunkelziffer auszugehen ist.

Krypto-Anlagebetrug EXW

Bei dem Prozess, der Ende September 2023 am Landesgericht Klagenfurt begann, handelt es sich um einen Fall von besonderer Tragweite, bei dem unter anderem der Verdacht der Geldwäsche im Raum steht. Der Prozess um den Krypto-Anlagebetrug EXW gegen elf Angeklagte wird wegen des Verdachts des gewerbsmäßigen schweren Betrugs, der

Geldwäscherei, des Pyramidenspiels und der kriminellen Vereinigung geführt. Laut Anklage sollen rund 40.000 Opfer um mindestens 17,6 Millionen Euro betrogen worden sein.

Die Krypto-Handelsplattform EXW präsentierte sich als Investitionsmöglichkeit für Anleger. Auf aufwendigen Werbeveranstaltungen wurde um Investments geworben und mit der eigens kreierten Kryptowährung EXW-Token Gewinne von mehr als 200 Prozent pro Jahr in Aussicht gestellt. Die Gelder flossen in Form von Kryptowährungen wie Bitcoins oder Bargeld an EXW. Die Anlegerinnen und Anleger hatten jedoch keine Verfügungsgewalt über den erworbenen EXW-Token, der nämlich von EXW verwaltet wurde. Tatsächlich dürften die Vermögenswerte jedoch über verschiedene Wallets und Konten weitertransferiert und ihre Herkunft verschleiert worden sein, um sie für den eigenen, luxuriösen Lebensstil zu verwenden. Es gilt die Unschuldsvermutung.

Sonstige Betrugsformen im Überblick

Die Zahl der Verdachtsmeldungen, die über erfolgte Betrugshandlungen berichten, steigt kontinuierlich. Der überwiegende Teil dieser Meldungen betrifft Bankkundinnen und -kunden, die über das Internet betrogen wurden. Dass das zu waschende Geld immer häufiger aus Onlinebetrug stammt, liegt an den immer einfacheren und rascheren Möglichkeiten zur Kontaktaufnahme mit potentiellen Opfern: Internet-Telefonie, 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 werden in der realen Welt immer noch begangen. 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 Platzes, den Betrugsdelikte bei den Vortaten zur Geldwäscherei einnehmen, hat das Büro für Betrugsermittlungen im Bundeskriminalamt 2022 ein Lagebild zum Betrug aufgebaut. Dieses gibt tagesaktuell Auskunft über die österreichweite Betrugslage, über regionale Häufungen von Betrugsanzeigen und hat sich wiederholt als Frühwarnsystem bewährt, das neueste Betrugsmaschen frühzeitig aufdeckt. Es bildet die Grundlage für Geldrückholungen bei großen Betrugssachverhalten und hilft bei der Steuerung bundesweiter Schwerpunktaktionen.

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

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. Sie sähen das Misstrauen gegenüber der Bank des Opfers mit der Begründung, korrupte Bankmitarbeiter würden die Schließfächer der Kundschaft heimlich ausräumen.

Falsche englischsprachige Polizeibedienstete

Im Dezember 2021 trat der Anrufbetrug erstmals in einer englischsprachigen Version auf. Die Täterschaft gab 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, durch Drücken der Taste 1 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 fälschte die Täterschaft 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 Geldüberweisung 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 aufscheinende 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 sodann eine Hausdurchsuchung durch, nahmen mehrere Täter in Haft und stellten Beweismaterial und Opfergelder sicher.

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 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, dem Versandbetrug einerseits und dem Warenbetrug andererseits. Beim Versandbetrug bestellen die Täter Waren im Internet 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 benutzen 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 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.

Eine weitere Form des Bestellbetrugs auf den privaten Verkaufsplattformen stellt sich so dar, dass die Täter aktiv mit den Opfern Kontakt aufnehmen. Sie geben sich als kaufwillige Interessenten aus und überreden die geschädigten 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 Ge-

schädigten 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 sodann 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, Ärztinnen, 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 Ver-

mieterplattformen geschaltet wurden. Nach Kontaktaufnahme – zumeist durch die Geschädigten selbst – wird eine Kaution in Vorauszahlung gefordert. Das Opfer erhält 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 Täterschaft 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 sodann ein vermeintliches Tradingkonto für die Opfer, oftmals unter der Bedingung, dass ein 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. 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 Email 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.

