

Lagebericht Geldwäsche 2024

Aktuelle Entwicklung der Geldwäsche
und der Vermögenskriminalität



Lagebericht Geldwäsche 2024

Aktuelle Entwicklung der Geldwäsche
und der Vermögenskriminalität

Wien, 2025

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, 2025

Vorwort

Sehr geehrte Damen und Herren,

das Jahr 2024 stellte die Geldwäschemeldestelle (A-FIU) im Bundeskriminalamt erneut vor erhebliche Herausforderungen. Während klassische Betrugs- und Geldwäscheformen weiterhin aktuell bleiben, haben sich kriminelle Methoden durch Digitalisierung und neue Technologien weiterentwickelt – insbesondere im Bereich neuer digitaler Zahlungsprodukte und Kryptowährungen.

Der Finanzplatz Österreich bleibt attraktiv für Kriminelle, die versuchen, Erlöse aus Betrug oder anderen Straftaten zu waschen. Digitale Zahlungsprodukte wie Echtzeitüberweisungen erhöhen die Geschwindigkeit und Anonymität von Transaktionen erheblich. Auch Kryptowährungen gewinnen weiter an Bedeutung – sowohl als Zahlungsmittel für illegale Geschäfte, beispielsweise im Darknet, als auch zur Verschleierung von Geldflüssen aus inkriminierten Quellen.

Zur effektiven Bekämpfung dieser Entwicklungen hat die A-FIU 2024 ihre Zusammenarbeit mit Aufsichtsbehörden und meldepflichtigen Berufsgruppen weiter intensiviert. Durch eine überarbeitete Kommunikationsstrategie und den Ausbau des Austauschs zwischen dem öffentlichen und dem privaten Sektor – etwa im Rahmen des Financial Intelligence Network Austria – wurde das gemeinsame Lageverständnis deutlich gestärkt.

Ein Schwerpunkt des Jahres war zudem die Vorbereitung auf die bevorstehende Evaluierung der Financial Action Task Force (FATF). Die Einhaltung der 40 FATF-Empfehlungen ist nicht nur für die Kriminalitätsbekämpfung zentral, sondern auch für den Erhalt eines starken und vertrauenswürdigen Wirtschaftsstandorts. Die enge Kooperation zwischen den BMI-internen Stakeholdern des Bundeskriminalamts, der Direktion Staatsschutz und Nachrichtendienst sowie dem Bundesamt zur Korruptionsbekämpfung war, neben dem intensiven Austausch mit externen Beteiligten, entscheidend für die Vorbereitung.

Wir danken allen Mitarbeitenden der A-FIU sowie unseren Partnerinnen und Partnern in Behörden und dem privaten Sektor für ihr Engagement und die konstruktive Zusammenarbeit im Berichtsjahr 2024. Gemeinsam konnten wir neue Typologien erkennen, Risiken besser bewerten und die Geldwäschebekämpfung weiterentwickeln. Diese Ziele werden auch im kommenden Jahr intensiv weiterverfolgt, um den Finanz- und Marktplatz Österreich noch sicherer zu machen.



Generaldirektor für die
öffentliche Sicherheit
Franz Ruf



Direktor des
Bundeskriminalamts
Andreas Holzer

A stylized handwritten signature in black ink.

Franz Ruf

Generaldirektor für die
öffentliche Sicherheit

A stylized handwritten signature in blue ink.

Andreas Holzer

Direktor des
Bundeskriminalamts

Inhalt

Vorwort	3
Einleitung	8
Das Phänomen Geldwäsche	8
Kampf gegen die Geldwäsche	10
Sorgfaltspflichten der Verpflichteten	10
Das Delikt Geldwäscherei – § 165 Strafgesetzbuch	12
Die Austrian Financial Intelligence Unit (A-FIU)	14
Organisationsaufbau	14
Funktionen der A-FIU	15
Filterfunktion	15
Analyseverfahren	17
Befugnisse der A-FIU	18
Erheben, Verarbeiten, Übermitteln	18
Vorläufiges Unterbinden oder Aufschieben von Transaktionen	19
Europäische und internationale Kooperationen	21
Egmont-Group	21
Financial Action Task Force (FATF)	22
Financial Intelligence Unit Plattform	23
Advisory Group	23
FIU.net	23
Legislativpaket der Europäischen Kommission	24
Das Jahr 2024 in Zahlen	25
Art und Herkunft der Akteneingänge	25
Qualität der Verdachtsmeldungen	26
Deliktsbereiche der Verdachtsmeldungen	28
Korrespondenz mit anderen Behörden	29
Nationale Kooperation	29

Internationale Kooperation.....	29
Weiterleitung von Analyseberichten.....	30
Auskunftsersuchen.....	32
Mitteilungen und Warnmeldungen.....	32
Transaktionsverbote, Sicherstellungen und Verurteilungen.....	33
Transaktionsverbote und Sicherstellungen.....	33
Verurteilungsstatistik.....	34
Phänomene, Muster und Trends.....	35
Identitätsdiebstahl und Gelwäsche über Online-Konten.....	35
Missbräuchliche Gründung von Vereinen.....	36
Lebensversicherungen.....	37
Echtzeitüberweisungen.....	38
Kryptowährungen.....	38
Gefahren im Zusammenhang mit künstlicher Intelligenz.....	40
Vortaten zur Geldwäscherei.....	41
Phishing-Phänomen „FinLink“.....	42
Krypto-Anlagebetrug EXW.....	42
Sonstige Betrugsformen im Überblick.....	44
Anrufbetrug.....	44
Bestellbetrug.....	46
Cyber-Trading-Fraud.....	47
CEO-Fraud und Business E-Mail Compromise.....	48
Phishing-Betrug.....	49
Vorauszahlungsbetrug.....	50
Kooperation mit Aufsichtsbehörden.....	52
Rechtsanwaltskammern und Notariatskammer.....	52
Glücksspielbehörde.....	53
Gewerbeaufsichtsbehörden.....	53

Strategische Entwicklungen	55
Mitteilungssystem	55
Financial Intelligence Network Austria (FINA)	56
Crypto-FINA	57
PPP Rechtsberatende Berufe	57
European Financial Intelligence Public-Private-Partnership (EFIPPP)	57
Nationales Koordinierungsgremium	58
Task-Force-Sanktionen	58
Geldwäschetagung	58
Schulungen und Vorträge	58
Ausblick	60

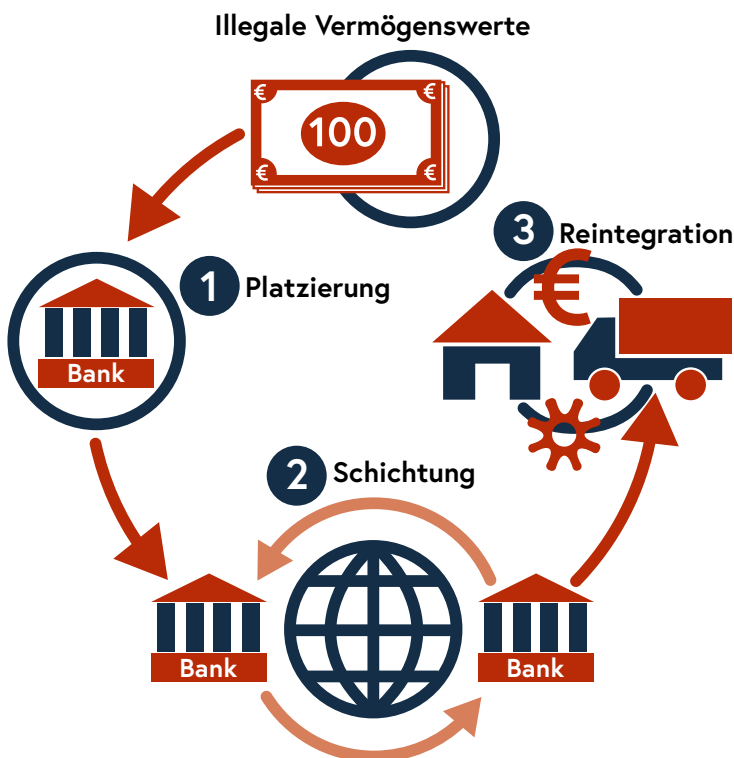
Einleitung

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 2024.

Die Analysen der Geldwäschemeldestelle zeigen, dass Onlinebetrug, Sozialmissbrauch und Abgabenhinterziehung in Form von Scheinunternehmen besonders häufig als Vortaten zur Geldwäscherei auftreten. Jedoch war auch ein Anstieg von Verdachtsmeldungen im Zusammenhang mit Terrorismusfinanzierung zu sehen. 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 hauptsächlich diesen Delikten – im Kapitel Vortaten zur Geldwäscherei.

Das Phänomen Geldwäsche

Typischer Geldwäscheprozess



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“)
- 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.

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 Dienstleisterinnen und Dienstleister am Finanzmarkt, Wirtschaftstreuhand-, Bilanzbuchhaltungs- und rechtsberatende Berufe, Immobilienmaklerinnen und Immobilienmakler sowie Anbieterinnen und Anbieter von Kryptowerte-Dienstleistungen (VASPs). 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 beziehungsweise Umgehung gezielter finanzieller Sanktionen im Zusammenhang mit Proliferationsfinanzierung für die Berufsgruppe der Kredit- und Finanzdienstleisterinnen und -dienstleister als auch VASPs. Dieses Gesetz dient regelmäßig als Vorbild für die Sorgfaltspflichten der anderen Berufsgruppen. Deren Sorgfaltspflichten sind teilweise gleichlautend in der Rechtsanwaltsordnung, der Gewerbeordnung, der Notariatsordnung oder dem Wirtschaftstreuhandberufsgesetz verankert.

Die wesentlichsten Sorgfaltspflichten der meldepflichtigen Berufe umfassen:

Unternehmensbezogene Risikoanalyse

Diese dient dazu, das konkrete Risiko für das Unternehmen einschätzen zu können, von Dritten für Geldwäsche oder Terrorismusfinanzierung missbraucht zu werden. Abhängig vom Kundenstock, Branche et cetera handelt es sich hierbei um eine individuelle Einschätzung der bzw. des Verpflichteten selbst.

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 berechnete 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 unter Berücksichtigung des Gesamtrisikos 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. Diese gilt gegenüber allen verpflichteten Berufsgruppen und stellt ein wichtiges Element in der Analysearbeit der A-FIU dar.

Die Melde- und Auskunftsverpflichtung 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 wie auch Versicherungsvermittler 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 die Täterin bzw. den Täter dabei zu unterstützen, sich der Strafverfolgung zu entziehen,

oder

wer die wahre Natur, Herkunft oder Lage von Vermögensbestandteilen, die aus bestimmten schweren Straftaten stammen, **verheimlicht** oder **verschleiert**.

Beispiel für die erste Form der Tatbegehung ist eine Frau, die mit den Erträgen eines Drogengeschäfts ins Casino geht und das Geld über ein paar risikolose Roulettespiele in vermeintlich sauberes Geld umwandelt. Oder ein Finanzagent, 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 haben gemeinsam, 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 eins ist es übrigens irrelevant, ob die Geldwäsche durch dieselben Kriminellen begangen wird, wie das vorgelagerte Delikt (sogenannte Eigengeldwäsche) oder ob sie durch Dritte erfolgt (sogenannte Fremdgeldwäsche). 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.

Die Austrian Financial Intelligence Unit (A-FIU)

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 A-FIU, auch als Geldwäschemelde-stelle bezeichnet, ist im Bundeskriminalamt angesiedelt. Sie bildet in ihrer Zentral-stellenfunktion die einzige Ansprechstelle für meldepflichtige Berufsgruppen bei den Sicherheitsbehörden in Sachen Geldwäscherei und Terrorismusfinanzierung.

Organisationsaufbau

Die Geldwäschemeldestelle ist in die Abteilung 7 (Wirtschaftskriminalität) des Bundes-kriminalamtes 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 Weiter-entwicklung und die laufende Optimierung von technischen und rechtlichen Kooperati-ons- und Kommunikationsmethoden zwischen der A-FIU und ihren weltweiten Partner-behörden.

Das Referat Strategische Finanzstromanalyse betrachtet Meldungen und sonstige Infor-mationen 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 Meldever-pflichteten weiter. Sie dienen der Bewusstseinsbildung bei den meldepflichtigen Berufs-gruppen sowie der frühzeitigen Erkennung von strafrechtlich relevanten Sachverhalten.

Dem Referat Operative Finanzstromanalyse obliegt die Entgegennahme der Verdachts-meldung 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.

Zudem steht der A-FIU ein dreiköpfiges Technikerinnen- und Technikerteam für die Entwicklung interner Softwarelösungen zur effizienteren Analyse und Hilfsmittel hierzu sowie für die statistische Erfassung von relevanten Daten und der laufenden Betreuung des Kommunikationskanals goAML zur Verfügung.

