

Lagebericht Geldwäsche 2025

Aktuelle Entwicklung der Geldwäsche
und der Vermögenskriminalität



Lagebericht Geldwäsche 2025

Aktuelle Entwicklung der Geldwäsche
und der Vermögenskriminalität

Wien, 2026

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres, Bundeskriminalamt
Josef-Holaubek-Platz 1, 1090 Wien
+43 1 24836 985025 (SPOC)
www.bundeskriminalamt.at

Layout: BMI I/C/10/a – Strategische Kommunikation und Kreation
Druck: Digitalprintcenter des Bundesministeriums für Inneres
Wien, 2026

Vorwort

Sehr geehrte Damen und Herren,

Geldwäsche und Terrorismusfinanzierung gefährden die Integrität unseres Finanz- und Wirtschaftsstandorts und ermöglichen es kriminellen Organisationen, Erträge aus Straftaten in den legalen Wirtschaftskreislauf einzuschleusen. Deren konsequente Bekämpfung ist daher ein wesentlicher Bestandteil einer wirksamen Sicherheits- und Kriminalpolitik. Digitalisierung, neue Zahlungsformen und Kryptowährungen stellen die Sicherheitsbehörden dabei laufend vor neue Herausforderungen.

Die Geldwäschemeldestelle (A-FIU) im Bundeskriminalamt nimmt in diesem System eine zentrale Rolle ein. Als Financial-Intelligence-Einheit verbindet sie Informationen über Finanztransaktionen mit den Bedürfnissen der Strafverfolgung. Durch die Analyse und Verknüpfung von Finanzinformationen werden verdächtige Finanzströme und Zusammenhänge sichtbar. Die daraus gewonnenen Erkenntnisse liefern wichtige Ermittlungsansätze für die Kriminalpolizei im Bundeskriminalamt, weitere Organisationseinheiten des Bundesministeriums für Inneres sowie für die Finanzverwaltung.

Das Jahr 2025 war wesentlich von der Evaluierung Österreichs durch die Financial Action Task Force (FATF) geprägt. Internationale Evaluierungen dieser Art sind von besonderer Bedeutung: Sie ermöglichen eine unabhängige Betrachtung der nationalen Strukturen, fördern den internationalen Vergleich und zeigen Möglichkeiten zur Weiterentwicklung der Systeme zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung auf. Gleichzeitig unterstreichen sie, dass eine wirksame Bekämpfung von Finanzkriminalität nur durch das koordinierte Zusammenwirken aller beteiligten staatlichen und privaten Akteure gelingen kann.

Eine wesentliche Grundlage erfolgreicher Financial Intelligence sind qualitativ hochwertige Verdachtsmeldungen. Unser besonderer Dank gilt daher den Meldeverpflichteten für die professionelle und konstruktive Zusammenarbeit. Ebenso danken wir den Mitarbeiterinnen und Mitarbeitern der A-FIU sowie allen beteiligten Behörden und internationalen Partnern für ihr großes Engagement.

Unser gemeinsames Ziel bleibt es, kriminelle Finanzströme frühzeitig zu erkennen, daraus konkrete Ermittlungsansätze zu gewinnen und kriminell erwirtschaftete Vermögenswerte konsequent aufzuspüren. Eine starke und moderne A-FIU leistet damit einen wesentlichen Beitrag zur Bekämpfung der organisierten Kriminalität sowie zur Sicherheit und Integrität des Finanz- und Wirtschaftsstandorts Österreich.



Franz Ruf

A stylized handwritten signature in black ink.

Generaldirektor für die
öffentliche Sicherheit



Andreas Holzer

A stylized handwritten signature in blue ink.

Direktor des
Bundeskriminalamts

Inhalt

Vorwort	3
Einleitung	8
Historischer Überblick	9
Al Capone und die Waschsalons	9
Entstehung des Begriffs „Geldwäsche“	10
Das Phänomen Geldwäsche	10
Kampf gegen die Geldwäsche	12
Sorgfaltspflichten der Verpflichteten	12
Das Delikt Geldwäscherei – § 165 Strafgesetzbuch	14
Die Austrian Financial Intelligence Unit (A-FIU)	16
Organisationsaufbau	16
Funktionen der A-FIU	17
Filterfunktion	17
Analyseverfahren	19
Befugnisse der A-FIU	20
Erheben, Verarbeiten, Übermitteln	20
Vorläufiges Unterbinden oder Aufschieben von Transaktionen	21
Europäische und internationale Kooperationen	23
Egmont-Group	23
Financial Action Task Force (FATF)	24
Financial Intelligence Unit Plattform	26
FIU.net	26
Legislativpaket der Europäischen Kommission	27
Die europäische Anti-Geldwäschebehörde (AMLA)	27
Das Jahr 2025 in Zahlen	29
Art und Herkunft der Akteneingänge	29
Qualität der Verdachtsmeldungen	30

Deliktsbereiche der Verdachtsmeldungen.....	31
Korrespondenz mit anderen Behörden.....	32
Nationale Kooperation.....	32
Internationale Kooperation.....	33
Weiterleitung von Analyseberichten.....	34
Auskunftsersuchen.....	35
Mitteilungen und Warnmeldungen.....	35
Transaktionsverbote, Sicherstellungen und Verurteilungen.....	36
Transaktionsverbote und Sicherstellungen.....	36
Verurteilungsstatistik.....	37
Phänomene, Muster und Trends.....	39
Identitätsdiebstahl und Geldwäsche über Online-Konten.....	39
Missbräuchliche Gründung von Vereinen.....	40
Echtzeitüberweisungen.....	41
Kryptowährungen.....	41
Gefahren im Zusammenhang mit Künstlicher Intelligenz.....	42
Vorfälle zur Geldwäscherei.....	44
Mord am 3. Mai 2025 in Salzburg.....	44
Scheinfirmenkonstrukt.....	44
Sonstige Betrugsformen im Überblick.....	45
Anrufbetrug.....	46
Bestellbetrug.....	47
Cyber-Trading-Fraud.....	48
CEO-Fraud und Business-E-Mail-Compromise.....	50
Phishing-Betrug.....	50
Vorauszahlungsbetrug	51
Kooperation mit Aufsichtsbehörden.....	54
Rechtsanwaltskammern und Notariatskammer.....	54

Glücksspielbehörde.....	55
Strategische Entwicklungen.....	56
Financial Intelligence Network Austria (FINA).....	56
PPP Rechtsberatende Berufe.....	57
European Financial Intelligence Public-Private Partnership (EFIPPP)	57
Nationales Koordinierungsgremium.....	57
Taskforce Sanktionen.....	58
Geldwäschetagung.....	58
Schulungen und Vorträge.....	58

Einleitung

Der vorliegende Geldwäschebericht gibt einen Überblick über die Tätigkeit der Geldwäschemeldestelle im Bundeskriminalamt (Austrian Financial Intelligence Unit – A-FIU), ihre Aufgaben sowie wesentliche Entwicklungen und Schwerpunkte des Jahres 2025. Das Berichtsjahr war von erheblichen fachlichen und organisatorischen Herausforderungen, aber auch von wichtigen Weichenstellungen für die weitere Entwicklung der A-FIU geprägt.

Ein bestimmendes Thema des Jahres war die **Evaluierung Österreichs durch die Financial Action Task Force (FATF)**. Der Evaluierungsprozess erforderte eine intensive Auseinandersetzung mit den Strukturen, Prozessen und der Wirksamkeit der österreichischen Geldwäschebekämpfung und stellte auch für die A-FIU einen wesentlichen Arbeitsschwerpunkt dar. Internationale Evaluierungen dieser Art sind eine wichtige Standortbestimmung und liefern wertvolle Impulse für die zukünftige Ausrichtung und Weiterentwicklung. Für die A-FIU verdeutlichte der Prozess insbesondere die Bedeutung einer konsequenten **risikobasierten Ausrichtung**. Angesichts der wachsenden Menge verfügbarer Finanzinformationen kommt es zunehmend darauf an, jene Sachverhalte zu identifizieren und prioritär zu analysieren, von denen ein besonders hohes Risiko im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung ausgeht. Dies erfordert eine kontinuierliche Weiterentwicklung der Analyseprozesse und technischen Möglichkeiten sowie einen zielgerichteten Einsatz der vorhandenen Ressourcen.

Eine wesentliche Grundlage für die Arbeit der A-FIU bleibt die Zusammenarbeit mit den **Meldeverpflichteten**. Die hohe Qualität der übermittelten Verdachtsmeldungen bildet den Ausgangspunkt für erfolgreiche Financial Intelligence. Der intensive Austausch mit dem privaten Sektor und den zuständigen Aufsichtsbehörden trägt dazu bei, aktuelle Risiken und Typologien frühzeitig zu erkennen und das gemeinsame Verständnis für neue Entwicklungen kontinuierlich zu verbessern.

Neben den nationalen Entwicklungen gewinnt die **europäische Dimension der Geldwäschebekämpfung** weiter an Bedeutung. Mit der Anti-Money-Laundering-Authority (AMLA) in Frankfurt wurde eine neue europäische Behörde geschaffen, die künftig auch die Zusammenarbeit und Koordinierung der nationalen Financial Intelligence Units wesentlich mitprägen wird. Für die A-FIU gilt es, diese Entwicklung aktiv mitzugestalten, österreichische Erfahrungen einzubringen und die Möglichkeiten einer noch engeren europäischen Zusammenarbeit zu nutzen.

Die Entwicklungen des Jahres 2025 zeigen damit auch die Richtung für die kommenden Jahre: Die A-FIU soll als **moderne, analytisch ausgerichtete und international ver-**

netzte Financial Intelligence Unit konsequent weiterentwickelt werden. Der Ausbau der operativen und strategischen Analysefähigkeiten, eine stärkere risikobasierte Priorisierung, moderne technische Analyseinstrumente sowie die enge Zusammenarbeit mit Meldeverpflichteten, nationalen Partnerbehörden und internationalen FIUs bilden dafür wesentliche Grundlagen.

Der vorliegende Bericht gibt Einblick in die Tätigkeit der A-FIU im Jahr 2025 und stellt aktuelle Entwicklungen, Zahlen, Kooperationen sowie ausgewählte Phänomene und Typologien der Geldwäsche und Terrorismusfinanzierung dar.