10 Kooperation mit Aufsichtsbehörden

Effektive Geldwäschebekämpfung beruht zu einem guten Teil auf einer engen Kooperation und einem vertrauensvollen Informationsaustausch zwischen der Geldwäschemeldestelle und den Aufsichtsbehörden. Während der A-FIU die Aufgabe zukommt, aus den übermittelten Verdachtsmeldungen jene mit besonders hohem Risiko für Geldwäsche und Terrorismusfinanzierung zu identifizieren, stellen die Aufsichtsbehörden sicher, dass die Wirtschaftsteilnehmenden ihre gesetzlichen Sorgfalts- und Meldepflichten auch verlässlich wahrnehmen.

Fallen der A-FIU Defizite bei der Einhaltung der Sorgfaltspflichten durch einzelne Meldeverpflichtete auf, so klärt sie diese üblicherweise bilateral mit den Verpflichteten: Unvollständige Meldungen werden beispielsweise zur Verbesserung zurückgestellt und vergessene Unterlagen telefonisch nachgefordert. Als vertrauensbildende Maßnahme lädt die A-FIU große Unternehmen mit hohem Meldeaufkommen einmal jährlich zu Abstimmungsgesprächen ein.

Dort, wo die Defizite strukturell sind oder so schwerwiegend, dass sie einer Überprüfung im Rahmen eines förmlichen Verwaltungsverfahrens bedürfen, schaltet die A-FIU die Aufsichtsbehörden ein und übermittelt die für ihre Aufsichtsverfahren notwendigen Informationen.

Doch die Kooperation beschränkt sich nicht nur auf Einzelfälle. Die A-FIU bemüht sich über konkrete Fälle von Sorgfaltsdefiziten hinaus um einen regelmäßigen strategischen Informationsaustausch mit allen Aufsichtsbehörden. Der wechselseitige Austausch von Phänomenen, Trends und Mustern soll den Aufsichtsbehörden einerseits dabei helfen, ihre Prüfungsschwerpunkte nach objektiven Risikobewertungen zu gestalten und andererseits die A-FIU auf bestimmte Verdachtsfälle für ihre Analysearbeit aufmerksam machen.

Rechtsanwaltskammern und Notariatskammer

Die Rechtsanwaltskammern, die Österreichische Notariatskammer und die A-FIU haben das Berichtsjahr dazu genutzt, ihren Informationsaustausch weiter zu intensivieren. Die Geldwäschemeldestelle stellte vermehrt Grundstücks- und Unternehmenskäufe durch vermögende Personen aus Osteuropa fest. Für Immobiliengeschäfte bedarf es der Mitwirkung von Rechtsanwältinnen und/oder Notaren, die außergewöhnlichen Geschäften oder politisch exponierten Kaufinteressenten besondere Aufmerksamkeit widmen müssen. Unter diesen Umständen müssen die Berufstragenden zum Beispiel die Rechtmäßigkeit der eingesetzten Mittel prüfen.

Die meisten Fälle vermuteter Geldwäsche im Kontext von Immobilien- oder Unternehmenskäufen erhält die A-FIU aber nicht von Angehörigen der rechtsberatenden Berufe oder von Immobilienmaklerinnen und -maklern, sondern von Banken. Bei vielen dieser

Fälle stellt sich im Zuge der Analyse der A-FIU heraus, dass die Risikoindikatoren schon bei den zuvor mit der Vertragsabwicklung befassten Berufstragenden hätten auffallen können und sollen.

Die A-FIU tauschte sich im Berichtsjahr mit den Aufsichtsbehörden intensiv über diese Fälle möglicher Sorgfaltspflichtenverletzungen und das dahinterstehende Phänomen aus. Die Kammern gehen diesen Fällen im Rahmen der Aufsichtsverfahren nach.