Als Beitrag zur neuen EU-Behörde zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (Anti Money Laundering Authority – AMLA) hat die A-FIU zwei neue Planstellen geschaffen. Die zwei Mitarbeitenden der A-FIU werden vor Ort die österreichischen Interessen vertreten, die notwendige Policy-Arbeit vorantreiben sowie bei sogenannten Joint Analysis Teams mitwirken und koordinieren, die bei wichtigen grenzüberschreitenden Fällen gebildet werden.

Im Jahr 2024 wurde zudem die zukunftsorientierte personelle Weiterentwicklung der A-FIU beschlossen. Demnach wird die A-FIU bis 2026 mit zusätzlichen 17 Planstellen ausgestattet, um so den kommenden Herausforderungen wie der stark steigenden Anzahl an Verdachtsmeldungen oder dem verstärkten Feststellen und Analysieren von Großakten entgegenzutreten zu können.

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

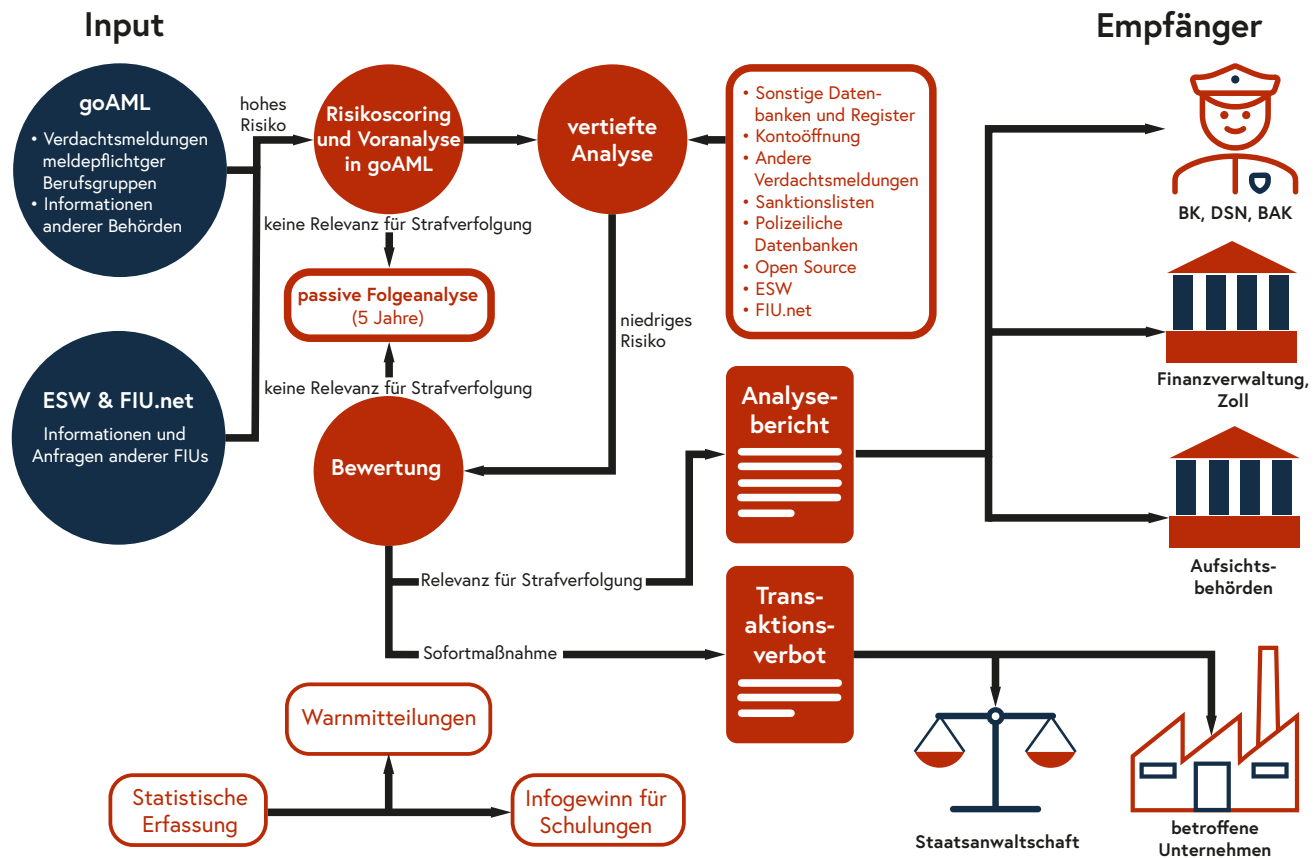
Funktionen der A-FIU

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 mit Geldwäscherei oder Terrorismusfinanzierung zusammenhängt. 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. Dies geschieht, indem diesen nur Sachverhalte übermittelt werden, deren strafrechtliche Verfolgung aufgrund eines vorliegenden Anfangsverdachts gerechtfertigt ist oder die für ihre Arbeit relevant 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 Geldwäsche, ihre Vortaten oder Terrorismusfinanzierung (Vollständigkeits- und Zulässigkeitsprüfung). Die Datenübermittlung erfolgt ausschließlich 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 unter anderem an der Nationalen Risikoanalyse oder internationaler Typologien beziehungsweise Berichte der FATF, aber auch basierend auf einer tiefgreifenden Analyse zusammenhängender Daten eingehender Verdachts-

meldungen. Das dient dazu, jene Fälle einer vertieften Analyse zu unterziehen, die auf Basis dieses komplexen risikobasierten Verständnisses als besonders geldwäschegeneigt einzustufen sind.

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 beginnt einen internationalen Schriftverkehr mit ausländischen Partnerdiensten.

Die A-FIU ist jedoch nicht im Dienst 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 für Staatsschutz und Nachrichtendienst (DSN) weiter, bei Verdacht auf Korruptionsdelikte an das Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung (BAK). Besteht der Verdacht der Geldwäscherei oder ihrer Vortaten, ist aber kein Zusammenhang mit besonderen Tatbeständen wie Sanktionsbrüchen, Proliferation, Steuerhinterziehung, Zollvergehen, Korruptionstatbeständen 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 solche 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. Im umgekehrten Wege gibt die A-FIU auch regelmäßig Informationen wie Typologien, Warnungen oder sonstige wichtige Hinweise über goAML an die Verpflichteten weiter.

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 Meldepflichtigen, 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 dem die A-FIU den Meldepflichtigen umfangreichen technischen Support lieferte. Die Anschaffung und der Betrieb von goAML wird durch den Fonds für die innere Sicherheit der Europäischen Union kofinanziert.

Die A-FIU ist befugt, ihre Analyseergebnisse und andere relevante Informationen – 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.

ISF-Projekt Interoperabilität

Im Jahr 2024 setzte die Geldwäschemeldestelle (A-FIU) ihre in den Vorjahren erfolgreich betriebene Projekttätigkeit im Rahmen des Internal Security Funds (ISF) der Europäischen Union fort. Dieses wichtige europäische Förderprogramm wurde für den Zeitraum 2021 bis 2027 mit einem Gesamtbudget von 1,93 Milliarden Euro eingerichtet und hat das Ziel, die Sicherheit in der EU zu erhöhen. Der Fonds unterstützt gezielt den Kampf gegen Terrorismus, Radikalisierung, schwere und organisierte Kriminalität sowie Cyberkriminalität.

Die Projektziele der A-FIU sind breit gefächert und umfassen mehrere wichtige Bereiche: den Betrieb und die Weiterentwicklung von IT-Systemen, personelle Aufstockung, die Beschaffung technischer Ressourcen sowie die Ermöglichung von internationalem Expertinnen- und Expertenaustausch zur Implementierung technischer Fortschritte. Dadurch wird die Zusammenarbeit zwischen den Behörden im Bereich der Geldwäsche und Terrorismusfinanzierung sowie die Interoperabilität – also die Fähigkeit verschiedener Systeme, miteinander zu arbeiten – deutlich verbessert.

Der Internal Security Fund ermöglicht es der A-FIU, ihre technischen und personellen Kapazitäten gezielt auszubauen. Besonders wichtig ist dabei die Verbesserung der grenzüberschreitenden Zusammenarbeit, da Geldwäsche und Terrorismusfinanzierung häufig internationale Dimensionen haben. Durch moderne IT-Systeme und den verstärkten Austausch mit europäischen Partnerbehörden können verdächtige Finanztransaktionen schneller erkannt, analysiert und verfolgt werden.

In diesem Zusammenhang werden sowohl technische Maßnahmen – wie die Weiterentwicklung von Soft- und Hardwarelösungen – als auch strukturelle Komponenten, darunter Personalkosten zur Sicherstellung der operativen Umsetzung, gefördert. Die Initiative unterstützt damit das übergeordnete Ziel des ISF, die innere Sicherheit in der Europäischen Union durch verbesserte polizeiliche Zusammenarbeit, effizientere Kriminalitätsbekämpfung und abgestimmte Präventionsmaßnahmen zu stärken.

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. Zudem haben sie das Recht von der A-FIU eine Entscheidung 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 steht die A-FIU jedoch 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 Transaktions Sperre für notwendig erachtet, regt sie diese 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 Rechtsschutz für die Betroffenen.

Zudem kann im Falle von erheblichen Bedenken gegen die Durchführung einer Transaktion, eines Geschäfts seitens der A-FIU die Aussprache einer sogenannte Bedenkenäußerung gemäß § 17 Absatz 3 FM-GwG erfolgen. In diesem Fall kann auf Basis des Gesamt Sachverhalts noch kein Transaktionsverbot beziehungsweise eine Sicherstellung durch die Staatsanwaltschaft durchgeführt werden. Jedoch besteht in diesen Fällen nicht plausibilisierbarer Finanzflüsse, beispielsweise aufgrund der handelnden Personen, ein erhöhtes Risiko im Bereich der Geldwäsche, welches in einer Bedenkenäußerung der A-FIU mündet. In diesen Fällen obliegt es den jeweiligen Meldeverpflichteten, entsprechend deren Risikoappetit, ob sie das Geschäft trotz der mitgeteilten Bedenken der A-FIU durchführen oder davon Abstand nehmen.

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 Kontakt mit internationalen Partnerinnen und Partnern aufzubauen und zu vertiefen.

Egmont-Group

Die Egmont-Gruppe ist ein weltweiter Zusammenschluss von 177 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. 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 Jahr 2023 Russlands Mitgliedschaft in der Gruppe und in der Kommunikationsplattform ESW suspendierte und diese auch im Berichtsjahr 2024 nach wie vor aufrecht ist.

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 die ihre Erfahrungen im operativen und technischen Bereich teilen. Die Ergebnisse werden präsentiert und anschließend den Mitgliedern zur Verfügung gestellt.

Membership, Support and Compliance Working Group (MSCWG)

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

Policy and Procedures Working Group (PPWG)

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

Technical Assistance and Training Working Group (TATWG)

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

Im Juli 2024 fand das Plenartreffen der Egmont-Gruppe in Paris 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 hat Empfehlungen und Standards für die effektive Bekämpfung von Geldwäsche und Terrorismusfinanzierung erarbeitet. 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.

2024 hat die nächste Evaluierung Österreichs begonnen. Die meisten behandelten Themen sind sogenannte Querschnittsmaterien. Zu ihrer Behandlung sind alleine 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 begann.

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 Expertinnen- und 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 war bis Mitte 2024 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 Geldwäsche 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.

FIU.net

Bei FIU.net handelt es sich um ein dezentralisiertes System, das von den 27 FIUs der Union, FIU Norwegen, der Europäischen Kommission und Europol, gemeinschaftlich verwendet wird. Über dieses System werden Informationen zu Geldwäsche und Terrorismusfinanzierung gesichert ausgetauscht, die einen Bezug zu einem anderen europäischen Mitgliedstaat 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. Seit Anfang 2023 arbeitet die Kommission an einer neuen Version der FIU.net-Anwendung, die in enger Zusammenarbeit mit der FIU-Gemeinschaft entwickelt wird. Die „Next-Generation“ FIU.net, die 2025 live gehen wird, bietet verbesserte Leistung, Stabilität, Flexibilität und Sicherheit durch den Einsatz modernster Technologien. Dies soll den Austausch zwischen den FIUs noch schneller und einfacher machen.

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 und am 9. Juli 2024 in Kraft getreten ist:

- Verordnung zur Schaffung einer neuen EU-Behörde für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AMLA)
- Verordnung zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung („Single Rulebook“)
- Sechste Richtlinie zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, sie ersetzt die fünfte Geldwäsche-Richtlinie
- Überarbeitung der Geldtransfer-Verordnung von 2015

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. Hierzu fanden im Berichtsjahr 2024 erste interministerielle sowie bilaterale Termine zur Umsetzung des Geldwäschepakets sowohl auf nationaler als auch auf europäischer Ebene statt. Die ersten Entwürfe sollen im Folgejahr entstehen. Die A-FIU ist intensiv in diese legislativen Vorgänge eingebunden.