Historischer Überblick

Geldwäsche ist kein modernes Phänomen. Seit Jahrhunderten versuchen Menschen, illegal erworbenes oder vor staatlichem Zugriff verborgenes Vermögen zu verschleiern. Was sich im Laufe der Zeit verändert hat, sind die Methoden, die Komplexität und die technischen Möglichkeiten, illegale Einnahmen in den legalen Wirtschaftskreislauf einzuschleusen.

Schon in der Antike und im Mittelalter wurden Vermögenswerte vor staatlichem Zugriff verborgen – etwa durch Strohmannen oder verschleierte Handelsgeschäfte. Ein oft zitiertes frühes Beispiel ist China vor rund 2.000 Jahren, wo Kaufleute Vermögen über weite Distanzen transferierten, um es vor Behörden zu schützen.

In der Neuzeit gewann das Thema besonders im Kontext der organisierten Kriminalität an Bedeutung. Während der Prohibition in den USA entstanden enorme illegale Gewinne aus Alkoholschmuggel, Glücksspiel und anderen verbotenen Aktivitäten. Diese Einnahmen mussten „legitimiert“ werden, um sie nutzen zu können.

Al Capone und die Waschsalons

Auch Al Capone ist ein Teil der Geschichte der Geldwäsche. Capone und andere Gangster investierten ihre illegalen Gewinne in bargeldintensive Geschäfte wie Waschsalons (engl.: laundromats), Restaurants oder Spielhallen. Diese Betriebe boten eine plausible Erklärung für große Bargeldmengen, da ihre tatsächlichen Einnahmen schwer nachvollziehbar waren.

Ob Capone selbst tatsächlich Waschsalons im großen Stil nutzte, ist historisch nicht eindeutig belegt. Der Begriff „Geldwäsche“ wurde jedenfalls erst später geprägt, aber die zugrundeliegende Idee, illegales Geld durch scheinbar legale Einnahmen zu „reinigen“, entspricht genau diesem Prinzip.

Interessanterweise wurde Capone letztlich nicht wegen seiner Gewaltverbrechen, sondern wegen Steuerhinterziehung verurteilt – ein Hinweis darauf, wie schwierig es damals war, Geldwäsche direkt nachzuweisen.

Entstehung des Begriffs „Geldwäsche“

Der Begriff „Geldwäsche“ (engl.: money laundering) tauchte erst deutlich später auf, vermutlich in den 1970er-Jahren in den USA. Bekannt wurde er insbesondere im Zusammenhang mit dem Watergate-Skandal, bei dem illegale Wahlkampfgelder über komplexe Finanzstrukturen verschleiert wurden. Medien und Ermittler begannen, diese Praxis als Geldwäsche zu bezeichnen.

Seit den 1980er-Jahren wurde der Begriff international etabliert, parallel zur zunehmenden Regulierung: Staaten erkannten, dass Geldwäsche ein zentrales Element organisierter Kriminalität ist und begannen, systematisch dagegen vorzugehen.

Das Phänomen Geldwäsche

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

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

- Platzierung („Placement“),
- Schichtung („Layering“) und
- Reintegration („Reintegration“).

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

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

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 beispielsweise 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 Weltbruttoinlandsproduktes 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- und rechtsberatende Berufe, Immobilienmaklerinnen und Immobilienmakler sowie 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 bzw. Umgehung gezielter finanzieller Sanktionen im Zusammenhang mit Proliferationsfinanzierung für die Berufsgruppe der Kredit- und Finanzdienstleister sowie 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 von Kundenstock, Branche etc. handelt es sich hierbei um eine individuelle Einschätzung 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 berechtigte Grund zur Annahme, dass ein Geschäft in Zusammenhang mit Geldwäsche oder mit Terrorismusfinanzierung steht, sind sie zur Erstattung einer Verdachtsmeldung an die A-FIU verpflichtet. Steht der konkrete Geschäftsfall oder die Transaktion noch bevor, kann von der A-FIU eine Entscheidung darüber verlangt werden, ob gegen die unverzügliche Durchführung Bedenken bestehen. Äußert sich die A-FIU nicht bis zum Ablauf des folgenden Bankarbeits- oder Werktags, darf das Geschäft 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 bildet 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 einer 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**.

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

Für die Strafbarkeit nach Absatz 1 ist es übrigens irrelevant, ob die Geldwäsche durch dieselben Täterinnen oder Täter begangen wird wie das vorgelagerte Delikt (sogenannte Eigengeldwäsche) oder ob sie durch Dritte erfolgt (sogenannte Fremdgeldwäsche). Auch

wer versucht, den illegalen Ursprung seiner eigenen Schwarzgelder durch komplexe Transaktionen über die eigenen Konten zu verschleiern, kann sich der Geldwäscherei strafbar machen.

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

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

Organisationsaufbau

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

Referat 7.3.1 – Internationale Angelegenheiten

Referat 7.3.2 – Strategische Finanzstromanalyse

Referat 7.3.3 – Operative Finanzstromanalyse

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

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

Dem Referat Operative Finanzstromanalyse obliegt die Entgegennahme der Verdachtsmeldung und die Durchführung des Analyseverfahrens. Es wertet die übermittelten

Informationen aus, zerlegt sie in ihre Bestandteile und gleicht gewonnene Informationen mit den vorhandenen Datenbeständen ab. Anschließend überprüft das Referat Operative Finanzstromanalyse, ob weitere polizeiliche Erkenntnisse oder sonstige finanznachrichtendienstliche Informationen bekannt sind, die den gemeldeten Verdachtsfall verdichten.

Zudem steht der A-FIU ein eigenes Technikerteam mit drei Personen für die Entwicklung interner Softwarelösungen zur effizienteren Analyse und Hilfsmittel hierzu, statistischer 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) wurden für 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 und auch bei sogenannten Joint Analysis Teams mitwirken und koordinieren, die bei wichtigen grenzüberschreitenden Fällen gebildet werden. Die erste dieser Planstellen wurde mit 1. Februar 2026 besetzt.

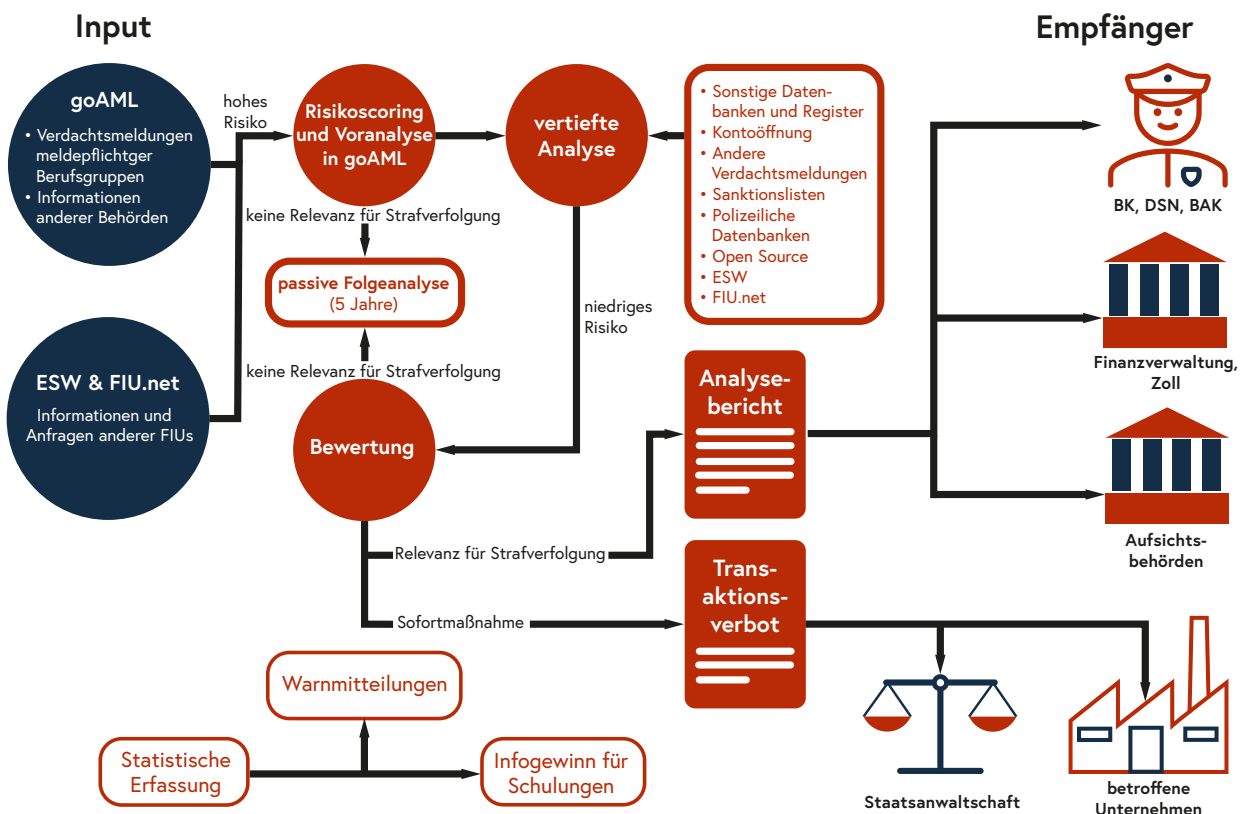
Im Berichtsjahr waren durchschnittlich 25 Mitarbeitende in der A-FIU beschäftigt.

Funktionen der A-FIU

Filterfunktion

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

Die niedrige Schwelle der Meldepflicht führt zu einem hohen Informationsaufkommen auf Seiten 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 Terrorismus zugrunde liegt. Die einlangenden Informationen durchlaufen ein besonderes Analyseverfahren. Dieser Vorgang dient unter anderem dazu, die Strafverfolgungsbehörden zu entlasten, indem diesen nur solche Sachverhalte übermittelt werden, deren strafrechtliche Verfolgung aufgrund eines vorliegenden Anfangsverdachts gerechtfertigt ist oder die für ihre Arbeit sonst von Relevanz zu sein 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 internationalen Typologien bzw. Berichten der FATF, aber auch basierend auf einer tiefgreifenden Analyse zusammenhängender Daten eingehender Verdachtsmeldungen. Dies dient dazu, möglichst jene Fälle einer vertieften Analyse zu unterziehen, die auf Basis dieses komplexen risikobasierten Verständnisses als besonders geldwäschegeneigt einzustufen sind.