Glücksspielbehörde

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 Interessenvertretungen 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.

Im Berichtsjahr erfolgte dann der nächste Schritt: Die Public Private Partnership wurde um die Glücksspielaufsicht im Bundesministerium für Finanzen erweitert. Heute ist der gesamte Glücksspielsektor (sogenanntes großes und kleines Glücksspiel) unabhängig von kompetenzrechtlichen Zuständigkeiten in einem Format gefasst.

11 Strategische Entwicklungen

Neben der Analyse einzelner Verdachtsmeldungen umfasst der Auftrag der A-FIU auch die fallübergreifende Feststellung von Phänomenen, Trends und Mustern der Geldwäsche und der Terrorismusfinanzierung. Die Geldwäschemeldestelle hat den Verpflichteten Zugang zu diesen Informationen und über Anhaltspunkte zu verschaffen, an denen sich verdächtige Transaktionen erkennen lassen. Aufbauend auf den vielen operativen Einzelfällen erkennt das Referat Strategische Finanzstromanalyse die verborgenen Zusammenhänge und zeichnet ein österreichweites Lagebild.

Neues Informationssystem

Im Berichtsjahr etablierte die A-FIU ein neues Informationssystem für den Privatsektor, das drei Kategorien von Mitteilungen und Warnungen unterscheidet, die farblich gekennzeichnet sind.

Red Notices sind dringliche Warnungen zu aktuellen und konkreten Modi Operandi. Die A-FIU erwartet von den Meldeverpflichteten eine rasche Reaktion und geeignete Gegenmaßnahmen im Sinne der Warnmitteilung. Red Notices führen die bereits bekannte Warnmitteilung der A-FIU fort. Zur Wahrung der Vertraulichkeit der darin enthaltenen Informationen werden Red Notices lediglich an die tatsächlich betroffenen Berufsgruppen übermittelt.

Purple Notices dienen der frühzeitigen Information über festgestellte Phänomene, Trends und Muster, die über den konkreten Einzelfall hinausgehen. Sie bieten der Privatwirtschaft einen allgemeinen Input im Kampf gegen Geldwäsche und Terrorismusfinanzierung und für ihre Risikobewertung und können nach eigener Einschätzung genutzt werden. Purple Notices werden auf der goAML-Website veröffentlicht.

Ergänzend zu diesen Mitteilungsarten informiert die A-FIU mittels Green Notices auch über Neuerungen im Zusammenhang mit goAML sowie über Ermittlungs- und Analyseerfolge, an denen die meldeverpflichteten Berufsgruppen Anteil haben.

Financial Intelligence Network Austria (FINA)

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. Wegen der Bedeutung des Finanzsektors – die Verpflichteten nach dem FM-GwG stellen die größte Meldegruppe dar – und seiner Funktion als Gatekeeper des heimischen Finanzsystems ist eine enge Zusammenarbeit mit diesem Sektor für jede FIU von

großer Wichtigkeit. Die Geldwäschemeldestelle und das Bundesministerium für Finanzen haben zu diesem Zweck die bereits seit mehreren Jahren bestehende Arbeitsgruppe zur Bekämpfung von Finanzkriminalität weiterentwickelt und zur größten nationalen Public-Private-Partnership-Initiative im Bereich Geldwäschebekämpfung gemacht. Die Mitglieder bestehen aus den meistmeldenden Instituten und den relevanten Behörden verschiedener Ressorts. Die Sitzungsleitung übernehmen abwechselnd das Bundesministerium für Finanzen und die A-FIU.

Die Private-Public-Partnership-Initiative dient als Diskussionsplattform zur vertrauensvollen Besprechung von komplexen Fällen und allgemeinen Herausforderungen bei der täglichen Arbeit und produziert regelmäßig gemeinsame Lösungen.

Im Jahr 2023 fanden drei reguläre FINA-Sitzungen zu einer Fülle an Themen statt. Es wurden Herausforderungen technischer Natur besprochen, wie die virtuelle IBAN und deren Risiken sowie aktuelle Phänomene und Trends und ein Schwerpunkt auf die Verbesserung der Meldequalität gelegt.