So soll eine nachhaltige und zielgerichtete Bekämpfung der Geldwäsche und der Terrorismusfinanzierung auch weiterhin gewährleistet werden.

Das Jahr 2024 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 Auskunftspflichten 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 2024 eingelangten Verdachtsmeldungen und ihre Herkunft, über den Akteneingang im Allgemeinen sowie über den weiteren Umgang mit Sachverhalten, deren Analyse weitergehende kriminalpolizeiliche Ermittlungen erforderten.

Art und Herkunft der Akteneingänge

Die A-FIU hat für das Berichtsjahr 2024 eine umfangreiche Umstellung der statistischen Berechnungsart (auf Basis der goAML Aufzeichnungen) aller Akteneingänge durchgeführt, weshalb eine direkte Gegenüberstellung mit Eingängen aus Vorjahren nicht mehr sinnvoll möglich ist. Um jedoch zumindest einen direkten Vergleich mit dem Vorjahr zu ermöglichen, wurde das Jahr 2023 nach den neuen statistischen Rechenmethoden berechnet. Zur Veranschaulichung und zum Vergleich mit dem Vorjahr wird der Anstieg an Meldungen prozentuell dargestellt. So erklären sich die Abweichungen in der Anzahl an Eingängen und Verdachtsmeldungen zum Vorjahresbericht.

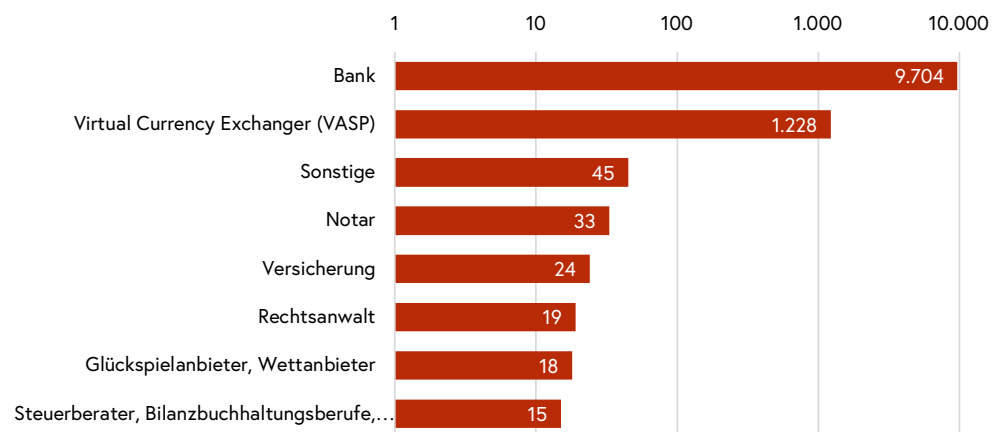
Im Jahr 2024 verzeichnete die Geldwäschemeldestelle insgesamt 12.924 Akteneingänge und überstieg somit erstmals die Hürde von 10.000 Eingängen. Unter Anwendung der eingangs erwähnten neuen Rechenmethode auf das Vorjahr 2023 wurde eine erneute deutliche Steigerung von rund 15 Prozent im Vergleich zum Vorjahr verzeichnet, womit sich der Trend der vergangenen Jahre fortsetzt. Nicht mitgezählt sind Meldungen, die die A-FIU wegen Nichterfüllung der Mindestanforderungen zur Verbesserung zurückstellte.

Den größten Teil der Eingänge bildeten wie in den vergangenen Jahren die Gruppe der Verdachtsmeldungen von Verpflichteten (11.086). Von Behörden erhielt die A-FIU im Berichtsjahr insgesamt 25 Verdachtsmeldungen.

Mit 9.704 Verdachtsmeldungen steht der Bankensektor erneut an der Spitze, gefolgt von dem Anbieter von Kryptowerte-Dienstleistungen (VASPs), die im Berichtsjahr 1.228 Verdachtsmeldungen erstattet haben. Das ist ein Anstieg von circa 20 Prozent, nach dem Rückgang im Vorjahr. Diese Entwicklung zeichnete sich aufgrund der massiven Kursgewinne diverser Kryptowährung im Berichtsjahr und damit verbundenem Zugewinn an Interesse ab. Die erhöhte Nachfrage hat im Umkehrschluss aber zu mehr Verdachtsfällen bei VASPs geführt. Durch die bevorstehende Umsetzung der Verordnung über Märkte für Kryptowerte (MiCAR – Markets in Crypto Assets Regulation) und der potenziellen Ansiedelung neuer Anbieterinnen und Anbieter am Standort Österreich ist in Zukunft mit einem erneuten starken Anstieg der Verdachtsmeldungen von VASPs (künftig CASPs) zu rechnen.

Erfreulicherweise zeigte das intensive Präventionsprogramm der A-FIU sowie die verstärkte Kooperation durch Schulungen und neuen PPP-Initiativen Wirkung. In fast allen verpflichteten Kategorien konnte ein Anstieg an Verdachtsmeldungen verzeichnet werden.

Verdachtsmeldungen gruppiert nach Sektoren

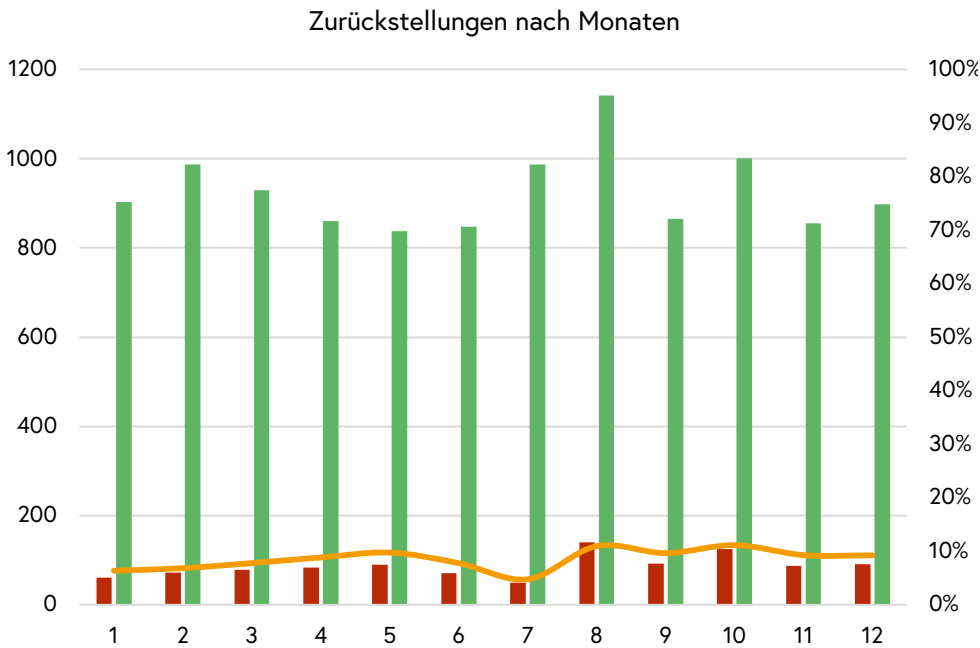


Qualität der Verdachtsmeldungen

Das Analyseergebnis der A-FIU sowie das Feststellen neuer Typologien und Trends 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, 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 gestiegen. Im Berichtsjahr stellte die A-FIU neun Prozent der erstmals einlangenden Verdachtsmeldungen zur Verbesserung zurück, was einen minimalen Anstieg zum Vorjahr darstellt. Und auch in diesen Fällen erfolgt die Verbesserung meist zeitnah und verlässlich. Die folgende Grafik zeigt die Gegenüberstellung von akzeptierten zu erstmals zurückgestellten Verdachtsmeldungen im Jahr 2024. Die Qualitätsverbesserung von Meldungen und die damit erhöhte Verlässlichkeit der erhaltenen Daten verschafft der A-FIU einen wertvollen Zeitvorteil für Sicherstellungen und andere Maßnahmen zur Verhinderung sowie zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung.

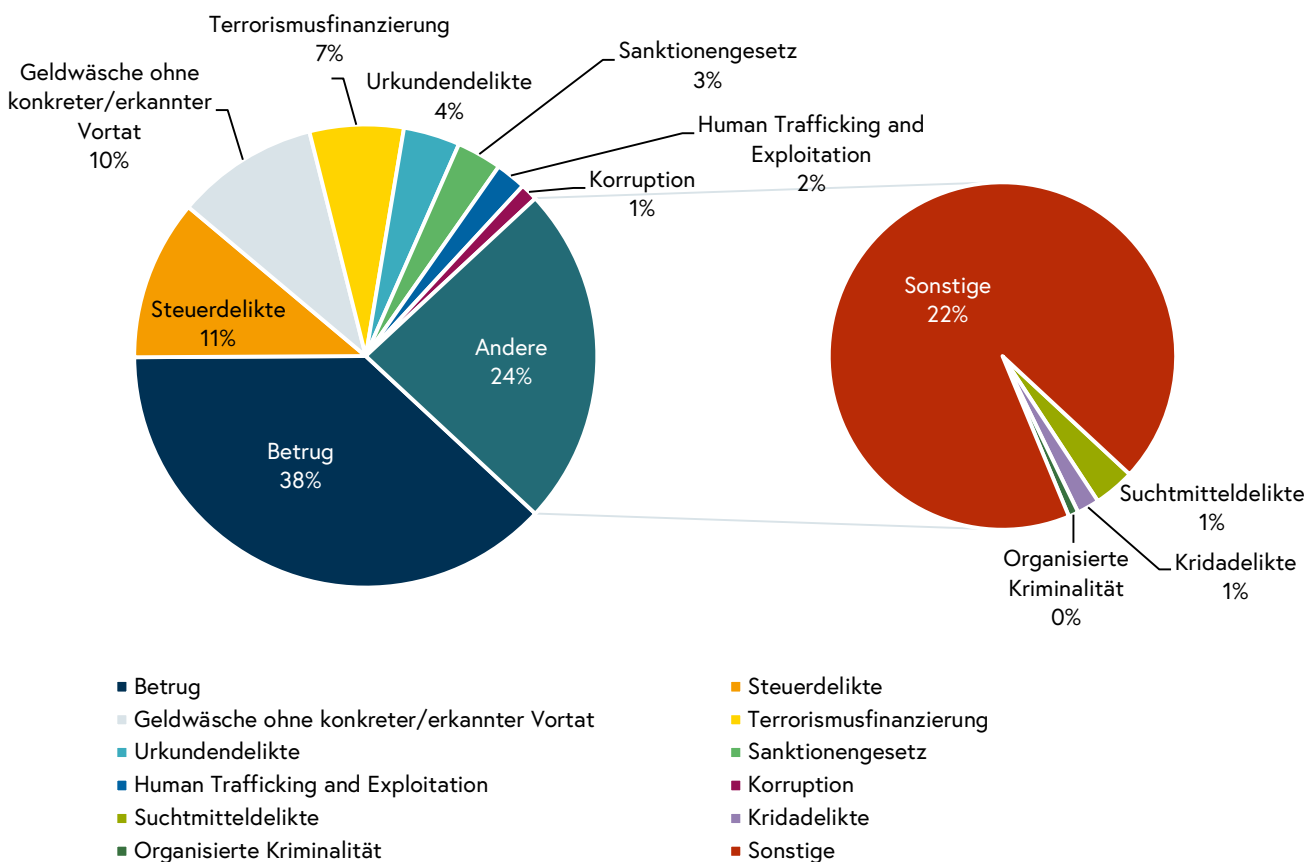


Deliktsbereiche der Verdachtsmeldungen

Die Analyse der Geldwäschemeldestelle erlaubt es, die meisten Verdachtsmeldungen bestimmten Deliktsbereichen zuzuordnen. Mit 38 Prozent der Verdachtsmeldungen dominierten nach wie vor Betrugshandlungen die festgestellten Vortaten. Die Gruppe der Meldungen basierend auf „Geldwäsche ohne konkreter/erkannter Vortat“ ging erfreulicherweise erneut auf zehn Prozent zurück.

Bei elf Prozent der Verdachtsmeldungen erkannte die A-FIU, dass die gemeldeten Sachverhalte in Zusammenhang mit Steuerdelikten stehen könnten. In sieben Prozent der Fälle lag Verdacht auf Terrorismusfinanzierung vor, während vier Prozent der Meldungen Verdachtsmomente im Zusammenhang mit Urkundendelikten berichteten. Mögliche Sanktionsverstöße konnten in drei Prozent der Verdachtsmeldungen als mögliche Vortat festgestellt werden. Zudem stellte die A-FIU in zwei Prozent der Meldungen Zusammenhänge mit Menschenhandel sowie in einem Prozent den Verdacht auf Korruptionsdelikten fest. 24 Prozent der Verdachtsmeldungen verteilen sich auf Suchtmitteldelikte, Kridadelikte und Delikte der organisierten Kriminalität.