Analyseverfahren

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 usw.). Die übermittelten Informationen werden verifiziert und mit weiteren Datenbeständen abgeglichen. Die A-FIU überprüft ferner, ob weitere polizeiliche Erkenntnisse oder sonstige finanznachrichtendienstliche Informationen bekannt sind, die den gemeldeten Verdachtsfall verdichten. Ist es zur Verhinderung oder zur Verfolgung von Geldwäscherei oder Terrorismusfinanzierung erforderlich, holt die A-FIU ergänzende Auskünfte von den meldepflichtigen Berufsgruppen ein oder leitet einen internationalen Schriftverkehr mit ausländischen Partnerdiensten ein.

Die A-FIU ist jedoch nicht im Dienste der Strafrechtspflege tätig. Ermittlungshandlungen im Sinne der Strafprozessordnung stehen ihr nicht zu: Erhärtet sich aufgrund des Analyseverfahrens der Verdacht, dass eine Straftat begangen worden ist, leitet die Geldwäschemeldestelle ihr Analyseergebnis sowie zusätzliche relevante Informationen an die für die Strafverfolgung zuständigen Stellen weiter. In Fällen vermuteter Terrorismusfinanzierung leitet die A-FIU ihr Analyseergebnis an die Direktion Staatsschutz und Nachrichtendienst (DSN) weiter, bei Verdacht auf Korruptionsdelikte an das Bundesamt 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 maximal fünf Jahren sind die ermittelten Daten zu löschen.

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

Befugnisse der A-FIU

Zur ordnungsgemäßen Erfüllung ihres Auftrags steht der Geldwäschemeldestelle eine Reihe von Befugnissen zur Verfügung:

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.

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

ISF-Projekt Interoperabilität

Im Jahr 2025 setzte die Geldwäschemeldestelle (A-FIU) ihre in den Vorjahren erfolgreich betriebene Projektstätigkeit im Rahmen des Internal Security Fund (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 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 unmittelbar 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. Ergänzend haben sie das Recht, von der A-FIU eine Entscheidung dahingehend zu verlangen, ob gegen die unverzügliche Durchführung des Geschäfts Bedenken bestehen.

Kommt die A-FIU aufgrund ihrer Analyse zu dem Ergebnis, dass hinsichtlich der 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 Transaktionssperre für notwendig erachtet, regt sie diese daher direkt bei der Staatsanwaltschaft an. Die Staatsanwaltschaft kann so von Beginn an über die dauerhafte Sicherstellung entscheiden und zwar ohne Dazwischentreten eines verwaltungsrechtlichen Transaktionsverbots der A-FIU. Die Vorgangsweise beschleunigt die Sicherstellung verdächtiger Vermögenswerte und vereinfacht den 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 sogenannten Bedenkenäußerung gemäß § 17 Abs 3 FM-GwG erfolgen. In diesem Fall kann auf Basis des Gesamtsachverhalts 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, das in einer Bedenkenäußerung der A-FIU mündet. In diesen Fällen obliegt die Entscheidung, ob das Geschäft trotz der von der A-FIU mitgeteilten Bedenken durchgeführt oder davon Abstand genommen wird, den jeweiligen Meldepflichtigen unter Berücksichtigung ihrer individuellen Risikobewertung.

Europäische und internationale Kooperationen

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

Egmont-Group

Die Egmont-Gruppe ist ein weltweiter Zusammenschluss von 177 nationalen FIUs mit Hauptsitz in Toronto (Kanada). 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 führten dazu, dass die Egmont-Gruppe im Jahr 2023 Russlands Mitgliedschaft in der Gruppe und in der Kommunikationsplattform ESW suspendierte und diese Suspendierung auch im Berichtsjahr 2025 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.

Das 31. Plenartreffen der Egmont-Gruppe fand vom 6. bis 11. Juli 2025 in Luxemburg statt, bei dem die österreichische A-FIU wieder vertreten war.

Financial Action Task Force (FATF)

Die Financial Action Task Force (FATF) ist ein 1989 gegründetes internationales Gremium, das globale Standards zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und Proliferationsfinanzierung entwickelt. Die 40 Empfehlungen der FATF bilden den internationalen Standard in diesen Bereichen und haben wesentlichen Einfluss auf nationale und europäische Regelungen.

Ein zentrales Instrument der FATF sind die sogenannten Mutual Evaluations. Dabei handelt es sich um umfassende Länderprüfungen in Form eines Peer-Review-Verfahrens. Expertinnen und Experten anderer Staaten untersuchen, inwieweit die FATF-Standards umgesetzt sind und ob die vorhandenen Maßnahmen in der Praxis tatsächlich wirksam funktionieren.

Die Bewertung erfolgt auf zwei Ebenen: Im Rahmen der Technical Compliance wird geprüft, inwieweit die rechtlichen und institutionellen Rahmenbedingungen den 40 FATF-Empfehlungen entsprechen. Einen besonderen Stellenwert nimmt die Bewertung der Effectiveness ein. Dabei wird anhand von elf sogenannten Immediate Outcomes (IOs) beurteilt, ob das nationale System in der Praxis die angestrebten Ergebnisse bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung erzielt.

Für die A-FIU ist insbesondere der Immediate Outcome 6 (IO.6 – Financial Intelligence) von zentraler Bedeutung. Dabei wird bewertet, inwieweit Financial Intelligence und andere relevante Informationen von den zuständigen Behörden für Ermittlungen im Zusammenhang mit Geldwäsche, deren Vortaten und Terrorismusfinanzierung genutzt werden. Im Mittelpunkt stehen unter anderem die Analyse von Verdachtsmeldungen und weiteren Informationen durch die A-FIU, die daraus entwickelten Intelligence-Produkte, deren Weitergabe an die zuständigen Behörden sowie deren tatsächlicher Nutzen für die operative Arbeit. Damit wird nicht allein die Menge der produzierten Informationen beurteilt, sondern insbesondere, ob Financial Intelligence einen konkreten Mehrwert für Ermittlungen und die Identifizierung krimineller Finanzströme schafft.

Mutual Evaluation Österreich

Die Vorbereitungen auf die Mutual Evaluation Österreichs begannen bereits 2023 unter Federführung des Bundesministeriums für Finanzen (BMF). Aufgrund des umfassenden Charakters der Evaluierung waren zahlreiche Ministerien, Behörden, Aufsichtsstellen und weitere Akteure des österreichischen Systems zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung eingebunden.

Die A-FIU ist ein wesentlicher Akteur des österreichischen Geldwäscheregimes und war dementsprechend intensiv in die Vorbereitungen und den Evaluierungsprozess eingebunden. Als zentrale Financial Intelligence Unit Österreichs kommt ihr insbesondere im Rahmen des IO.6 eine bedeutende Rolle zu. Neben der Darstellung ihrer eigenen Analyseleistungen war dabei auch das Zusammenspiel mit Strafverfolgungsbehörden, anderen zuständigen Behörden, Meldeverpflichteten und internationalen Partnern von Bedeutung.

Ein zentraler Meilenstein der Evaluierung war der On-Site-Visit im Juli 2025 in Wien, der sich über insgesamt zwei Wochen erstreckte. Im Zuge dieses Vor-Ort-Besuchs führte das internationale Evaluierungsteam Gespräche mit zahlreichen österreichischen Akteuren. Auch die A-FIU wurde vor Ort umfassend zu ihren Aufgaben, Arbeitsweisen und zur Wirksamkeit ihrer Tätigkeit befragt.

Die ersten Feststellungen des Evaluierungsteams, die in weiterer Folge auch Gegenstand medialer Berichterstattung wurden, waren für die A-FIU Anlass für eine intensive und akribische Nachberichterstattung. In den darauffolgenden Monaten wurden zusätzliche Informationen, Statistiken, Fallbeispiele und Nachweise aufbereitet, um die Tätigkeit und insbesondere die Wirksamkeit der A-FIU umfassend und nachvollziehbar darzustellen.

Einen weiteren wesentlichen Meilenstein bildete das Face-to-Face-Meeting im Dezember 2025 in Washington. Dort konnten offene Fragestellungen und die zwischenzeitlich übermittelten Informationen unmittelbar mit dem Evaluierungsteam erörtert werden. Die intensive Nachbereitung nach dem On-Site-Visit trug dazu bei, dass erste Feststellungen

der Evaluatoren in einzelnen Bereichen nochmals einer vertieften Betrachtung unterzogen und verbessert werden konnten.

Der Evaluierungsprozess war mit Ende des Berichtsjahres 2025 noch nicht abgeschlossen. Den formellen Abschluss der Mutual Evaluation bildet die FATF-Plenarversammlung im Februar 2026 in Mexiko-Stadt, in deren Rahmen der Evaluierungsbericht und die finalen Bewertungen Österreichs beraten und beschlossen werden. Die konkreten Ergebnisse und Bewertungen der Mutual Evaluation werden daher nicht vorweggenommen und im Geldwäschebericht 2026 dargestellt.

Unabhängig von den abschließenden Ergebnissen hat der Evaluierungsprozess bereits im Berichtsjahr wichtige Impulse geliefert. Insbesondere die intensive Auseinandersetzung mit IO.6 und der tatsächlichen Nutzung von Financial Intelligence verdeutlicht die Bedeutung einer leistungsfähigen, risikobasiert arbeitenden und analytisch ausgerichteten FIU für eine wirksame Bekämpfung von Geldwäsche und Terrorismusfinanzierung.