Ein weiterer Termin war dem Thema Bekämpfung von Menschenhandel und der Rolle des Finanzsektors gewidmet, den das Bundesministerium für Finanzen und die A-FIU in Kooperation mit der FAST-Initiative (Finance against Slavery and Trafficking) der Vereinten Nationen im Februar 2023 organisierte. Neben Fachvorträgen wurden Möglichkeiten zur verbesserten Erkennung von Transaktionsmustern, die auf Menschenhandel hindeuten könnten, diskutiert.

European Financial Intelligence Public-Private Partnership (EFIPPP)

Die A-FIU ist auch am internationalen Dialog mit der Privatwirtschaft beteiligt. 2017 initiierte Europol die European Financial Intelligence Public-Private Partnership. Sie bringt Interessensvertretungen aus den unterschiedlichsten Bereichen auf europäischer Ebene zusammen. Zu Beginn waren 28 Institutionen aus acht Ländern vertreten. Dieses Forum entwickelte sich zu einer breiten internationalen PPP-Initiative mit circa 81 Institutionen, darunter FIUs und Finanzinstitute aus über 20 EU- und Nicht-EU-Ländern. Die EFIPPP dient zum einen dem Austausch aktueller strategischer Informationen auf multilateraler Ebene und bietet zum anderen die Möglichkeit zu persönlichen Treffen mit Expertinnen und Experten. Die zu bearbeitenden Themenfelder sind auf sieben Work-Streams verteilt. Die A-FIU ist seit 2023 aktives Mitglied der Work-Streams zu den Themen Money-Mule-Accounts und Investment Fraud und trägt in regelmäßigen Abständen mit einschlägigen Fällen und festgestellten Phänomenen bei.

Nationales Koordinierungsgremium

Das nationale Koordinierungsgremium ist ein gesetzlich eingerichtetes Forum, das sich der Entwicklung von Maßnahmen und Strategien zur Verhinderung von Geldwäsche und Terrorismusfinanzierung widmet. Es findet unter dem Vorsitz des Bundesministeriums für Finanzen statt. Neben der A-FIU nehmen Delegierte des Justizministeriums, der DSN, des Wirtschaftsministeriums, des Außenministeriums, der Finanzmarktaufsicht und der Österreichischen Nationalbank an den Sitzungen teil. Im Berichtsjahr fanden zwei Sitzungen des Nationalen Koordinierungsgremiums statt.

Task Force Sanktionen

Nach dem russischen Angriffskrieg auf die Ukraine und den darauffolgenden EU-Sanktionen richtete Österreich eine interministerielle Task Force zum Thema der Sanktionsdurchsetzung ein. Unter der Leitung der DSN war die A-FIU auf Seiten des Innenministeriums eine weitere zentrale Vertreterin. Wichtige Themen der Task Force waren legistische Arbeiten zur geplanten Novellierung des Sanktionenrechts, der Informationsaustausch mit und in der EU und die Steuerung und Koordination der Maßnahmen innerhalb der beteiligten Ressorts in Österreich.

Geldwäschetagung

Am 5. und 6. Oktober 2023 fand zum achten Mal die Österreichische Geldwäschetagung in den Wiener Räumlichkeiten der Wirtschaftskammer Österreich statt. Das völlig neue Konzept der Großveranstaltung bestand neben den Keynote-Vorträgen aus Paneldiskussionen mit den Titeln „Eine GW-Richtlinie – 27 Systeme: AML und FIUs in Europa unter kritischem Blick der Praktiker“ und „Selbstverwaltungskörper im Fokus: Was ändert sich wirklich?“.

Der zweite Tag war den meldepflichtigen Berufsgruppen gewidmet: In branchenspezifischen Workshops stellten sich die Wirtschaftskammer, die Finanzmarktaufsicht, die Notariats- und Rechtsanwaltskammer und andere den Fragen der interessierten Praktikerinnen und Praktiker.