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 Bundesministerium für Finanzen (BMF) haben bei der Wahrnehmung ihrer Aufgaben im Berichtsjahr 2024 in 18 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.

Daneben wird die A-FIU auch von anderen Behörden wie etwa der Finanzmarktaufsicht (FMA) oder der Österreichischen Nationalbank (OeNB) gemäß § 18 FM-GwG über Verdachtsfälle in Kenntnis gesetzt, wenn diesen bei der Ausübung ihrer Aufsichtstätigkeit mit Geldwäscherei oder Terrorismusfinanzierung in Zusammenhang stehende Transaktionen auffallen. Von den eben angeführten Behörden erhielt die Geldwäschemeldestelle im Berichtsjahr sieben Meldungen.

Internationale Kooperation

Die A-FIU leitete in über 900 Fällen einen internationalen Schriftverkehr ein, um nähere Informationen zu den analysierten Sachverhalten einzuholen beziehungsweise die Partnerinnen- und Partnerdienste über eigene Erkenntnisse zu informieren. Dabei wurde in diesem Berichtsjahr am häufigsten FIU.net verwendet, gefolgt von Egmont Secure Web.



Abbildung: Top 5 der Empfänger- und Senderländer im Berichtsjahr 2024

Weiterleitung von Analyseberichten

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

Von den insgesamt 11.111 im Berichtsjahr erhaltenen Verdachtsmeldungen gingen nach Durchführung des Analyseverfahrens 2.973 in Form von Analyseberichten an die Strafverfolgungsbehörden zur weiterführenden Ermittlung beziehungsweise an ausländische Partnerinnen- und Partnerdienste weiter. Das entspricht einem Anteil von 27 Prozent der eingelangten Verdachtsmeldungen. Demgegenüber steht die Differenz von 8.138 Fällen, die die A-FIU mangels Anfangsverdachts oder weiterer Analyseansätze zur passiven Folgeanalyse bei sich behält.

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 oder – mangels ausreichenden Österreichbezugs für weitere Ermittlungen – an ausländische Partnerdienste weiter. Österreich ist ein attraktiver internationaler Finanzplatz. Das verursacht auch Verdachtsfälle bei ausländischen Kundinnen und Kunden inländischer Meldeverpflichteter, die aufgrund ihrer Ortsansässigkeit in Österreich der A-FIU melden müssen. Wenn kein weiterer Anhaltspunkt für österreichische Ermittlungen besteht, die Verdachtsmomente aber ins Ausland zeigen, leitet die A-FIU diese Sachverhalte dorthin weiter. Daher werden erstmals auch die internationalen Weiterleitungen von Analyseergebnissen zur weiteren Analyse beziehungsweise zur Veranlassung eines Ermittlungsverfahrens im Ausland selbstständig angeführt. Diese Gruppe an Weiterleitungen stellt im Berichtsjahr 2024 die zahlenmäßig größte Empfängerinnen- und Empfängergruppe mit 15 Prozent dar.

Wie auch in den Vorjahren, wurden Analyseberichte häufig (sieben Prozent) an die Fachabteilungen und Büros im Bundeskriminalamt gesandt. Rund zwei Prozent der Analyseberichte gingen wegen vermutetem Steuer- oder Zollvergehens an die Abgabenbehörden des Bundes und rund zwei Prozent an die Direktion für Staatsschutz und Nachrichtendienst.

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

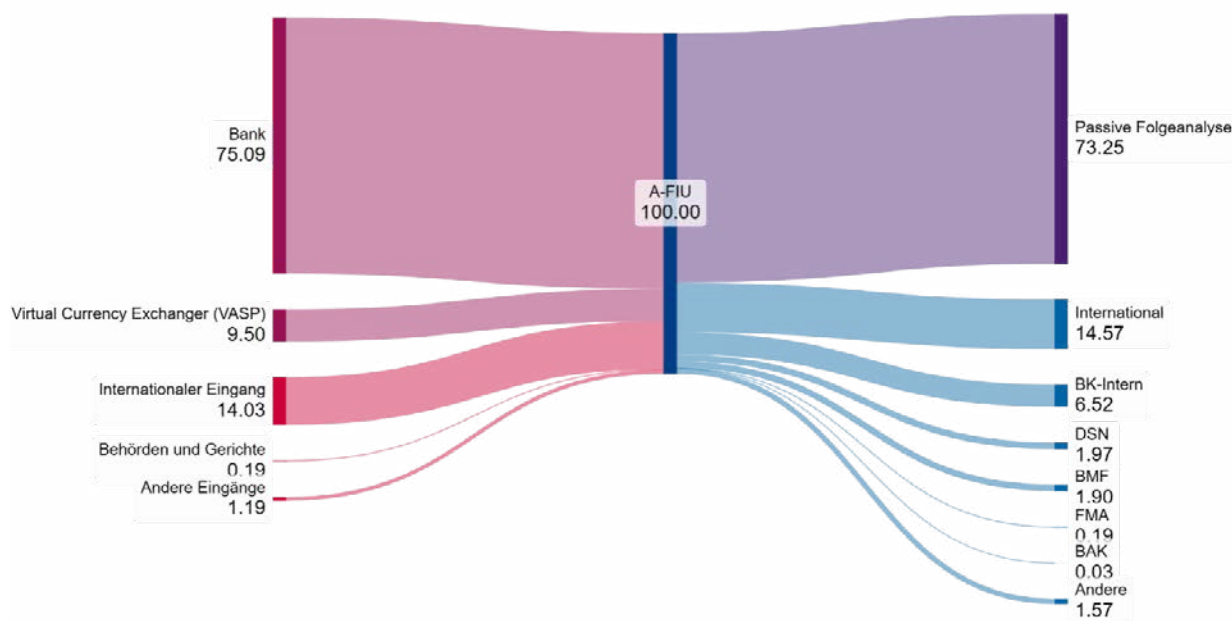


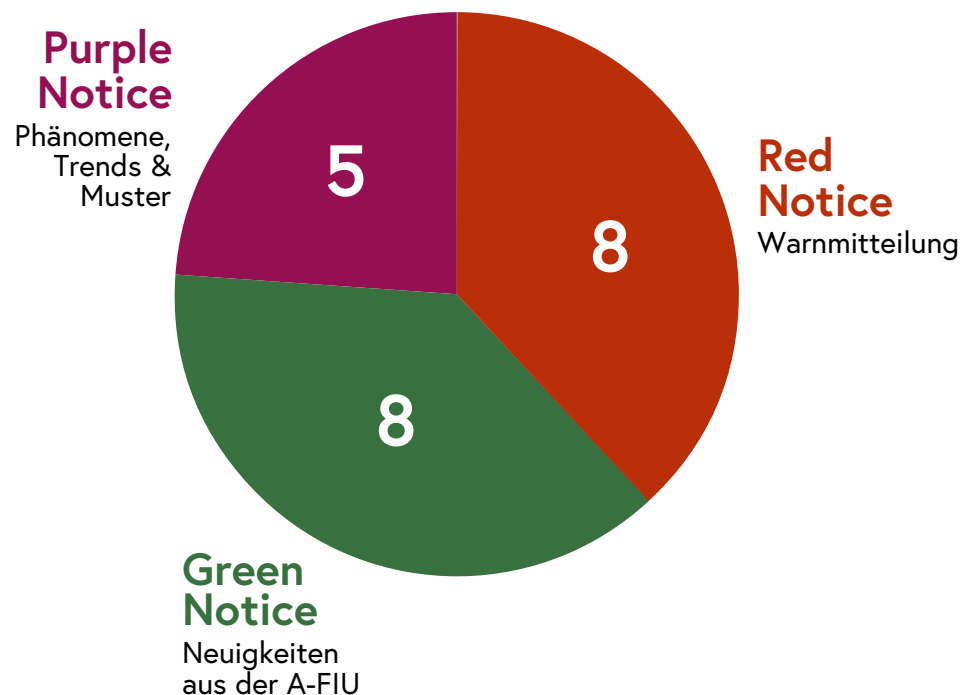
Abbildung: Ursprünge des Akteneingangs und Ziele der Analyseberichte

Auskunftsersuchen

Alle Verpflichteten haben mit der Geldwäschemeldestelle zusammenzuarbeiten und ihr auf Verlangen – ungeachtet einer zuvor erstatteten Verdachtsmeldung – alle erforderlichen Auskünfte zu erteilen, die ihr zur Verhinderung oder zur Verfolgung von Geldwäscherei oder von Terrorismusfinanzierung erforderlich scheinen. Von ihrem Recht derartige Auskünfte von den meldeverpflichteten Berufsgruppen zu verlangen, machte die A-FIU im Berichtsjahr 370 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 der Geldwäsche. Entsprechend ihrem gesetzlichen Auftrag teilt die A-FIU ihr so gewonnenes Wissen mit den Meldeverpflichteten. Die regelmäßig veröffentlichten Notices 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. Neben der laufenden Information zu allgemeinen Phänomenen, Mustern und Trends sowie hilfreiche Informationen für Verpflichtete in den Purple Notices der A-FIU, bietet die Red Notice die Möglichkeit, alle relevanten Sektoren mit personenbezogenen Daten zu einem der A-FIU konkret vorliegenden Modus Operandi zu versorgen und so im Umkehrschluss wichtige Hinweise für die Analyse und in weiterer Folge Ermittlungstätigkeit der Behörden zu generieren.



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.

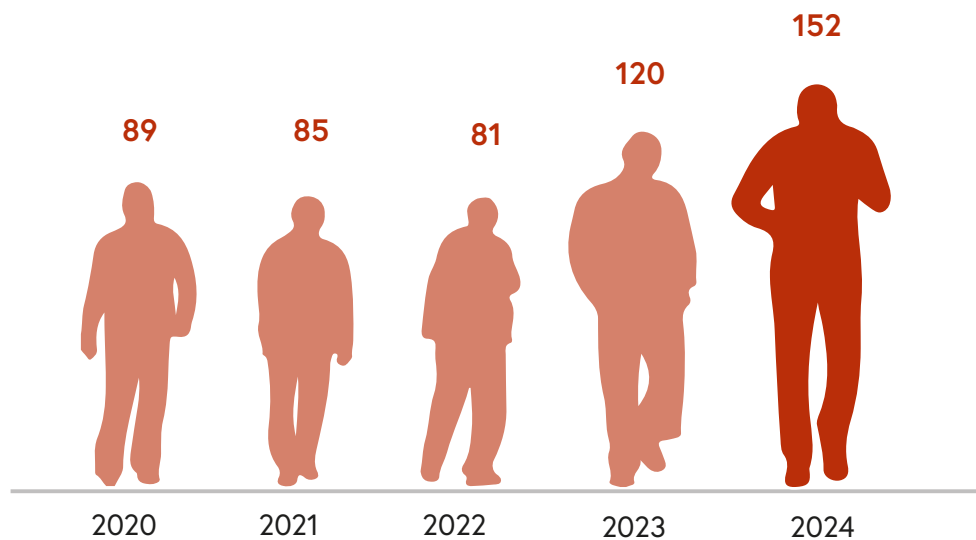
In der Praxis jedoch steht die A-FIU als Teil der Sicherheitsbehörden in direktem Kontakt mit den Staatsanwaltschaften, die über die dauerhafte Beschlagnahme der bedenklichen Vermögenswerte zu entscheiden haben. Wenn die Geldwäschemeldestelle eine Transaktionssperre für notwendig erachtet, regt sie diese 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 Rechtsschutz für die Betroffenen. In Fällen vermuteter Abgabenhinterziehung regt die Geldwäschemeldestelle Sicherungsmaßnahmen bei den Abgabenbehörden des Bundes an.

Die Geldwäschemeldestelle hat 2024 zahlreiche vermögensrechtliche Anordnungen angeregt. Diese dienten der Sicherstellung von verdächtigen Vermögenswerten. Der Gesamtwert dieser Vermögenswerte belief sich im Jahr 2024 auf rund 20 Millionen Euro. Die im Berichtsjahr weiter ausgebaut Zusammenarbeit zwischen der A-FIU, Kriminalpolizei, Staatsanwaltschaften und Abgabenbehörden sowie der exzellenten Mitwirkung der Verpflichteten führte dazu, dass in den meisten Fällen rasche Sicherungsmaßnahmen erwirkt, werden konnten.