Financial Intelligence Unit Plattform

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

FIU.net

Bei FIU.net handelt es sich um ein dezentralisiertes System, das von den 27 FIUs der Europäischen 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 Mitgliedsstaat aufweisen. Das Grundprinzip von FIU.net ist, dass jede FIU ihre Informationen in ihrer eigenen lokalen Datenbank speichert und diese mit anderen europäischen FIUs mithilfe des lokalen FIU.net-Applikationsservers austauscht. Bis 2021 wurde FIU.net von Europol betreut und gewartet. Im Zuge einer Weiterentwicklung des Systems hat der europäische Datenschutzbeauftragte zum Jahresende 2019 ausgesprochen, dass die technische Betreuung von FIU.net durch Europol nicht mehr zulässig sei, und dessen Transfer zu einer anderen EU-Institution gefordert. Seit Anfang 2023 arbeitet die Kommission an einer neuen Version der FIU.net-Anwendung, die in enger Zusammenarbeit mit der FIU-Gemeinschaft entwickelt wird. Im Zusammenhang mit dem Aufbau der AMLA kommt der Weiterentwicklung von FIU.net als zentralem euro-

päischen Austauschsystem für FIUs besondere Bedeutung zu. Ziel ist insbesondere die Sicherstellung eines stabilen operativen Betriebs sowie die weitere Verbesserung des grenzüberschreitenden Informationsaustausches zwischen den europäischen FIUs.

Legislativpaket der Europäischen Kommission

Im Juli 2021 hat die Europäische Kommission einen Vorschlag für ein neues Legislativpaket zur Bekämpfung von Geldwäsche 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 2025 weitere interministerielle sowie bilaterale Termine zur Umsetzung des Geldwäschepakets sowohl auf nationaler als auch auf europäischer Ebene statt. 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 bleiben.

Die europäische Anti-Geldwäschebehörde (AMLA)

Die europäische Anti-Geldwäschebehörde Anti-Money Laundering Authority (AMLA) wurde am 26. Juni 2024 gegründet und hat ihre operative Tätigkeit am 1. Juli 2025 in Frankfurt am Main (Deutschland) aufgenommen.

Die AMLA soll die Zusammenarbeit der europäischen Behörden im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung weiter stärken. Ein besonderer Schwerpunkt liegt dabei auf der Unterstützung der nationalen Financial Intelligence Units (FIUs), der Verbesserung des Informationsaustausches sowie der Förderung gemeinsamer Analyseansätze bei grenzüberschreitenden Sachverhalten.

Die zunehmende Internationalisierung von Geldwäschehandlungen und komplexen Finanzstrukturen erfordert eine enge operative Zusammenarbeit zwischen den europäischen FIUs. AMLA soll hierzu insbesondere die Zusammenarbeit in gemeinsamen Analyseprojekten und sogenannten Joint Analysis Teams unterstützen sowie technische und organisatorische Kooperationsmechanismen innerhalb der Europäischen Union weiterentwickeln.

Seit Februar 2026 unterstützt ein Vertreter der österreichischen A-FIU die Zusammenarbeit zwischen AMLA und den Vertreterinnen und Vertretern nationaler FIUs vor Ort in Frankfurt am Main. Die Tätigkeit umfasst insbesondere die Mitwirkung an operativen und strategischen Arbeitsgruppen sowie die Unterstützung gemeinsamer Analyseansätze im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung.

Für die österreichische A-FIU stellt die Einbindung in die AMLA-Strukturen einen wichtigen Schritt zur weiteren Vertiefung der europäischen Zusammenarbeit dar. Gleichzeitig ermöglicht sie einen noch engeren Austausch mit europäischen Partnerbehörden und trägt zur Stärkung der grenzüberschreitenden Finanzstromanalyse innerhalb der Europäischen Union bei.

Das Jahr 2025 in Zahlen

Entsteht bei den meldeverpflichteten Berufsgruppen der berechtigte Grund zur Annahme, dass ein Geschäft in Zusammenhang mit Geldwäscherei oder 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 2025 eingelangten Verdachtsmeldungen und ihre Herkunft, über den Akteneingang im Allgemeinen und über den weiteren Umgang mit Sachverhalten, deren Analyse weitergehende kriminalpolizeiliche Ermittlungen erforderten.

Art und Herkunft der Akteneingänge

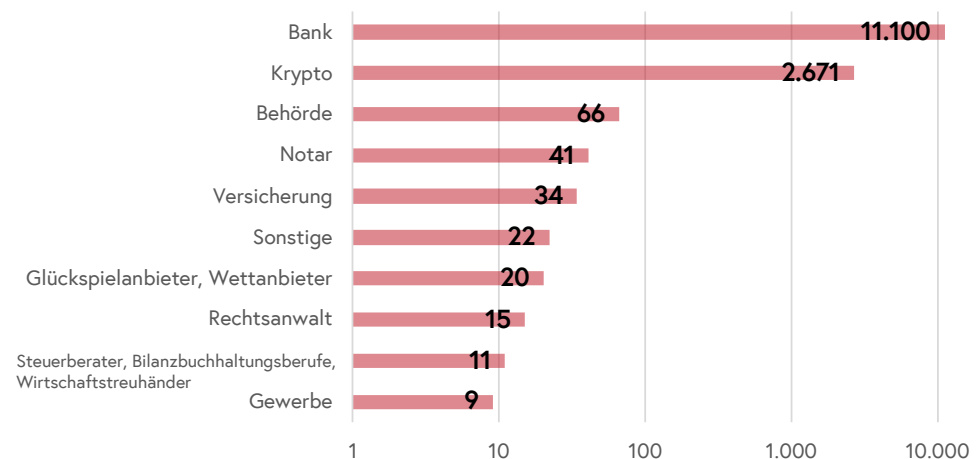
Einführend muss erläutert werden, dass die A-FIU für das Berichtsjahr 2025 eine umfangreiche Umstellung der statistischen Berechnungsart (auf Basis der goAML-Aufzeichnungen) aller Akteneingänge durchgeführt hat. Dies führt dazu, dass eine direkte Gegenüberstellung mit Eingängen aus Vorjahren nicht mehr sinnvoll möglich ist. Um jedoch zumindest einen direkten Vergleich mit dem Vorjahr zu ermöglichen, wurde das Jahr 2024 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 2025 verzeichnete die Geldwäschemeldestelle insgesamt 19.292 Akteneingänge – eine erneute deutliche Steigerung von rund 49 Prozent im Vergleich zum Vorjahr, 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 bildete wie in den vergangenen Jahren die Gruppe der Verdachtsmeldungen von Verpflichteten (13.923). Von Behörden erhielt die A-FIU im Berichtsjahr insgesamt 66 Verdachtsmeldungen.

Mit 11.100 Verdachtsmeldungen steht erneut der Bankensektor an der Spitze, gefolgt von den Anbietern von Kryptowerte-Dienstleistungen, die im Berichtsjahr 2.671 Verdachtsmeldungen erstattet haben. Das ist ein Anstieg von ca. 117 Prozent. Diese Entwicklung zeichnete sich aufgrund der massiven Kursgewinne diverser Kryptowährungen im Berichtsjahr und dem damit verbundenen Zugewinn an Interesse ab. Die erhöhte Nachfrage hat in weiterer Folge auch wieder zu mehr Verdachtsfällen bei Kryptowerte-Dienstleistern geführt. Durch die bevorstehende Umsetzung der Verordnung über Märkte für Kryptowerte (MiCAR – Markets in Crypto Assets Regulation) und die bereits erkennbare Ansiedlung neuer Anbieter am Standort Österreich ist in Zukunft mit einem erneuten starken Anstieg der Verdachtsmeldungen von künftigen Crypto Asset Service Providern zu rechnen.

Erfreulicherweise zeigte das intensive Präventionsprogramm der A-FIU, die verstärkte Kooperation durch Schulungen und neue Public-Private-Partnership-Initiativen (PPP-Initiativen) Wirkung und es konnte so in fast allen Verpflichtetenkategorien ein Anstieg an Verdachtsmeldungen verzeichnet werden.

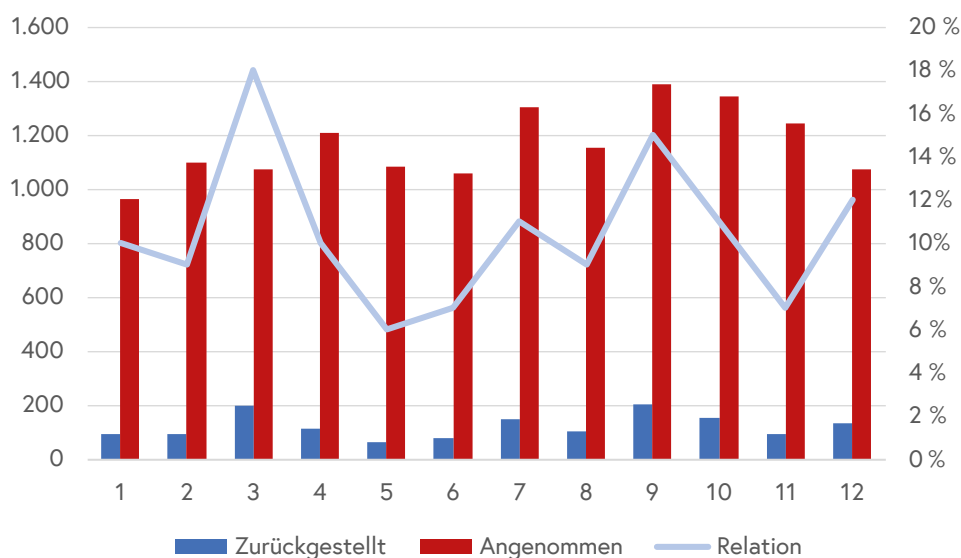


Qualität der Verdachtsmeldungen

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.