Schulungen und Vorträge

Neben ihrem repressiven Auftrag, Geldwäsche 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 27 Schulungen ab und trug bei unterschiedlichsten Fachveranstaltungen vor, um unter anderem das Bewusstsein für die Meldepflichten zu schärfen.

Die A-FIU trug unter anderem bei sechs Schulungen für Landeskriminalämter (für angehende dienstführende Polizeibedienstete) und Staatsanwaltschaften vor, um auch im Bereich der Strafverfolgung mehr Verständnis für die Themen Geldwäsche und Terrorismusfinanzierung zu schaffen.

Auch die technischen Aspekte der Geldwäschebekämpfung wurden thematisiert. Bei sieben Schulungen vor Verpflichteten und Ministerien bildete die A-FIU die Teilnehmenden über das Meldesystem 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 mehrere Fallstudien und Phänomene bei Expertentreffen der UNODC oder regionalen FIU-Workshops.

12
Ausblick

Im Jahr 2024 beginnt 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. Ihr Ausgang entscheidet unter anderem über Österreichs (un)eingeschränkte Teilnahme am internationalen Finanzmarkt in den kommenden Jahren. Ein schlechtes Evaluierungsergebnis kann zu einer sogenannten Graulistung führen, was die Teilnahme Österreichs am internationalen Geldverkehr stark einschränken würde und Studien des Internationalen Währungsfonds und der Weltbank zufolge zu einem Kapitalabfluss von sieben bis acht Prozent (circa 36 Milliarden Euro) führen könnte. Der wirtschaftliche Gesamtschaden wird für den Fall einer Graulistung Österreichs auf rund 76 Milliarden Euro geschätzt.

Österreich ist eines der ersten Länder, das anhand der neuen fünften Prüfmethodologie geprüft wird. 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 DSN wird sich die A-FIU dem Prüfprozess im kommenden Jahr intensiv widmen.

Die umfassenden Fragenkataloge, die im Laufe des Jahres 2024 zu beantworten sind, haben die korrekte Umsetzung der FATF-Vorgaben ins österreichische Recht zum Inhalt. Die schriftlichen Antworten werden ergänzt durch eine Vor-Ort-Kontrolle eines Prüfteams im Laufe des Jahres 2025. Das Team wird zahlreiche Behörden, Kreditinstitute, Gewerbetreibende, rechtsberatende Berufe und andere interviewen und prüfen, ob es ein österreichweit gemeinsames und fundiertes Verständnis für Geldwäsche und Terrorismusfinanzierung gibt.

2024 kam es zum Abschluss der Verhandlungen über das neue Geldwäschepaket der Europäischen Union. Dieses als Single Rule Book bezeichnete Legislativpaket harmonisiert das europäische Geldwäscherecht und besteht aus vier verschiedenen Verordnungen und Richtlinien, die ins österreichische Recht umgesetzt werden müssen. Die neue EU-Anti-Geldwäschebehörde oder Anti Money Laundering Authority (AMLA) wird ihren Sitz in Frankfurt am Main haben. Die neue Geldwäsche-Richtlinie betrifft unter anderem die Kernaufgaben der europäischen FIUs, sodass ihre österreichischen Rechtsgrundlagen ab dem kommenden Jahr zu novellieren sein werden.

Aufgrund der verbundenen Risiken wird die A-FIU einen Fokus auf die Analyse der häufig eingesetzten Video-Ident-Verfahren legen. Bisherige Erfahrungen der A-FIU zeigen, dass diese Verfahren eine große Angriffsfläche für KI-Technologie bieten und für die Eröffnung von Bankkonten mit gefälschten Identitäten anfällig sind.

Wegen der großen Relevanz der Kryptowährungen für Zwecke der Geldwäsche und im Bereich der Finanzkriminalität plant die A-FIU, ihre Kooperation im kommenden Jahr sowohl mit den Ermittlungsbehörden als auch mit dem Privatsektor weiter auszubauen. Die „Crypto-FINA“ wird sich auf die Krypto-Exchanger fokussieren und ein vertrauensvolles Diskussionsforum mit diesem Sektor bieten.