Verurteilungssstatistik

Der Analysebericht der A-FIU, der Informationen über die zugrundeliegende Verdachtsmeldung, über kriminalpolizeiliche Daten, Finanzdaten und Ergebnisse des internationalen Informationsaustauschs beinhaltet, wird an die zuständigen Stellen übermittelt, was das kriminalpolizeiliche Ermittlungsverfahren oft erst auslöst. Das Verfahren beschränkt sich nicht bloß auf Geldwäscherei oder Terrorismusfinanzierung, weshalb die Analyseberichte häufig ausschlaggebend für Verurteilungen anderer Straftaten, wie etwa den Vortaten, sind.

2024 gab es 152 rechtskräftige Verurteilungen wegen Geldwäscherei zu verzeichnen, das entspricht einem Anstieg von rund 27 Prozent im Vergleich zum Vorjahr.



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

Phänomene, Muster und Trends

Neben andauernden internationalen Konflikten und den Sanktionspaketen der Europäischen Union, beschäftigte auch das Verschieben von verdächtigen Geldmitteln aus der Ukraine nach Österreich im Berichtsjahr 2024 immer noch die A-FIU. Zudem konnte die Gründung und Nutzung von Vereinen zu vermeintlichen Geldwäschezwecken festgestellt und analysiert werden. Daneben war die Etablierung bereits bestehender technischer Trends und das Hinzukommen neuer Produkte auf dem Markt besonders bemerkbar und zeichnete sich auch aufgrund der eingehenden Verdachtsfälle ab. Diese Entwicklungen erleichtern es Kriminellen, inkriminierte Gelder schnell, anonym und kontaktlos zu transferieren und erschweren die Rückverfolgbarkeit der Geldflüsse immer mehr.

Die folgenden Beispiele zeigen, wie die technologischen Weiterentwicklungen im Zahlungsverkehr aber auch andere bereits lang bestehende Methoden wiederentdeckt und genutzt werden, um inkriminierte Gelder zu waschen.

Identitätsdiebstahl und Gelwäsche über Online-Konten

Die A-FIU berichtet über ein zunehmendes Phänomen im Bereich der Online-Kriminalität: die Eröffnung von Bankkonten unter Verwendung gefälschter Ausweisdokumente. Dabei steht insbesondere die Nutzung sogenannter Fake-IDs im Fokus, welche durch qualifizierte elektronische Signaturen oder Ein-Cent-Legitimationsverfahren (Referenzzahlung) zur Identitätsbestätigung eingesetzt werden. Die Täterinnen- und Tätergruppen verwenden gefälschte Ausweise, die auf die Personendaten real existierender, unbeteiligter Personen ausgestellt sind – Identitätsdiebstahl. Als Adressen auf den gefälschten Dokumenten werden häufig Arztpraxen, Geschäftslokale oder ähnliche Einrichtungen angegeben. Es handelt sich dabei um österreichische Reisepässe oder Dienstpässe. Einer konkreten Täterinnen- und Tätergruppe konnten zunächst zehn gefälschte Identitäten zugeordnet werden, wobei von einer weit höheren Dunkelziffer ausgegangen wird. Insgesamt wurden 38 Bankkonten festgestellt, die auf diesem Wege eröffnet wurden. Hierbei betroffen waren drei Banken, wobei 21 Konten allein bei einem Institut lagen. Die Konten wurden einerseits genutzt, um weitere Konten mittels der Ein-Cent-Legitimation zu eröffnen und andererseits wurden sie zum Empfang und Weitertransfer von Betrugsgeldern verwendet, die im nahen Ausland bar behoben wurden. In diesem Zusammenhang musste die A-FIU feststellen, dass teilweise die echten Personen bereits Konten bei den betroffenen Banken unter demselben Namen hatten. Hier bietet die derzeitige gesetzliche Möglichkeit zur Auslagerung der dafür notwendigen Fernidentifikation viel Spielraum im Bereich der

Auslegung. Es gibt eine Vielzahl an unterschiedlichen Anbieterinnen und Anbietern, die wiederum unterschiedliche Produktpakete offerieren. Die Divergenz zwischen der Qualität dieser ist nach Auffassung und Feststellung der A-FIU enorm.

Die Geldwäschemeldestelle verfasste mehrere Red Notices, um die Banken vor den falschen Identitäten zu warnen, sowie eine Purple Notice, um generell auf dieses Phänomen aufmerksam zu machen. Die A-FIU arbeitet diesbezüglich in enger Abstimmung mit der FMA zusammen.

Wird ein Identitätsdiebstahl nicht sofort erkannt, kann das für die betroffenen Personen massive Auswirkungen haben, die bis zu strafrechtlichen Ermittlungen und deren Folgen führen können. Im Falle von Kontosperren oder Rückforderungen erleiden die Opfer finanzielle Schäden. Außerdem kann es zu Kreditschädigung kommen, wenn die Opfer negative Einträge in Schuldnerregistern erhalten.

Die Nutzung gefälschter Ausweise zur Online-Identifikation sowie die Möglichkeit der Ein-Cent-Legitimation stellen erhebliche Bedrohungen für Banken, die Finanzmarktstabilität und betroffene Personen dar. Eine enge Zusammenarbeit zwischen Finanzinstituten, Behörden und der A-FIU ist essenziell, um diese Form der digitalen Kriminalität zu bekämpfen und künftige Schäden zu minimieren.

Missbräuchliche Gründung von Vereinen

Im vergangenen Jahr häufte sich ein bis dato unbekanntes Phänomen in Österreich – die Gründung von Vereinen durch ausländische Staatsbürgerinnen und Staatsbürger zu Zwecken der vermeintlichen Geldwäsche.

Hier war die Häufung von Vereinen an bestimmten Adressen auffallend. Teilweise konnten mehrere hundert Vereine an einer Adresse festgestellt werden. Zudem waren die Vereinsnamen durch unlogische, sehr lange (über mehrere Zeilen) und nichtssagende Namen vor allem im Bildungs- beziehungsweise Esoterikbereich gekennzeichnet.

Warum beschäftigte dieser Umstand die A-FIU?

Zum einen aufgrund der auffälligen Häufung von hunderten Vereinen mit ausländischen Staatsbürgerinnen und Staatsbürgern als Organe der Vereine an wenigen Adressen. Zum anderen waren auffällige Finanzflüsse der Vereine feststellbar, die den Verdacht der Geldwäsche stützten. Durch die Analyse der Finanzströme konnten folgende Besonderheiten festgestellt werden: Am Vereinskonto waren keine für einen Vereinsbetrieb übliche Zahlungen wie beispielsweise Mitgliedsbeiträge festzustellen. Daneben gingen hohe fünfstellige Summen aus dem Ausland von dortigen GmbHs auf den Vereinskonto ein.

Diese Gelder wurden dann innerhalb kurzer Zeit wiederum auf das Konto einer anderen zweiten ausländischen GmbH und teilweise auf die Privatkonten der Vereinsorgane weitertransferiert. Dieser Vorgang war Anlassfall einer tiefgreifenden Analyse dieses Phänomens, insbesondere aufgrund der hohen Geldbewegungen. Das Phänomen wurde hinsichtlich seiner Anwendbarkeit auf andere Vereinskonstrukte hin überprüft.

Im Zuge dessen wurde auch mit der für das WiEReG zuständigen Behörde im BMF zusammengearbeitet und eine Reihe von verdächtigen Vereinen identifiziert. Unter Einbeziehung ausländischer FIUs konnten konkrete Straftaten der Vereinsorgane im Ausland als Vortat festgestellt beziehungsweise in Verbindung gebracht werden. In diesen Fällen bestätigte sich das angenommene Phänomen der Geldwäsche durch Vereinskonstrukte in Österreich.

Vereine können in Österreich sehr einfach und schnell gegründet werden. Nach Eintragung des Vereins im Vereinsregister kann ein Vereinskonto eröffnet werden. Damit verbunden sind wesentlich höhere Schwellen im Transaktionsmonitoring als bei Privatkonten, was solche Konten für Kriminelle dementsprechend interessant macht.

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 rasch an ihr Vermögen. Die Auszahlung durch ein Versicherungsunternehmen vermittelt zudem 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 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, 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.

Echtzeitüberweisungen

Die A-FIU verzeichnete vermehrt den Trend, insbesondere im Zusammenhang mit der Vortat Betrug, aber auch zu Zwecken der Geldwäsche, dass Echtzeitüberweisungen („Instant Payments“) von Kriminellen verstärkt genutzt werden. Die Echtzeitüberweisung an sich stellt ein erhöhtes Risiko für Geldwäsche dar, weil damit in wenigen Sekunden eine Transaktion durchgeführt werden kann. Man denke nun an eine Kette solcher Transaktionen, die es den Behörden damit massiv erschweren Gelder am Ende der Kette festzustellen und allenfalls noch zu sichern. Die Entscheidung der EU, ab Januar 2025 die Nutzung der Echtzeitüberweisungen kostenlos zu machen, wird das Verwenden dieses Produktes noch attraktiver machen und damit auch die Nutzung für illegale Zwecke. Das konnte bereits in einer Vielzahl von Fällen festgestellt werden. Durch ihre Vorteile im Zusammenhang mit der Geschwindigkeit von Transaktionen, ist die Echtzeitüberweisung ein Phänomen, das die A-FIU und die Ermittlerinnen sowie Ermittler in den nächsten Jahren stark beschäftigen wird.

Kryptowährungen

Der Aufwärtstrend bei Kryptowährungen hält weiterhin an. Zum Jahresende 2024 verzeichneten mehrere Kryptowährungen, darunter der Bitcoin, einen deutlichen Wertzuwachs. Diese Entwicklung zieht erfahrungsgemäß nicht nur Investorinnen und Investoren, sondern auch Kriminelle an. Wenig verwunderlich ist daher, dass auch im Cybercrime Report 2024 des Unternehmens Chainalysis darauf hingewiesen wird, dass 2024 ein Rekordjahr für sogenannte illicit actors – also Akteurinnen und Akteure, die ihre Dienste kriminellen Organisationen zur Geldwäsche anbieten – gewesen sein dürfte.

Zwar zielen Verordnungen wie die Markets in Crypto-Assets Regulation (MiCAR) und die Transfer of Funds Regulation (ToFR, auch bekannt als Geldtransferverordnung) speziell auf europäischer Ebene darauf ab, genau solche Dienstleisterinnen und Dienstleister stärker zu regulieren, doch die praktische Umsetzung bleibt herausfordernd. Obwohl durch diese Verordnungen sowohl die Prüfpflichten als auch der Kryptosektor insgesamt

strenger reguliert werden, stellt die Analyse von Transaktionen – sowohl on-chain als auch off-chain – die zuständigen Behörden weiterhin vor erhebliche Herausforderungen.

On-Chain versus Off-Chain

Unter On-Chain-Transaktionen werden sämtliche Transaktionen verstanden, die direkt auf der Blockchain stattfinden und somit öffentlich, transparent und in Echtzeit nachvollziehbar sind. Im Gegensatz dazu stehen die kostengünstigeren Off-Chain-Transaktionen, die außerhalb der eigentlichen Blockchain abgewickelt werden, wie etwa über CEX (zentralisierte Börsen), Peer-to-Peer Transaktionen oder Layer-2-Lösungen.

Die Herausforderung für Behörden und Verpflichtete liegt darin, dass On-Chain-Daten zwar grundsätzlich zugänglich sind, jedoch meist eine aufwändige und fachlich anspruchsvolle Analyse erfordern – etwa zur Verknüpfung von Wallet-Adressen mit realen Personen oder Organisationen. Off-Chain-Transaktionen hingegen entziehen sich vielfach dieser Transparenz, da sie außerhalb der Blockchain stattfinden und man daher auf interne Systeme der Anbieterinnen und Anbieter angewiesen ist.

Dies spielt eine wichtige Rolle in der durch die ToFR strenger regulierte Prüfungspflicht der Mittelherkunft, da die Überprüfung der Angaben zur Herkunft der eingesetzten Mittel eine solche fachlich anspruchsvolle Analyse erfordert.

Bridge

Unter Blockchain-Bridges versteht man technische Infrastrukturen, die den Transfer von Kryptowährungen zwischen unterschiedlichen Blockchain-Netzwerken ermöglichen. Da Blockchains in der Regel nicht direkt miteinander kommunizieren können, dienen Bridges als vermittelnde Instanzen, die Vermögenswerte auf der Quell-Blockchain sperren (locken) oder verbrennen (burn) und auf der Ziel-Blockchain abbilden (minten) können.

In der Praxis bedeutet dies, dass ein Token – beispielsweise USDT auf der Ethereum-Blockchain – über eine Bridge auf ein anderes Netzwerk, wie die BNB Chain übertragen werden kann, ohne dass der Token physisch „wandert“. Stattdessen wird der Vermögenswert auf der Ausgangs-Chain eingefroren und auf der Ziel-Chain in Form eines entsprechenden Tokens (zum Beispiel Wrapped USDT) neu ausgegeben.