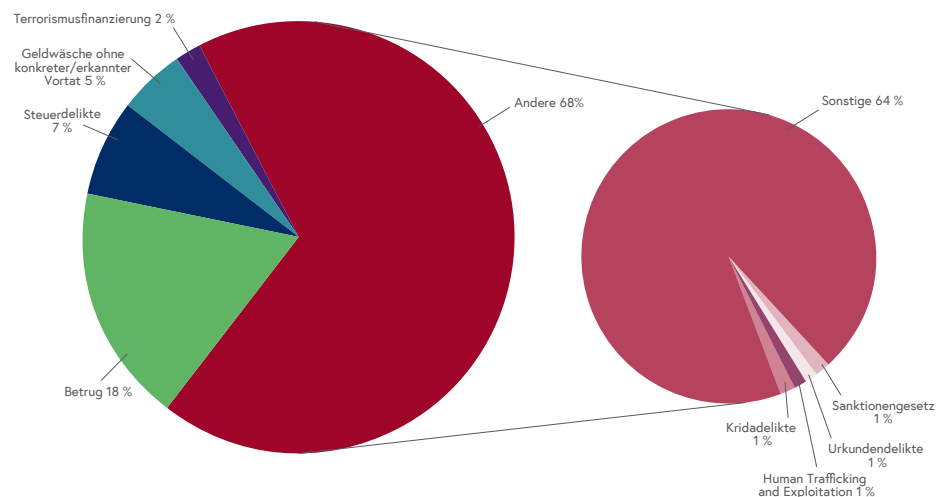
Die Qualität der Verdachtsmeldungen ist in den vergangenen Jahren gestiegen. Im Berichtsjahr stellte die A-FIU noch zehn Prozent der erstmals einlangenden Verdachtsmeldungen zur Verbesserung zurück, dies stellt einen minimalen Anstieg zum Vorjahr dar. Auch in diesen Fällen erfolgt die Verbesserung meist zeitnah und verlässlich. Die folgende Grafik zeigt die Gegenüberstellung von akzeptierten zu erstmals zurückgestellten Verdachtsmeldungen im Jahr 2025. Die Qualitätsverbesserung von Meldungen und die damit erhöhte Verlässlichkeit der erhaltenen Daten verschafft der A-FIU auch einen wertvollen Zeitvorteil für Sicherstellungen und andere Maßnahmen zur Verhinderung sowie Bekämpfung von Geldwäsche und Terrorismusfinanzierung.



Deliktsbereiche der Verdachtsmeldungen

Die Analyse der Geldwäschemeldestelle erlaubt es, die meisten Verdachtsmeldungen bestimmten Deliktsbereichen zuzuordnen. Mit 18 Prozent der Verdachtsmeldungen dominierten nach wie vor Betrugshandlungen die festgestellten Vortaten. Die Gruppe der Meldungen basierend auf „Geldwäsche ohne konkreter/erkannter Vortat“ ging auf nur mehr fünf Prozent zurück.

Bei sieben Prozent der Verdachtsmeldungen erkannte die A-FIU, dass die gemeldeten Sachverhalte in Zusammenhang mit Steuerdelikten stehen könnten. In zwei Prozent der Fälle lag der Verdacht auf Terrorismusfinanzierung vor, während ein Prozent der Meldungen Verdachtsmomente im Zusammenhang mit Urkundendelikten berichtete. Mögliche Sanktionsverstöße konnten in einem Prozent der Verdachtsmeldungen als mögliche Vortat festgestellt werden. Zudem stellte die A-FIU in einem Prozent der Meldungen Zusammenhänge mit Menschenhandel fest. Bei den Verdachtsmeldungen wurden zudem keine Zusammenhänge mit Korruptionsdelikten festgestellt. 65 Prozent der Verdachtsmeldungen konnten anderen Straftaten zugeordnet werden. Sie verteilen sich auf Suchtmitteldelikte, Kridadelikte und organisierte Kriminalität.



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 Bundesministerium für Finanzen (BMF) und das Finanzamt Österreich haben bei der Wahrnehmung ihrer Aufgaben im Berichtsjahr 2025 in 58 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 gleich-

gestellte Zahlungsmittel (zum Beispiel Gold- oder Silbermünzen) zum Zweck der Geldwäscherei oder Terrorismusfinanzierung verbraucht werden. In diesem Zusammenhang erhielt die A-FIU 13 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 diese bei der Ausübung ihrer Aufsichtstätigkeit mit Geldwäscherei oder Terrorismusfinanzierung in Zusammenhang stehende Transaktionen auffallen. Von diesen Behörden erhielt die Geldwäschemeldestelle im Berichtsjahr zwei Meldungen.

Internationale Kooperation

Die A-FIU leitete in über 3.567 Fällen einen internationalen Schriftverkehr ein, um nähere Informationen zu den analysierten Sachverhalten einzuholen beziehungsweise die Partnerdienste über eigene Erkenntnisse zu informieren. Dabei wurde in diesem Berichtsjahr am häufigsten FIU.net verwendet, gefolgt von Egmont Secure Web.



Weiterleitung von Analyseberichten

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

Von den insgesamt 13.989 im Berichtsjahr erhaltenen Verdachtsmeldungen gingen nach Durchführung des Analyseverfahrens 4.324 in Form von Analyseberichten an die Strafverfolgungsbehörden zur weiterführenden Ermittlung bzw. an ausländische Partnerdienste weiter. Das entspricht einem Anteil von 31 Prozent der eingelangten Verdachtsmeldungen. Dem gegenüber steht die Differenz von 9.665 Fällen, die die A-FIU mangels Anfangsverdachts oder weiterer Analyseansätze zur passiven Folgeanalyse bei sich behielt.

Insbesondere die komplexen Fälle von vermuteter Geldwäsche erfordern weiterführende Sachverhaltsklärungen im Rahmen eines Ermittlungsverfahrens. Besteht der Verdacht der Geldwäsche oder ihrer Vortaten, ist aber kein Zusammenhang mit besonderen Tatbeständen wie Steuer- oder Zollvergehen, Terrorismus- oder Korruptionstatbeständen erkennbar, leitet die A-FIU ihr Analyseergebnis an die zuständigen Stellen im Bundeskriminalamt oder – mangels ausreichenden Österreichbezugs für weitere Ermittlungen – an ausländische Partnerdienste weiter. Österreich ist ein attraktiver internationaler Finanzplatz. Das verursacht natürlich auch Verdachtsfälle bei ausländischen 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 in jenes weiter. Daher werden erstmals auch die internationalen Weiterleitungen von Analyseergebnissen zur weiteren Analyse bzw. in weiterer Folge zur Veranlassung eines Ermittlungsverfahrens im Ausland selbstständig angeführt. Diese Gruppe an Weiterleitungen stellt im Berichtsjahr 2025 die zahlenmäßig größte Empfängergruppe mit 25 Prozent dar.

Wie auch in den Vorjahren wurden Analyseberichte häufig (zwei Prozent) an die Fachabteilungen und Büros im Bundeskriminalamt gesandt. Rund zwei Prozent der Analyseberichte gingen wegen vermuteter Steuer- oder Zollvergehen an die Abgabenbehörden des Bundes und rund ein Prozent an die Direktion Staatsschutz und Nachrichtendienst weiter.

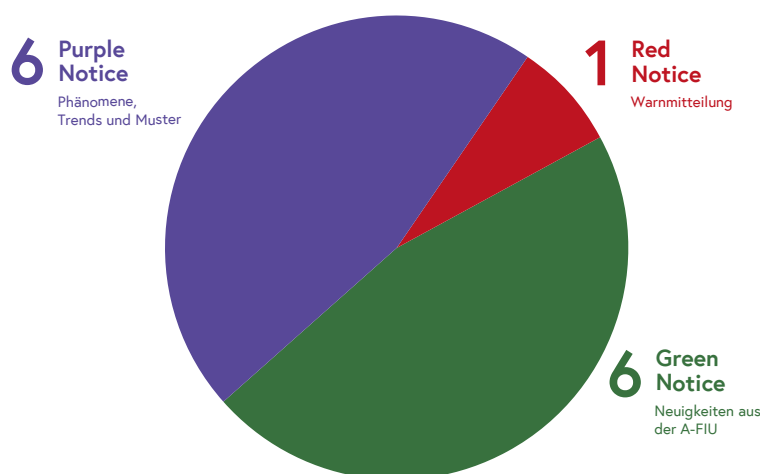
Fälle vermuteter Verletzungen der Vorschriften des Finanzmarkts gehen an die Finanzmarktaufsicht und Sachverhalte im Zusammenhang mit Korruptionsdelikten an das Bundesamt zur Korruptionsprävention und -bekämpfung.

Auskunftersuchen

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 265 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 in 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 für Verpflichtete hilfreiche Informationen 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

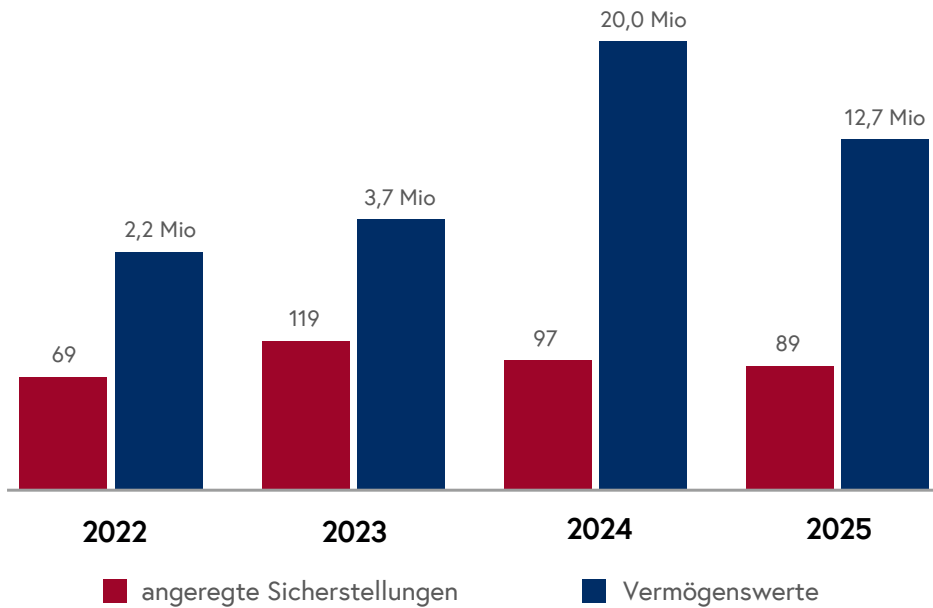
Transaktionsverbote und Sicherstellungen

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, 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.