Insbesondere im Zusammenhang mit betrügerischen Aktivitäten wurde diese Vorgehensweise im Jahr 2024 bei Analysen vermehrt festgestellt. Dabei wurden Vermögenswerte nicht nur über eine, sondern gezielt über mehrere Bridges transferiert, um die Nachverfolgbarkeit zu erschweren und die Herkunft der Mittel zu verschleiern.

P2P-Plattformen versus E2EE-Kommunikationsplattformen

Unter Peer-to-Peer(P2P)-Plattformen versteht man digitale Marktplätze beziehungsweise Netzwerke, auf denen Nutzerinnen und Nutzer (Peers) direkt miteinander handeln und

Dienste austauschen können. Ein Blick in den aktuellen IOCTA-Bericht (Internet Organised Crime Threat Assessment) von Europol zeigt, dass solche Plattformen zunehmend durch Messenger-Dienste mit End-to-End-Encryption (E2EE) verdrängt werden. Diese bieten kriminellen Gruppierungen die Möglichkeit, sich der Einhaltung von gesetzlichen Vorgaben gezielt zu entziehen, da Kommunikationsinhalte weder von Anbieterinnen und Anbietern noch von Strafverfolgungsbehörden eingesehen werden können.

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 künstlicher Intelligenz nutzt, wird zur Herstellung von Fälschungen aller Art genutzt. Solche Fälschungen zu erkennen ist ohne technische Expertise beziehungsweise Verifizierungssysteme oft nicht mehr möglich, weil die Qualität dieser Fälschungen sehr hoch ist. Das bedeutet, dass diese Technologie unter anderem bei Online-Identifikationsverfahren für Missbrauch angewendet wird und zu erheblichen Schäden oder Mehraufwand führen kann.

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, Transaktion durchzuführen. Bereits drei Sekunden einer 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 Alltäglichkeiten auf diversen Plattformen, ist es keine große Herausforderung, an Stimmbeispiele vieler Menschen zu gelangen. Gerade in großen Unternehmen, in denen wegen langer Hierarchieketten eine gewisse Anonymität herrscht, können Kriminelle erheblichen monetären und reputierlichen Schaden anrichten.

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 und 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 die A-FIU zur Prävention und Bekämpfung von Geldwäsche und Terrorismusfinanzierung den Aufsichtsbehörden, gegebenenfalls Verpflichteten und erforderlichenfalls den Strafverfolgungsbehörden weiter.

Betrachtung von Überwachungssystemen im Geldautomatenbetrieb

Im Jahr 2024 stand in der A-FIU ein Fall im Fokus, der die internationale Verflechtung der Geldwäsche verdeutlicht. Im Rahmen der Analyse stellte die A-FIU fest, dass rund 150 Personen (ausschließlich Nicht-EU-Bürgerinnen und -Bürger) über einen mehrjährigen Zeitraum Bargelderläge in einem dreistelligen Millionenbereich durchführten. Die internationale Dimension dieses Falls wird besonders deutlich, da Gelder in mehr als 30 verschiedene Empfängerstaaten transferiert wurden. Dies gelang durch gezielte Ausnutzung eines bestimmten Bankenprodukts und der damit verbundenen beschränkten Monitoringmöglichkeit der Banken.

Die komplexe Finanzstromanalyse ergab, dass zahlreiche Personen durchschnittliche monatliche Bargeldeinzahlungen von bis zu 550.000 Euro vornahmen, welche in einem erheblichen Missverhältnis zu ihren deklarierten legalen Einkommensquellen standen. Darüber hinaus konnten mehrere geldwäscherelevante Vortaten identifiziert werden. Aufgrund dieser und weiterer Erkenntnisse entstanden zahlreiche kriminalpolizeiliche Anfangsverdachtsmomente, weshalb der Sachverhalt den zuständigen Strafverfolgungsbehörden übermittelt wurde.

Im kooperativen Zusammenwirken mit dem Finanzsektor und der Finanzmarktaufsicht gelang es, die Monitoringsysteme für diese Art von Phänomenen zu sensibilisieren und entsprechende Erkennungsverfahren zu optimieren. Das angeführte Produkt wurde zudem in der vorhandenen Art und Weise eingestellt.

Phishing-Phänomen „FinLink“

Auch im Jahr 2024 konnte zu Jahresbeginn durch die A-FIU eine Zunahme von Phishing-Aktivitäten beobachtet werden, bei denen sich Cyberkriminelle als österreichische Finanzverwaltung ausgaben. Kriminelle haben gefälschte SMS- und E-Mail-Nachrichten im Namen von FinanzOnline und anderen offiziellen Stellen versendet, um Bürgerinnen und Bürger zur Preisgabe persönlicher Daten zu verleiten. Die betrügerischen Nachrichten enthielten Links zu nachgeahmten Webseiten im Design von FinanzOnline und Oesterreich.gv.at, die zur Eingabe von Zugangsdaten und anderen sensiblen Informationen aufforderten.

Im Frühjahr 2024 stellte die A-FIU ein weiteres Phishing-Phänomen im Zusammenhang mit Online-Banking fest, bei dem Kriminelle gefälschte Banking-Links prominent in Suchmaschinen platzierten. Opfer, die sich in ihr Online-Banking einloggen wollten, gaben entsprechende Begriffe ihrer Bank bei Suchmaschinen ein und klickten unbedacht auf manipulierte Ergebnislinks. Diese führten zu fingierten Login-Seiten, über die die Täterinnen- und Täterschaft die Zugangsdaten der Kundinnen und Kunden abfangen konnte. In beiden Fällen hat die A-FIU aufgrund der Relevanz für den Finanzsektor entsprechende „Notices“ an die meldepflichtigen Berufsgruppen übermittelt und gemeinsam mit Stakeholdern auf dieses Phänomen hingewiesen sowie Präventionsarbeit geleistet, sodass höhere Schäden verhindert werden konnten.

Krypto-Anlagebetrug EXW

Im Jahresbericht 2023 wurde erstmals über den groß angelegten Betrugsfall rund um die vermeintliche Krypto-Handelsplattform EXW berichtet. Im Zentrum stand ein Verfahren von erheblicher Dimension, in dem elf Personen unter anderem wegen gewerbsmäßigen schweren Betrugs, Geldwäscherei, Beteiligung an einem Pyramidenspiel sowie wegen Bildung einer kriminellen Vereinigung angeklagt wurden. Die Beschuldigten sollen rund 40.000 Anlegerinnen und Anleger zur Investition in die eigens geschaffene Kryptowährung „EXW-Token“ bewegt und dabei einen Schaden von mindestens 17,6 Millionen Euro verursacht haben. Die Einlagen – meist in Form von Kryptowährungen oder Bargeld – wurden den Ermittlungen zufolge jedoch nicht investiert, sondern über verschiedene Wallets und Konten weitergeleitet, um letztlich private Ausgaben im luxuriösen Stil zu finanzieren.

Im Berichtsjahr 2024 kam es zu weiteren, entscheidenden Verfahrensfortschritten: Nach Anklageerhebung im Juni 2023 gegen zunächst acht, letztlich elf, Personen, begann im September 2023 der Strafprozess am Landesgericht Klagenfurt. Im Zentrum der Anklage standen irreführende Investitionsversprechen in Immobilienprojekte und Kryptowährungsgeschäfte – ohne dass tatsächliche Investitionen erfolgt wären.

Im Oktober 2024 wurden die Urteile gesprochen: Fünf Angeklagte wurden freigesprochen, fünf weitere erhielten Freiheitsstrafen zwischen 18 Monaten bedingt und fünf Jahren unbedingt. Gegen mehrere Entscheidungen wurden Rechtsmittel erhoben. Das Verfahren gegen einen Angeklagten wurde ausgedient. Mit Stand Ende 2024 sind vier Freisprüche und ein Schuldspruch rechtskräftig. Der von der Staatsanwaltschaft bezifferte Gesamtschaden beträgt rund 20 Millionen Euro – eine Zeugin nannte im Verfahren sogar einen möglichen Gesamtschaden von bis zu 120 Millionen Euro. Die Zahl der Geschädigten wird weiterhin auf mindestens 40.000 Personen geschätzt. Es gilt die Unschuldsvermutung.

Der Fall EXW markiert den ersten großflächigen Anlagebetrug mit Kryptowährungsbezug seit der Reorganisation der A-FIU. Mitunter den Ausgangspunkt für die kriminalpolizeilichen Ermittlungen bildeten die umfangreichen Finanzstromanalysen der A-FIU. Bereits vor Einleitung des Ermittlungsverfahrens konnten auf diesem Weg wesentliche Verdachtsmomente identifiziert werden. Diese Analyseergebnisse gaben entscheidende Impulse für das weitere Vorgehen der Strafverfolgungsbehörden und legten die Grundlage für die behördenübergreifende Zusammenarbeit mit den Aufsichts- und Finanzbehörden. Darüber hinaus stellte die A-FIU der Kriminalpolizei eine Vielzahl aufbereiteter Finanzinformationen zur Verfügung, die für die weiteren Ermittlungsschritte von zentraler Bedeutung waren.

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 potenziellen 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 jedoch auch 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 Vorfällen zur Geldwäsche einnehmen, hat das Büro für Betrugsermittlungen im Bundeskriminalamt 2022 ein Lagebild zum Betrug aufgebaut. Dieses gibt tagesaktuell Auskunft über die österreichweite Betrugslage sowie über regionale Häufungen von Betrugsanzeigen und hat sich wiederholt als Frühwarnsystem bewährt, das neueste Betrugsmaschen frühzeitig aufdeckt, und unterstützt bei der Steuerung bundesweiter Schwerpunktaktionen.

Anrufbetrug

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

Falsche Polizistinnen und Polizisten

Durch die Installation der Ermittlungsgruppe Falsche Polizisten, die bundesweit proaktiv operiert, konnten die Fallzahlen als auch die Schadenssummen im Jahr 2024 – verglichen zum Vorjahr – um mehr als die Hälfte reduziert werden.

Bei diesem Modus rufen Kriminelle 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.

Bei einer anderen Variante behaupten die falschen Polizistinnen und 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 Kriminelle in die Rolle von Bankangestellten. Sie sähen das Misstrauen gegenüber der Bank des Opfers mit der Begründung, dass korrupte Bankmitarbeiterinnen und Bankmitarbeiter die Schließfächer der Kundschaft heimlich ausräumen würden.

2024 trat kurzzeitig ein neuer Modus hierzu in Erscheinung, bei welchem Kriminelle behaupteten, ein naher Angehöriger wäre in einen Unfall verwickelt, wodurch dieser eine dringende Operation beziehungsweise kostspielige Medikamente benötige. Sie gaben in weiterer Folge vor, dass die medizinische Versorgung nur durch Bezahlung eines hohen Betrags gewährleistet werden könne. Zum Schaden kommt es in den meisten Fällen durch die Übergabe von Bargeld an einen Kriminellen.

Tochter-Sohn-Modus

Im Vergleich zum Jahr 2023 konnte bei diesem Betrugsmodus 2024 ein Rückgang registriert werden, der sich gegen Jahresende nochmals verschärfte.

Kriminelle verschicken massenweise SMS und 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 sie – wieder per Textnachricht – vor, dringend Geld zu benötigen, meist wegen angeblicher Spontangebühren oder wegen Notfällen. Zahlungsempfängerinnen und -empfänger sind oftmals ausländische Konten. Im Glauben, der Tochter oder dem Sohn etwas Gutes zu tun, überweisen die Geschädigten via Sofortüberweisung den geforderten Geldbetrag.

Falsche Bankmitarbeiterinnen und Bankmitarbeiter

Bei der Weiterentwicklung dieser 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 die Opfer die Legitimation für das Online-Banking verlängern müssten. In weiterer Folge werden diese 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 Täterinnen- und Täterschaft mit gefälschten Telefonnummern an und angebliche Bankbedienstete melden sich, um so Vertrauen aufzubauen. Die Opfer werden aufgefordert, Überweisungen zu bestätigen beziehungsweise freizugeben. Da es sich vorrangig um Echtzeitüberweisungen handelt, besteht nur eine geringe Wahrscheinlichkeit, die Geldbestände durch die Banken oder die Behörden wiederzuerlangen.

Tech-Support-Scam

Im Jahr 2024 etablierte sich zunehmend der sogenannte Tech-Support-Scam (falsche Software-Mitarbeiterinnen und -Mitarbeiter). Dabei kontaktieren angebliche Mitarbeiterinnen und Mitarbeiter von namhaften Software- sowie Retail-Unternehmen die Geschädigten via Telefon und versuchen auf diesem Weg, unter Vorspiegelung falscher Tatsachen, die späteren Opfer zu Geldüberweisungen zu drängen, eine Schadsoftware herunterzuladen (Phishing) oder eine Fernwartungssoftware zu installieren (Ausspähen von sensiblen Daten).