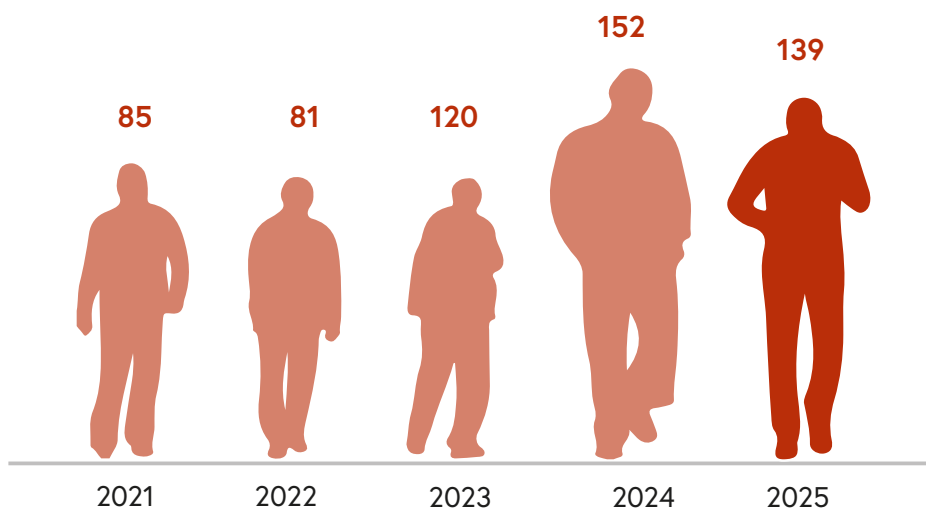
Die Geldwäschemeldestelle hat 2025 zahlreiche vermögensrechtliche Anordnungen angeregt. Diese dienten der Sicherstellung von verdächtigen Vermögenswerten. Der Gesamtwert dieser Vermögenswerte belief sich im Jahr 2025 auf rund 13 Millionen Euro. Die im Berichtsjahr weiter ausgebaut Zusammenarbeit zwischen der A-FIU, Kriminalpolizei, Staatsanwaltschaften und Abgabenbehörden sowie die exzellente Mitwirkung der Verpflichteten führten dazu, dass in den meisten Fällen rasche Sicherungsmaßnahmen erwirkt werden konnten.



Verurteilungsstatistik

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

2025 gab es 139 rechtskräftige Verurteilungen wegen Geldwäscherei zu verzeichnen, das entspricht rund neun Prozent weniger Verurteilungen im Vergleich zum Vorjahr.



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

Phänomene, Muster und Trends

Neben andauernden internationalen Konflikten und den Sanktionspaketen der Europäischen Union beschäftigte die A-FIU auch weiterhin die Verschiebung von verdächtigen Geldmitteln aus der Ukraine nach Österreich. Zudem konnten die Gründung und Nutzung von Vereinen zu vermeintlichen Geldwäschezwecken festgestellt und analysiert werden. Daneben waren die Etablierung bereits bestehender technischer Trends und das Hinzukommen neuer Produkte auf dem Markt besonders bemerkbar und zeichneten 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 technologische Weiterentwicklungen im Zahlungsverkehr, aber auch seit Langem bestehende Methoden genutzt werden, um inkriminierte Gelder zu waschen.

Identitätsdiebstahl und Geldwäsche 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, die durch qualifizierte elektronische Signaturen oder 1-Cent-Legitimationsverfahren (Referenzzahlung) zur Identitätsbestätigung eingesetzt werden. Die Tätergruppen verwenden gefälschte Ausweise, die auf die Personendaten real existierender, unbeteiligter Personen ausgestellt sind – ein Fall von Identitätsdiebstahl. Als Adressen auf den gefälschten Dokumenten werden häufig Arztpraxen, Geschäftslokale oder ähnliche Einrichtungen angegeben. Es handelt sich dabei um österreichische Reisepässe oder Dienstpässe. Die Konten wurden wiederum genutzt, um weitere Konten mittels der 1-Cent-Legitimation zu eröffnen und anschließend zum Empfang sowie Weitertransfer von Betrugsgeldern, die in weiterer Folge im nahen Ausland bar behoben wurden. In diesem Zusammenhang musste die A-FIU feststellen, dass zum Teil auch 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 Anbietern dafür, die wiederum unterschiedliche Produktpakete offerieren. Die Divergenz zwischen der Qualität dieser ist nach Auffassung und Feststellung der A-FIU enorm.

Ein Identitätsdiebstahl kann – wenn er nicht sofort erkannt wird – für die betroffenen Personen massive Auswirkungen bis hin zu strafrechtlichen Ermittlungen bzw. deren Folgen haben. Die Opfer können auch finanzielle Schäden erleiden, da es zu Kontosperrungen oder Rückforderungen kommen kann. 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 1-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

Auch im Berichtsjahr 2025 wurde vermehrt die Gründung von Vereinen durch ausländische Staatsbürgerinnen und Staatsbürger zu Zwecken der vermeintlichen Geldwäsche beobachtet.

Hierbei besonders war die Häufung von Vereinen an bestimmten Adressen. 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 -bürgern 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 üblichen Zahlungen wie 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 privaten Konten der Vereinsorgane weitertransferiert. Dieser Vorgang, insbesondere aufgrund der hohen Geldbewegungen, war Anlassfall einer tiefgreifenden Analyse des Phänomens und Überprüfung der Anwendbarkeit dieses auch auf andere Vereinskonstrukte.

Im Zuge dessen wurde auch mit der für das Wirtschaftliche Eigentümer Registergesetz (WiEReG) zuständigen Behörde im BMF zusammengearbeitet und eine Reihe von verdächtigen Vereinen identifiziert. In bestimmten Fällen, auch 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 in weiterer Folge ein Vereinskonto eröffnet werden. Damit verbunden sind wesentlich höhere Schwellen im Transaktionsmonitoring als bei Privatkonten, was solche Konten für Kriminelle dementsprechend interessant macht.

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 Nutzung und Attraktivität der Echtzeitüberweisung konnten 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 und Ermittler in den nächsten Jahren stark beschäftigen wird.

Kryptowährungen

Im Jahr 2025 hat die EU-Kryptoregulierung MiCAR (Markets in Crypto-Assets Regulation) den europäischen Kryptomarkt stark verändert. Die MiCAR hat das Ziel, einen einheitlichen Rechtsrahmen für Kryptowerte innerhalb der Europäischen Union zu schaffen. Anbieter von Krypto-Services benötigen nun eine offizielle Lizenz, die von der Finanzmarktaufsicht (FMA) vergeben wird, und müssen strengere Anforderungen bei Risikomanagement, Transparenz, Geldwäscheprävention und Kundenschutz erfüllen. Besonders im Fokus standen 2025 Zulassungsverfahren für sogenannte Crypto-Asset-Service-Provider (CASPs) sowie die Regulierung von Stablecoins und Krypto-Börsen. Anbieter müssen umfangreiche Sicherheitsstandards erfüllen, Eigenkapital nachweisen, transparente Geschäftsmodelle offenlegen und strenge Maßnahmen zur Geldwäscheprävention umsetzen. Ziel der Europäischen Union ist es, Risiken für Verbraucherinnen

und Verbraucher sowie für das Finanzsystem zu reduzieren, ohne Innovation vollständig einzuschränken.

Österreich entwickelt sich dadurch zunehmend zu einem attraktiven europäischen Standort für regulierte Kryptounternehmen – unter anderem, weil bekannte internationale Plattformen ihre EU-Lizenzen über Österreich beantragt haben. Insgesamt gilt die MiCAR als wichtiger Schritt hin zu mehr Rechtssicherheit, stärkerem Anlegerschutz und einer Professionalisierung des Kryptomarktes.

Auch für die A-FIU bringt die MiCAR weitreichende Veränderungen mit sich. Mit der zunehmenden Ansiedlung neuer meldepflichtiger Unternehmen in Österreich ist künftig mit einem Anstieg an Verdachtsmeldungen zu rechnen. Um darauf vorbereitet zu sein, hat die A-FIU bereits frühzeitig entsprechende Entwicklungs- und Vorbereitungskonzepte erarbeitet, damit potenzielle Ressourcenengpässe vermieden werden können.

Bis Ende 2025 wurde bereits acht Unternehmen in Österreich die Zulassung als Anbieter von Kryptowerte-Dienstleistungen erteilt.

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 verwendet. Solche Fälschungen zu erkennen ist ohne technische Expertise bzw. 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, Transaktionen durchzuführen. Bereits drei Sekunden Tonaufnahme genügen, um damit jede Wortfolge einer Person in einem täuschend echt klingenden „Originalton“ nachzuahmen. In Zeiten von sozialen Medien und den häufig unbedachten Veröffentlichungen von Alltäglichkeiten auf diversen Plattformen ist es keine große Herausforderung mehr, an Stimmbeispiele vieler Menschen zu gelangen.

Gerade in großen Unternehmen, in denen wegen langer Hierarchieketten eine gewisse Anonymität herrscht, können Kriminelle so 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 einer einjährigen Freiheitsstrafe bedroht sind, oder aus den §§ 223, 229, 289, 293, 295 StGB oder §§ 27 oder 30 Suchtmittelgesetz stammt, ist Geldwäsche überhaupt möglich.

Die folgenden Fallbeispiele veranschaulichen die bedeutendsten Vortaten des Berichtsjahres und geben einen Einblick in die Risikolandschaft Österreichs. Die daraus gewonnenen Analysen und Erkenntnisse stellt die A-FIU den Aufsichtsbehörden sowie Verpflichteten und Strafverfolgungsbehörden zur Prävention und Bekämpfung von Geldwäsche und Terrorismusfinanzierung zur Verfügung.

Mord am 3. Mai 2025 in Salzburg

Am 3. Mai 2025 wurde in Maria Alm eine Frau von ihrem ehemaligen Lebenspartner auf offener Straße ermordet. Da der Täter auf der Flucht war und eine Alarmfahndung vorerst erfolglos blieb, wurde die A-FIU vom Landeskriminalamt Salzburg, das die Ermittlungen wegen Verdacht des Mordes übernommen hatte, um Unterstützung ersucht.

Durch die A-FIU konnten Transaktionsdaten einer vom vermeintlichen Mörder verwendeten Kreditkarte zur Verfügung gestellt werden. Anhand dieser Daten konnte der Täter in den Niederlanden lokalisiert und in weiterer Folge von der Zielfahndung festgenommen werden.