Bei diesen Scheintatsachen handelt es sich um angebliche Fremdzugriffe auf Benutzerinnen- bzw. Benutzerkonten der Geschädigten, sodass spezielle Sicherheitsupdates im virtuellen Beisein der angeblichen Mitarbeiterin bzw. des angeblichen Mitarbeiters durchgeführt werden müssten oder dass es zum Beispiel zu einer Fehlbuchung gekommen wäre und die bzw. der Betroffene nun eine angebliche Gutschrift erhalten solle (Bekanntgabe von Bankdaten).

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 Kriminelle Waren im Internet mit dem Vorsatz, diese nach Erhalt nicht zu bezahlen. Warenbetrug bedeutet, dass Kriminelle Waren mit dem Ziel anbieten, ihre Opfer zu einer Bezahlung zu bringen, ohne die versprochene Ware jemals zu liefern, oder anstatt der eigentlich bestellten Ware eine qualitativ minderwertigere Ware zu versenden.

Bestellung auf fremden Namen

Diese Begehungsform definiert sich dadurch, dass Kriminelle frei erfundene oder 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 erhalten im Nachgang die unwissenden Opfer, deren Identität missbraucht wurde.

Warenbetrug bei Kleinanzeigenplattformen

Kriminelle geben sich als Privatpersonen aus und bieten auf Kleinanzeigenplattformen Waren zum scheinbaren Verkauf an. In weiterer Folge überweisen die Opfer den vereinbarten Kaufpreis, ohne jemals eine Ware zu erhalten.

Versand minderwertiger Waren

Hierbei bestellen die Geschädigten eine (meist) hochpreisige Ware im Internet. Von den Kriminellen wird jedoch nicht das eigentliche bestellte Produkt versendet, sondern etwas gänzlich Anderes oder ein Fakeprodukt, welches dem Wert des bezahlten Kaufpreises nicht entspricht.

Fakeshops

Die Opfer werden zunächst zufällig auf Werbeanzeigen im Internet aufmerksam oder suchen gezielt nach einem bestimmten Produkt. Dadurch locken Kriminelle die Geschädigten auf Onlineshops von täuschend echt wirkenden Firmen, bei welchen die Produkte zu einem unterdurchschnittlichen Preis offeriert werden. Die Geschädigten bestellen dort das gewünschte Produkt und überweisen den Kaufbetrag im Vorhinein. Ein Warenversand tritt jedoch nicht ein oder es werden Pakete mit wertlosem Inhalt versendet.

Cyber-Trading-Fraud

Bei der Betrugsform Cyber-Trading-Fraud (CTF) handelt es sich um ein Phänomen innerhalb der Betrugsdelikte, welches zwar von der Quantität nicht zu den führenden Anzeigen zählt, in Österreich 2024 jedoch den größten finanziellen Schaden verursacht hat.

Oftmals suchen Opfer selbst im Internet aktiv nach Investmentmöglichkeiten und stoßen dabei auf von den Tätern generierte Werbeschaltungen auf diversen Social-Media-Plattformen.

Zwischen folgenden Formen der Erstanbahnung kann unterschieden werden:

- Hochprofessionelle und echt wirkende Internetauftritte von Investitionsplattformen, auf die die Opfer nach eigener Suche stoßen
- Werbung auf Internetseiten und in Printmedien
- Ungefragte Anrufe von „Investmentspezialistinnen bzw. -spezialisten“
- Empfehlungen durch Dating-App-Kontakte („Pig Butchering“)

Die Opfer erhalten meist Telefonanrufe, nachdem sie ihre Kontaktdaten bekanntgegeben haben. Die Kriminellen eröffnen dann ein vermeintliches Tradingkonto für die Opfer, oftmals unter der Bedingung, dass ein niedriger Betrag als Erstinvestment eingezahlt werden muss. Das Portfolio entwickelt sich zunächst vermeintlich prächtig und die Opfer erzielen scheinbar gute Gewinne. In der ersten Phase werden diese sogar teilweise an die Opfer ausbezahlt, um ein Vertrauensverhältnis aufzubauen und zu höheren Folgeinvestments zu animieren.

Gelingt dies, zeigt das Tradingkonto rasch erneut enorme Gewinne an. Eine Auszahlung der Gewinne erfolgt jedoch nicht, da diese Gelder in der Realität nie veranlagt werden, sondern sofort an komplexe Geldwäschenetze weitertransferiert werden. Vielmehr werden weitere Forderungen gestellt, um zu einer etwaigen Auszahlung zu gelangen (Steuern, Notariatskosten et cetera).

Die Kriminellen setzen meist eine Fernwartungssoftware ein, um selbst auf die PCs der Geschädigten zugreifen zu können, mit dem Ziel, möglichst viele Informationen des Gegenübers in Erfahrung zu bringen. In diesem Zusammenhang werden in der Regel Kryptowährungen zur Verschleierung der Geldflüsse von den Kriminellen verwendet.

Oftmals werden die Geschädigten nach einiger Zeit erneut von vermeintlichen Institutionen kontaktiert, welche vorgeben, die verloren geglaubte Investition wieder retour überweisen zu können. Geschädigte bezahlen abermals an diese Täterinnen- und Täterschaft, eine Rückbuchung erfolgt nicht (Recovery-Scam).

Pig-Butchering

Dies Form des Betrugs verursacht bundesweit einen enorm hohen finanziellen Schaden und kombiniert den klassischen Romance-Scam (Vorauszahlungsbetrug) mit dem zuvor erwähnten Cyber-Trading-Fraud. Die Anbahnung der Kriminellen zu den Opfern erfolgt vorrangig über Dating-Plattformen sowie Social-Media-Plattformen.

Nachdem das Vertrauen der Opfer erschlichen wurde, beginnen sie damit, das Interesse des Opfers auf ein vermeintlich lukratives Investitionsmodell zu lenken, welches in Wirklichkeit wiederum ein Anlagebetrugsvehikel ist (siehe CTF).

CEO-Fraud und Business E-Mail Compromise

Beim CEO-Fraud handelt es sich um eine Form des Betrugs, bei der gefälschte E-Mails an Firmen verschickt werden. Diese stammen scheinbar von Mitgliedern der Geschäftsführung des Unternehmens. Im E-Mail fordern die vermeintlichen Geschäftsführenden von der Buchhaltung die dringliche Überweisung hoher Geldbeträge an angebliche Partnerinnen- und Partnerfirmen mit ausländischen Bankverbindungen und ersuchen die Beteiligten um absolute Verschwiegenheit. Nach der ersten schriftlichen Kontaktaufnahme rufen die Kriminellen 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 Kriminellen schalten sich unbemerkt in die E-Mail-Kommunikation ein und manipulieren den Schriftverkehr. Meist

verändern sie die Kontodaten der Empfängerin bzw. des Empfängers, sodass es zur Übermittlung einer falschen IBAN kommt und die Rechnungsbegleichung an die Kriminellen selbst geht.

Phishing-Betrug

Unter dem Begriff Phishing versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdige Kommunikationspartnerin bzw. 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 Kriminellen selbst die erlangten persönlichen Daten für weitere Straftaten oder nehmen Kontakt mit den Opfern auf, um an deren finanzielle Vermögenswerte zu gelangen.

Phishing-Betrug auf Kleinanzeigenplattformen

Opfer eines Phishing-Betrugs werden auch Menschen, die private Gegenstände auf Kleinanzeigenplattformen verkaufen wollen. Die Kriminellen stellen den Kontakt zu den Geschädigten her und bekunden ihr scheinbares Kaufinteresse, um dann das Vertrauen der Opfer zu erlangen, werden Fragen über die Waren gestellt und Smalltalk betrieben. Die Kriminellen wirken seriös und ernsthaft interessiert. Schließlich schlagen sie vor, die weitere Kommunikation von der Kleinanzeigenplattform zu einem anderen Messengerdienst zu verlagern, die Zahlung über eine Drittanbieterin bzw. einen Drittanbieter und/oder die Warenübergabe über einen Kurierdienst abzuwickeln.

Die Opfer erhalten sodann einen Phishing-Link, der sie auf eine gefälschte Webseite weiterleitet. Dies 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 ihr Geld an die Täterinnen- und Täterschaft.

Banken-Phishing

Bei dieser Weiterentwicklung der bekannten Betrugsmasche mittels Phishing-SMS erhalten die Opfer zur Vorbereitung des Betrugs 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 damit 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 Täterinnen- bzw. 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 vorrangig um Echtzeitüberweisungen handelt, besteht nur eine geringe Wahrscheinlichkeit, die Geldbestände durch die Banken oder die Behörden wiederzuerlangen.

Kryptoexchanger-Phishing

2024 kam es auch verstärkt zu Phishingbetrug, bei welchem sich die Täterinnen- und Täterschaft als Bedienstete von nationalen sowie internationalen Kryptoexchangern ausgaben. Der Modus ist nahezu ident zu jenem, welcher im Unterkapitel Bankenphishing (siehe oben) erläutert wurde.

SEO-Banken-Phishing

Die Kriminellen erstellen gefälschte Webseiten, die nahezu ident zu echten Onlinebanking-Seiten wirken. Anschließend platzieren sie diese Fake-Seiten in den Suchmaschinenergebnissen, zum Beispiel bei Bing oder Google, möglichst weit oben. Ziel ist es, durch Suchmaschinenoptimierung (SEO) die Sichtbarkeit der betrügerischen Seiten zu erhöhen, sodass potenzielle Geschädigte sich den falschen Onlinebanking-Seiten bedienen, anstatt sich auf der Originalseite der Bank einzuloggen. Beim Login werden dem Opfer die Bankzugangsdaten abgephischt. Mit diesen Daten führen die Kriminellen unautorisierte Transaktionen von den Konten der Geschädigten durch. Meist wird hier die Funktion der Sofortüberweisung ausgeführt, um eine mögliche Sicherstellung des inkriminierten Betrages zu erschweren.

Vorauszahlungsbetrug

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

Love- oder Romance-Scam

Die Betrugsanbahnung erfolgt über Dating-Plattformen und soziale Medien. Durch regelmäßigen Kontakt schaffen es die Kriminellen, dass die Opfer eine emotionale Bindung zu ihnen aufbauen. Oft geben sie sich als Ingenieurinnen und Ingenieure, Ärztinnen und Ärzte oder Konstrukteurinnen und Konstrukteure aus der Ölindustrie oder als US-Soldatinnen bzw. -Soldaten aus. Beispielsweise werden den Opfern Geschichten präsentiert, wonach sich die Soldatin bzw. der Soldat im Auslandsaufenthalt befinde und derzeit nicht an ihr bzw. sein privates Vermögen gelange. Die Kriminellen bitten die verliebten Opfer um

finanzielle Unterstützung, meist via Zahlungsdienstleisterinnen und -anbieter oder mittels Überweisung. Wiederholt versprechen die Kriminellen, bald nach Österreich zu kommen und das Geld zurückzuzahlen. Die Lügengeschichten werden leicht abgewandelt, wiederholen sich aber solange, wie die Opfer zahlungswillig sind.

Vorauszahlungsbetrug Kredite

Bei dieser Art des Vorauszahlungsbetrugs werden auf verschiedenen Internetplattformen Privatkredite angeboten. Die Kriminellen geben vor, wegen Gebühren, Versicherungen oder Ähnlichem gewisse finanzielle Vorleistungen zu benötigen. Meist überweisen die Geschädigten dreistellige Beträge an das angegebene Bankkonto. Zu einer eigentlichen Kreditgewährung kommt es 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, vergleichsweise kostengünstige Angebote, die vorwiegend in sozialen Medien und einschlägigen Vermieterinnen- bzw. Vermieterplattformen geschaltet wurden. Nach Kontaktaufnahme – zumeist durch die Geschädigten selbst – wird eine Kautionszahlung gefordert. Das Opfer erhält im Nachgang nie Zugang zum gewünschten Objekt.

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. Für Immobiliengeschäfte und für diverse gesellschaftsrechtliche Maßnahmen bedarf es der Mitwirkung von Rechtsanwältinnen und Rechtsanwälten sowie Notarinnen und Notaren, die außergewöhnlichen Geschäften oder politisch exponierten Kaufinteressentinnen und -interessenten beziehungsweise der Kundschaft 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 von den Aufsichtsverfahren nach.

Zudem wurde im Berichtsjahr gemeinsam mit den Kammern, dem Bundesministerium für Justiz und dem Bundesministerium für Finanzen eine neue PPP-Initiative für rechtsberatende Berufe ins Leben gerufen.