Scheinfirmenkonstrukt

Im Frühjahr 2024 hat die A-FIU Verbindungen zwischen

- acht Personen,
- drei Firmen und
- 91 Konten

durch Analyse feststellen können. Es hat sich der Verdacht auf Übertretungen nach steuerrechtlichen Vorschriften ergeben. Daher wurde der Sachverhalt an das Amt für Betrugsbekämpfung im Bundesministerium für Finanzen (BMF ABB) weitergeleitet. Durch

die enge, sehr gute Kooperation und weitere Analysen (Verschneidung der Daten) konnte schnell erkannt werden, dass es sich um ein großes Scheinfirmenkonstrukt handelte. Da sich im Zuge der Analyse zunehmend auch Verdachtsmomente hinsichtlich verschiedener strafrechtlich relevanter Delikte – darunter kriminelle Vereinigung, gewerbsmäßiger Betrug, betrügerischer Datenverarbeitungsmissbrauch, Urkundenfälschung, Geldwäsche, Schlepperei und Sozialleistungsbetrug – ergaben, wurde im März 2025 auch das Büro 3.1 des Bundeskriminalamtes (Ermittlungen gegen die organisierte Kriminalität) in die weiteren Ermittlungen einbezogen.

Die Ermittlungen wurden in weiterer Folge unter dem Namen „AG Dolus“ geführt. Im März 2026 wurden über Anordnung der zuständigen Staatsanwaltschaft Wien vier Festnahmen, vier Vorführungen zur sofortigen Vernehmung sowie zwölf Hausdurchsuchungen im Raum Wien und Niederösterreich durchgeführt.

Insgesamt konnten rund 190 Beschuldigte ausgeforscht und eine vorläufige Schadenssumme von rund 4,8 Millionen Euro festgestellt werden. Die Ermittlungen dauern weiterhin an.

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: Internettelefonie, Messengerdienste und Echtzeitüberweisungen haben unser Wirtschaftsleben derart beschleunigt und anonymisiert, dass sich Betrugereien 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 Geldwechselbetrugereien 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 Geldwäscherei einnehmen, hat das Büro für Betrugsermittlungen im Bundeskriminalamt 2022 ein Lagebild zum Betrug aufgebaut. Dieses gibt tagesaktuell Auskunft über die österreichweite Betrugslage und über regionale Häufungen von Betrugsanzeigen und hat sich wiederholt als Frühwarnsystem bewährt, das neueste Betrugsmaschen frühzeitig aufdeckt und bei der Steuerung bundesweiter Schwerpunktaktionen unterstützt.

Anrufbetrug

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

Falsche Polizistinnen und Polizisten

Diese Form des Betrugs zielt insbesondere auf das Vertrauen älterer Menschen ab. Betrügerinnen und Betrüger geben sich als Polizistinnen und Polizisten, Staatsanwältinnen und Staatsanwälte oder Bankangestellte aus und nutzen Angst und Verunsicherung, um die Opfer zu manipulieren. Die Kriminellen warnen vor vermeintlichen Einbrecherinnen und Einbrechern oder korrupten Bankangestellten, die das Vermögen der Opfer gefährden würden. Wertsachen werden anschließend „zu Sicherungszwecken“ abgeholt. Unter Anwendung des „Kautionsstricks“, auch „Schockanruf“ genannt, werden die Opfer dazu gedrängt, hohe Summen für Angehörige zu zahlen, die einen tödlichen Unfall verursacht haben sollen, um sie vor einer Haftstrafe zu bewahren.

Bei der Bekämpfung dieses Modus Operandi konnten im vergangenen Jahr große Erfolge verzeichnet werden. Die verursachte Schadenssumme durch falsche Polizistinnen und Polizisten stieg allerdings im Vergleich zum Vorjahr auf über zehn Millionen Euro. Lag die Zahl der Anzeigen im Jahr 2024 noch bei 687, ist im Jahr 2025 ein Anstieg auf 756 Anzeigen zu verzeichnen. Die skrupellose Professionalität der Tätergruppen spiegelt sich bei einem drastischen Anstieg von 40 Prozent bei den Vollendungen der Tathandlungen und somit, wie bereits oben erwähnt, beim Anstieg der Schadenssumme.

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 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

Auch im Jahr 2025 führte der sogenannte Tech-Support-Scam (falsche Software-Mitarbeiterinnen und -Mitarbeiter) zu hohen Schadenssummen. 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 Benutzerkonten der Geschädigten, dass spezielle Sicherheitsupdates im virtuellen Beisein der angeblichen Mitarbeiterin bzw. des angeblichen Mitarbeiters durchgeführt werden müssen oder dass es z. B. zu einer Fehlbuchung kam und die bzw. der Betroffene nun eine angebliche Gutschrift erhalten soll (Bekanntgabe von Bankdaten).

Microsoft-Pop-up-Scam

2025 wurde ein neues Betrugsphänomen registriert, das unter dem Begriff „Microsoft-Pop-up-Betrug“ subsumiert wird. Dieses Phänomen zeigt einen weitgehend einheitlichen Modus Operandi und ist dem zuvor erwähnten „Tech-Support-Scam“ ähnlich.

Typischerweise werden die Geschädigten mittels gefälschter Sicherheitswarnungen oder Pop-up-Meldungen auf angebliche Schadsoftware, Hackerangriffe oder Sicherheitsprobleme aufmerksam gemacht und in weiterer Folge durch Abbildung einer „Service-Hotline“ zur Kontaktaufnahme mit vermeintlichen „Microsoft-“ oder „Windows-Supportmitarbeitern“ veranlasst. Durch die Installation von Fernwartungssoftware erlangen die Täterinnen und Täter Zugriff auf die betroffenen Systeme und bewegen die Opfer unter erheblichem psychischem Druck zu Vermögensverfügungen. Danach werden Onlinebanking-Zugänge kompromittiert, Überweisungen durchgeführt oder Gelder über Täter- beziehungsweise Mule-Konten weitertransferiert. Zusätzlich treten vermehrt Kryptowährungs-Transaktionen, Sicherheitskonten sowie Gutschein-/Gift-Card-Modelle in Erscheinung.

Bestellbetrug

Der „Bestellbetrug“ bildet den Überbegriff verschiedener Varianten von Betrugereien im Onlinehandel. Man unterscheidet zwischen zwei unterschiedlichen Begehungsformen, dem Versandbetrug einerseits und dem Warenbetrug andererseits. Beim Versandbetrug bestellen die Täterinnen und Täter Waren im Internet mit dem Vorsatz, diese nach Erhalt nicht zu bezahlen. Von Warenbetrug spricht man, wenn Täterinnen und Täter Waren mit dem Ziel anbieten, Opfer zu einer Bezahlung zu bringen, ohne jedoch die versprochene

Ware jemals liefern zu wollen oder anstatt der eigentlich bestellten Ware eine qualitativ minderwertigere Ware zu versenden.

Bestellung auf fremden Namen

Diese Begehungsform definiert sich dadurch, dass die Kriminellen frei erfundene oder tatsächlich existierende Identitäten benutzen und in deren Namen Waren bestellen. Zumeist werden mit den Daten der Geschädigten Einkaufsaccounts 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

Die Kriminellen 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 Fake-Produkt, das 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 die Täterinnen und Täter die Geschädigten auf Onlineshops von täuschend echt wirkenden Firmen, bei denen die Produkte zu einem bedeutend unterdurchschnittlichen Preis offeriert werden. Die Geschädigten bestellen dort das gewünschte Produkt und überweisen den Kaufbetrag im Vorhinein. Ein Warenversand tritt in weiterer Folge nicht ein oder es werden nur Pakete mit wertlosem Inhalt versendet.

Cyber-Trading-Fraud

Bei der Betrugsform Cyber-Trading-Fraud (CTF) handelt es sich um jenes Phänomen innerhalb der Betrugsdelikte, das zwar von der Quantität nicht zu den führenden Anzeigen zählt, jedoch jenes darstellt, das in Österreich 2025 den größten finanziellen Schaden verursachte.

Oftmals suchen Opfer selbst aktiv im Internet nach Investmentmöglichkeiten und stoßen dabei auf von den Täterinnen und 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 und -spezialisten“ und
- Empfehlungen durch Dating-App-Kontakte („Pig Butchering“).

Die Opfer erhalten meist Telefonanrufe, nachdem sie ihre Kontaktdaten bekanntgegeben haben. Die Kriminellen eröffnen sodann ein vermeintliches Tradingkonto für die Opfer, oftmals unter der Bedingung, dass ein niedriger Betrag als Erstinvestment eingezahlt werden muss. Das Portfolio entwickelt sich zunächst prächtig und die Opfer erzielen scheinbar gute Gewinne. 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 weiter an komplexe Geldwäschenetze transferiert werden. Vielmehr werden weitere Forderungen gestellt, um zu einer etwaigen Auszahlung zu gelangen (Steuern, Notariatskosten etc.).

Die Kriminellen setzen hierbei 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, die vorgeben, die verloren geglaubte Investition wieder retour überweisen zu können. Geschädigte bezahlen abermals an diese Täterschaft, eine Rückbuchung erfolgt nicht (Recovery-Scam).

Pig-Butchering

Diese Form des Betrugs ist ebenso für einen hohen finanziellen Schaden verantwortlich und kombiniert den klassischen Romance-Scam (Vorauszahlungsbetrug) mit den zuvor erwähnten Cyber-Trading-Fraud. Die Anbahnung der Täterinnen und Täter zu den Opfern erfolgt vorrangig über Dating- sowie Social-Media-Plattformen.

Nachdem das Vertrauen der Opfer erschlichen wurde, beginnen die Kriminellen damit, das Interesse des Opfers auf ein vermeintlich lukratives Investitionsmodell zu lenken, das 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 Partnerfirmen mit ausländischen Bankverbindungen und ersuchen die Beteiligten um absolute Verschwiegenheit. Nach der ersten schriftlichen Kontaktaufnahme rufen die Täterinnen und Täter die ausführenden Mitarbeitenden in der Buchhaltung an und setzen sie unter Druck, die Zahlung möglichst rasch vorzunehmen.

Unter Business-E-Mail-Compromise (BEC) versteht man das Kompromittieren eines Unternehmens durch betrügerische Phishing-E-Mails. Dabei treten zwei Firmen in Kontakt zueinander, mit der Absicht, ein Geschäft abzuwickeln. Die Täterinnen und Täter 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 Täterinnen und Täter geht.

Phishing-Betrug

Unter dem Begriff Phishing versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner auszugeben. Ziel der Kontaktaufnahme ist zunächst, an persönliche Daten eines zukünftigen Opfers zu gelangen. In der Regel handelt es sich hierbei um Online-Banking-Zugangsdaten. Im Anschluss daran missbrauchen die Täterinnen und Täter 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 Täterinnen und Täter 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 Täterinnen und Täter wirken seriös und ernsthaft interessiert. Schließlich schlagen sie vor, die weitere Kommunikation von der Kleinanzeigenplattform zu einem anderen Messenger-Dienst zu verlagern, die Zahlung über einen Drittanbieter und/oder die Warenübergabe über einen Kurierdienst abzuwickeln.

Die Opfer erhalten sodann einen Phishing-Link, der sie auf eine gefälschte Webseite weiterleitet. Diese vermittelt den Opfern den Eindruck, die verkaufte Ware sei bereits

bezahlt. Die Opfer werden weiter aufgefordert, ihre Kreditkartendaten einzugeben, damit der Betrag scheinbar überwiesen werden kann. Mit dem Bestätigen der Freigabe erhalten die Opfer jedoch kein Geld – im Gegenteil: In Wirklichkeit geben die Opfer eine Zahlung frei und überweisen damit Geld an die Täterinnen und Täter.

Banken-Phishing

Bei dieser Weiterentwicklung der bekannten Betrugsmasche mittels Phishing-SMS erhalten die Opfer zur Vorbereitung des Betrugs zumeist eine SMS im Namen einer vermeintlichen Bank. Die SMS informiert die Opfer darüber, dass angeblich widerrechtliche Abbuchungen von ihrem Konto erfolgt seien oder dass die Opfer die Legitimation für das Online-Banking verlängern müssten. Die Opfer werden 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 Täterschaft mit gefälschten Telefonnummern an und angebliche Bankbedienstete melden sich und bauen Vertrauen auf. Die Opfer werden aufgefordert, Überweisungen zu bestätigen bzw. freizugeben. Da es sich vorrangig um Echtzeitüberweisungen handelt, besteht nur eine geringe Wahrscheinlichkeit, die Geldbestände durch die Banken oder die Behörden wiederzuerlangen.

Kryptoexchanger-Phishing

Auch dieses Phishing-Phänomen führte im Jahr 2025 erneut zu einem hohen Schadensanfall. Die Täterschaft tritt dabei im Namen von nationalen und internationalen Kryptohandelsbörsen auf und gibt vor, dass Probleme mit den Kundenkonten beziehungsweise der Transaktionssicherheit vorliegen. In weiterer Folge veranlassen die Kriminellen die Geschädigten zu vermeintlichen Sicherheitstransaktionen. In Wahrheit transferieren die Geschädigten deren Vermögenswerte in die Sphären der Täterschaft.

Der Modus ist nahezu ident zu jenem, der im Unterkapitel „Falsche Bankmitarbeiterinnen und Bankmitarbeiter“ (siehe oben) erläutert wurde.

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.

Handmade/Heimarbeit/Jobangebot

Im Jahr 2025 zeigte sich erstmals, dass das Betrugsphänomen „Handmade/Heimarbeit/Jobangebot“ nicht nur für die Akquise von klassischen Money Mules beziehungsweise

deren Bankkonten verwendet wurde, sondern dass damit auch die „Bewerberinnen und Bewerber“ für derartige Jobs geschädigt werden können.

Die Opfer werden über soziale Medien auf Inhalte aufmerksam, in denen einfache und zugleich lukrative Heimarbeit in Aussicht gestellt wird.

Dabei wird der Eindruck vermittelt, dass durch den Ankauf, die Bearbeitung oder Weiterverarbeitung halbfertiger Produkte, wie etwa Kugelschreiber, Perlenketten, Haarspangen oder vergleichbarer Waren, rasch Provisionen erzielt werden können.

Zu Beginn leisten die Opfer kleinere Überweisungen für den angeblichen Erwerb dieser Produkte. In weiterer Folge werden sie in Messengergruppen eingeladen, in denen zunehmend höherwertige Produkte angeboten werden. Parallel dazu steigen sowohl die geforderten Überweisungsbeträge als auch das den Opfern angezeigte, von ihnen selbst eingerichtete Provisionskonto.

Im weiteren Verlauf wird den Opfern mitgeteilt, sie hätten bei der Bestellung Fehler begangen, und das Provisionskonto wird eingefroren. Um die bereits angezeigten Provisionen wieder freischalten zu können, werden die Opfer zu weiteren, beträchtlicheren Zahlungen aufgefordert.

Diese Gelder werden anschließend ins Ausland transferiert.

Love- oder Romance-Scam

Die Betrugsanbahnung erfolgt hierbei über Dating-Plattformen und soziale Medien. Durch regelmäßigen Kontakt schaffen es die Kriminellen, dass die Opfer eine emotionale Bindung zu ihnen aufbauen. Die Betrügerinnen und Betrüger geben sich oftmals als Ingenieurinnen und Ingenieure, Ärztinnen und Ärzte, Konstrukteurinnen und Konstrukteure aus der Ölindustrie oder als US-Soldatinnen und US-Soldaten aus. Beispielsweise geben die Täterinnen und Täter vor, sich als Soldaten im Auslandseinsatz zu befinden und vorübergehend keinen Zugriff auf ihr eigenes Vermögen zu haben. Unter diesem Vorwand ersuchen sie ihre bereits emotional gebundenen Opfer um finanzielle Unterstützung, meist über Zahlungsdienstleister oder mittels Überweisung. Gleichzeitig stellen sie eine baldige Rückkehr nach Österreich sowie die Rückzahlung der überwiesenen Beträge in Aussicht. Die erfundenen Geschichten werden dabei immer wieder leicht angepasst und so lange fortgeführt, wie die Opfer bereit sind, weitere Zahlungen zu leisten.

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 Vermieterplattformen geschaltet wurden. Nach Kontaktaufnahme – zumeist durch die Geschädigten selbst – wird eine Kautionszahlung in Vorauszahlung 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 als auch für diverse gesellschaftsrechtliche Maßnahmen bedarf es der Mitwirkung von Rechtsanwältinnen und Rechtsanwälten und/oder Notarinnen und Notaren, die außergewöhnlichen Geschäften oder politisch exponierten Kaufinteressentinnen und -interessenten 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 Aufsichtsverfahren nach.

Die Public-Private-Partnership-Initiative für rechtsberatende Berufe, die im Jahr 2024 gemeinsam mit den Kammern, dem Bundesministerium für Justiz und dem Bundesministerium für Finanzen ins Leben gerufen wurde, ist auch im Berichtsjahr 2025 erfolgreich weitergeführt worden.

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. Daneben steht die Zuständigkeit für die Gesetzgebung und Aufsicht des großen Glücksspiels der Bundeskompetenz zu. Im Berichtsjahr tauschte sich die A-FIU mehrfach mit den Glücksspielaufsichtsbehörden im Bundesministerium für Finanzen und dem Finanzamt Österreich, Dienststelle Sonderzuständigkeit, aus und nahm zudem an Koordinierungstreffen der Aufsichtsbehörden auf Bundes- und Länderebene teil. Ebenso wurde bei der Jahreskonferenz Glücksspiel ein Vortrag im Zusammenhang mit Geldwäsche im Bereich Glücksspiel seitens der A-FIU übernommen.

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 wie auch öffentlichen Sektor zu gewährleisten.

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 sollen. Wegen der Bedeutung des Finanzsektors – die Verpflichteten nach dem FM-GwG stellen die größte Meldegruppe dar – und seiner Funktion als „Gatekeeper“ des heimischen Finanzsystems ist eine enge Zusammenarbeit mit diesem Sektor für jede FIU von großer Wichtigkeit. Die Geldwäschemeldestelle und das Bundesministerium für Finanzen haben zu diesem Zweck die bereits seit mehreren Jahren bestehende Arbeitsgruppe zur Bekämpfung von Finanzkriminalität weiterentwickelt und zur größten nationalen Public-Private-Partnership-Initiative im Bereich Geldwäschebekämpfung gemacht. Die Mitglieder bestehen aus den meistmeldenden Instituten, weiteren strategischen Partnern und den relevanten Behörden verschiedener Ressorts. Die Sitzungsleitung übernehmen abwechselnd das Bundesministerium für Finanzen und die A-FIU.

Die Private-Public-Partnership-Initiative dient als Diskussionsplattform zur vertrauensvollen Besprechung von komplexen Fällen 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.

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 und der 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, die im Berichtsjahr an zwei Terminen zusammentraf. Hierbei waren vor allem für die Berufsgruppen relevante Trends, die Abgabe und der Inhalt von Verdachtsmeldungen sowie 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 Bundesministeriums für Justiz, des Bundesministeriums für Wirtschaft, Energie und Tourismus, des Bundesministeriums für europäische und internationale Angelegenheiten, der Direktion Staatsschutz und

Nachrichtendienst, 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 Taskforce) war dies das Hauptthema der Sitzungen.

Taskforce Sanktionen

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

Geldwäschetagung

Die Geldwäschetagung fand im Berichtsjahr 2025 am 23. und 24. Oktober in Salzburg statt. Burkhard Mühl vom European Financial and Economic Crime Centre (EFECC) bei Europol eröffnete die Tagung mit einer Keynote, in der er Einblicke in die Arbeit des EFECC und aktuelle Entwicklungen im Bereich der Finanz- und Wirtschaftskriminalität gab. Im Rahmen einer Podiumsdiskussion gewährte unter anderem Claude Bocqueraz von der Financial Crime Unit der Europäischen Kommission wertvolle Einblicke zum Thema AMLA. Die nächste Geldwäschetagung ist für den Oktober 2026 geplant.

Schulungen und Vorträge

Neben ihrem repressiven Auftrag, Geldwäsche und Terrorismusfinanzierung aktiv zu bekämpfen, hat die A-FIU auch die präventive Aufgabe, den beteiligten Akteurinnen und Akteuren aktuelle Informationen über Methoden der Geldwäscherei und der Terrorismusfinanzierung und Anhaltspunkte hierzu zu verschaffen, anhand derer sich verdächtige Transaktionen erkennen lassen.