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, weshalb der intensive länderübergreifende Austausch auch so wichtig ist. Die Zuständigkeit für die Gesetzgebung und Aufsicht des großen Glücksspiels steht der Bundeskompetenz zu. Im Berichtsjahr tauschte sich die A-FIU mehrfach mit den Glückspielaufsichtsbehörden im Bundesministerium für Finanzen und dem Finanzamt Österreich Dienststelle Sonderzuständigkeit aus und nahm zudem an Koordinierungstreffen der Aufsichtsbehörden auf Bund- und Länderebene teil. Ebenso wurde bei der Jahreskonferenz Glückspiel ein Vortrag im Zusammenhang mit Geldwäsche im Bereich Glückspiel seitens der A-FIU übernommen.

Gewerbeaufsichtsbehörden

Die A-FIU nahm sich 2024 zum Anlass, verstärkt mit Aufsichtsbehörden und Verpflichteten aus dem Bereich des Gewerberechts zusammenzuarbeiten. Die A-FIU veranstaltete insbesondere für die zuständigen Ämter in Wien zwei Schulungen, bei denen Trends

und Bezüge zwischen Geldwäscherei, Terrorismusfinanzierung und dem Missbrauch von Gewerbetreibenden veranschaulicht wurden.

Im Berichtsjahr bot die A-FIU auch verstärkt Unterstützungsleistungen für die Aufsichtsbehörden an, welche vermehrt in Anspruch genommen wurden. Die Prüfungen der jeweiligen Bezirksaufsichtsbehörden über die Einhaltung der Geldwäsche-Präventionsbestimmungen nach der GewO tragen einen wichtigen Teil zum Funktionieren der Geldwäschebekämpfung bei. Das Bündeln von Kompetenzen auf diesem Gebiet für ein ganzes Bundesland, wie beispielsweise durch die Schaffung eines Service-Centers für ganz Oberösterreich, hat sich als weiterer wichtiger und sinnvoller Schritt zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung herausgestellt.

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. Im Referat Strategische Finanzstromanalyse wird zudem ein aktives Stakeholder-Management betrieben, um so den laufenden Austausch mit allen relevanten Stakeholdern aus dem privaten und öffentlichen Sektor zu gewährleisten.

Mitteilungssystem

Bereits im Vorjahr wurde ein neues System zur Weitergabe relevanter Informationen insbesondere von Warnungen und Typologien entwickelt und im Berichtsjahr ausgebaut. Hierbei stehen den Meldeverpflichteten nun drei Kategorien von Mitteilungen und Warnungen, die farblich gekennzeichnet sind, als Informationsquelle zur Verfügung.

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 bekannten 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 und das Meldeverhalten sowie die Qualität verbessern soll. 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 der Geldwäschebekämpfung gemacht. Die Mitglieder bestehen aus den meist-meldenden Instituten, anderer strategischer Partnerinnen und Partner und den relevanten Behörden verschiedener Ressorts. Die Sitzungsleitung übernehmen abwechselnd das Bundesministerium für Finanzen und die A-FIU.

Die Public-Private-Partnership-Initiative dient als Diskussionsplattform zur vertrauensvollen Besprechung von komplexen Fällen sowie allgemeinen Herausforderungen bei der täglichen Arbeit und produziert regelmäßig gemeinsame Lösungen. In diesem Zusammenhang können auch regelmäßig effektivere Workflows für bestimmte Angelegenheiten in der Gruppe erarbeitet, umgesetzt und evaluiert werden. So wurde beispielsweise im Bereich der Scheinfirmenthematik ein neuer zielführender Workflow zur schnelleren Sicherstellung allfälliger Guthaben in Zusammenarbeit mit der Finanzpolizei entwickelt. Dieser Workflow hat sich mittlerweile als äußerst effektiv herausgestellt und wird regelmäßig zur Sicherung dieser inkriminierten Gelder angewendet.

Zudem wurde erstmals ein gemeinsames Risikopapier als Beitrag zur Nationalen Risikoanalyse erstellt und per goAML veröffentlicht.

Im Jahr 2024 fanden zwei reguläre FINA-Sitzungen zu einer Fülle an Themen statt. Dort wurden Herausforderungen technischer Natur besprochen. Zudem stellte die A-FIU ihren internen neuen Workflow dar, ebenso wie aktuelle Fälle, Phänomene und Trends. Ein wichtiger Schwerpunkt hierbei blieb auch im Jahr 2024 die Verbesserung der Meldequalität. Erfreulich war zudem die Aufnahme eines neuen regulären Mitglieds in das Financial Intelligence Network Austria.

Crypto-FINA

Im Jänner 2024 startete die A-FIU eine neue Untergruppe des bestehenden Formats FINA mit den österreichischen Kryptowerteanbieterinnen- und -anbietern, der A-FIU, dem BMF und Ermittlerinnen sowie Ermittlern des Bundeskriminalamtes. Diese PPP-Initiative soll das gegenseitige Verständnis sowie die vertrauensvolle Zusammenarbeit fördern. Aus diesem Grund fand im Berichtsjahr ein Kick-off-Event zum ersten Austausch auf dieser Ebene statt. Regelmäßige Termine sind für 2026 eingeplant, da im Jahr 2025 aufgrund der FATF-Überprüfung Österreichs vorhandene Ressourcen anderweitig im Einsatz waren sowie die Vergabe der MiCAR-Lizenz im Jahr 2025 startete und dies den Anbieterinnen- und Anbietermarkt in Österreich auch massiv verändern wird.

PPP Rechtsberatende Berufe

Der starke Fokus des Referats Strategische Finanzstromanalyse lag im Jahr 2024 neben der Analysetätigkeit im Bereich Prävention und Stakeholder-Management. Daher nahm es sich die A-FIU zum Anlass auch andere Branchen abseits des Finanzsektors stärker zu bespielen und forcierte den Austausch mit den Berufsgruppen der Rechtsanwältinnen und Rechtsanwälte sowie Notarinnen und Notare. Als Produkt dieser Zusammenarbeit wurde eine eigene Public-Private-Partnership mit aktiven Vertreterinnen und Vertretern der Berufsgruppen, der Kammern, des BMJ, des BMF und der A-FIU gestartet, welche im Berichtsjahr an zwei Terminen stattfand. Hierbei waren vor allem für die Berufsgruppen relevante Trends sowie die Abgabe und Inhalte von Verdachtsmeldungen als auch die FATF-Prüfung die wichtigsten Themen.

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 unterschiedlicher Bereiche. Die zu bearbeitenden Themenfelder sind auf sieben Work-Streams verteilt. Die A-FIU war im Berichtsjahr aktives Mitglied in den Work-Streams „Investment Fraud“, „Crypto-Assets“ und der „Innovation-Working-Group“.

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 Direktion für Staatsschutz und Nachrichtendienst, des Wirtschaftsministeriums, des Außenministeriums, der Finanzmarktaufsicht und der Österreichischen Nationalbank an den Sitzungen teil. Im Berichtsjahr fanden zwei Sitzungen des Nationalen Koordinierungsgremiums statt. Aufgrund der im Berichtsjahr gestarteten Überprüfung des österreichischen Systems zur Bekämpfung von Geldwäsche, Terrorismus- und Proliferationsfinanzierung durch die FATF (Financial Action Task Force) war dies das Hauptthema der Sitzungen.

Task-Force-Sanktionen

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

Geldwäschetagung

Aufgrund der umfangreichen Vorbereitungsarbeiten im Zusammenhang mit der FATF-Überprüfung wurde die nächste Geldwäschetagung auf das Jahr 2025 verschoben. Sie wird am 23. und 24. Oktober 2025 in Salzburg stattfinden.

Schulungen und Vorträge

Neben ihrem repressiven Auftrag Geldwäsche und Terrorismusfinanzierung aktiv zu bekämpfen, hat die A-FIU die präventive Aufgabe, den beteiligten Akteurinnen und Akteuren aktuelle Informationen über Methoden der Geldwäscherei und der Terrorismusfinanzierung sowie Anhaltspunkte hierzu zu verschaffen, anhand derer sich verdächtige Transaktionen erkennen lassen. Im Berichtsjahr hielt die Geldwäschemeldestelle über 30 Schulungen ab und trug bei unterschiedlichsten Fachveranstaltungen vor, um unter anderem das Bewusstsein für die Meldepflichten zu schärfen.

2024 wurde insbesondere ein Schwerpunkt auf Schulungen für den Nichtfinanzsektor sowie deren Aufsichtsbehörden gelegt.

Die A-FIU trug jedoch auch regelmäßig bei polizeiinternen Schulungen und Fortbildungsprogrammen vor, um auch im Bereich der Strafverfolgung mehr Verständnis für die Themen Geldwäsche und Terrorismusfinanzierung und die Tätigkeit der A-FIU zu schaffen.

Im Rahmen der Behördenleiterinnen- und Behördenleiterkonferenz des BMI durfte die A-FIU die Thematik Geldwäsche im Bereich des Gewerbes aufgreifen und dem hochkarätigen Publikum, darunter der Generaldirektor für öffentliche Sicherheit Franz Ruf, und der Direktor des Bundeskriminalamtes, Andreas Holzer, das dazugehörige Lagebild sowie zusammenhängende Fälle präsentieren.

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

Die Erfahrungen der A-FIU waren auch international gefragt. So präsentierte die A-FIU mehrere Fallstudien und Phänomene bei Expertinnen- und Expertentreffen der UNODC oder internationalen Konferenzen.

Ausblick

Im Berichtsjahr trat die neue EU-Verordnung MiCAR zur Vereinheitlichung des Rechtsrahmens für Kryptowerte und der damit verbundenen Dienstleistungen in Kraft. MiCAR steht für Markets in Crypto-Assets Regulation und umfasst auch umfangreiche Bestimmungen im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Im Jahr 2025 starten die Lizenzvergaben durch die österreichische Finanzmarktaufsicht für beantragende Kryptowerteanbieterinnen und -anbieter. Hierbei besonders ist, dass diese Unternehmen für ihr gesamtes EU-Geschäft lediglich in einem Mitgliedstaat ihre MiCAR-Lizenz beantragen und die Verdachtsmeldungen für ihr gesamtes Europageschäft nur im Lizenzstaat bei der dort ortsansässigen FIU abwickeln müssen. Aufgrund des zu erwartenden erhöhten Meldeaufkommens stellt dies die jeweiligen FIUs und damit auch die A-FIU künftig vor neue Herausforderungen.

International führende Kryptowertedienstleisterinnen und -dienstleister planen in Österreich die MiCAR-Lizenz zu beantragen, um ihr Europageschäft abzuwickeln und damit Meldungen an die A-FIU abzugeben. Dieser Umstand wird die A-FIU im Jahr 2025 stark beschäftigen und führt auch unter anderem zur erweiterten Personaloffensive der A-FIU sowie zum Ausbau des risikobasierten Ansatzes im Analyseverfahren, um damit auch für die künftigen Herausforderungen gewappnet zu sein.

Daneben wird auch die Implementierung und Umsetzung des neuen EU-Geldwäschepakets die A-FIU fordern, bietet im Umkehrschluss jedoch auch neue Chancen. Mit dem im Frühjahr 2024 vom Europäischen Parlament verabschiedeten Gesetzespaket zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung steht ein tiefgreifender Wandel des unionsweiten Regulierungsrahmens bevor, dessen Umsetzung in den kommenden Jahren auch auf nationaler Ebene spürbar werden wird.

Die neuen Vorschriften stärken die Rolle der zentralen Meldestellen (FIUs) deutlich: Sie erhalten erweiterte Befugnisse zur Analyse verdächtiger Finanzaktivitäten und zur Aussetzung auffälliger Transaktionen. Gleichzeitig wird der Zugang zu den Registern wirtschaftlicher Eigentümerinnen und Eigentümer für berechtigte Stellen erheblich erleichtert.

Darüber hinaus stehen verschärfte Sorgfaltspflichten für Verpflichtete wie Banken, Krypto-Dienstleisterinnen und -Dienstleistern sowie Immobilienvermittlerinnen und -vermittlern im Fokus. Diese Maßnahmen werden ergänzt durch eine europaweite Bargeldobergrenze, neue Vorschriften für besonders vermögende Personen sowie Maßnahmen zur besseren Durchsetzung von Finanzsanktionen.

Ein bedeutender struktureller Meilenstein ist die Errichtung der EU-Aufsichtsbehörde AMLA mit Sitz in Frankfurt, die ab 2025 als zentrale Instanz die wirksamere Koordinierung der nationalen Aufsichtsorgane gewährleisten und risikoreiche Finanzakteurinnen und Finanzakteure direkt beaufsichtigen soll.

Die A-FIU wird ihre nationale Rolle im Kontext dieser Neuregelungen entsprechend anpassen, insbesondere im Hinblick auf den Informationsaustausch und die internationale Zusammenarbeit. Es gilt, den Großteil der Bestimmungen bis zum 10. Juli 2027 in nationales Recht umzusetzen.

