

Financial Intelligence Unit

Jahresbericht 2025



Financial
Intelligence Unit



Financial Intelligence Unit
Jahresbericht 2025

Inhalt

Vorwort	07
Kennzahlen	11
Im Fokus	17
Entwicklungen	27
Digitalisierung und Technologie	45
Strategische Auswertung	49
Anhang	57
Verzeichnisse	77

Vorwort



Quelle: Andrea Zahler

Daniel Thelesklaf
Leiter der FIU Deutschland

Liebe Leserinnen und Leser,

das Jahr 2025 hat für die Financial Intelligence Unit (FIU) Deutschland eine Reihe wichtiger Veränderungen gebracht. Ich freue mich, Ihnen den Jahresbericht der Zentralstelle für Finanztransaktionsuntersuchungen für das Berichtsjahr 2025 vorzulegen.

Mit der GwG-Meldeverordnung hat das Bundesministerium der Finanzen im September 2025 klare bundeseinheitliche Standards für Form und Inhalt von Verdachtsmeldungen geschaffen. Sie verbessert die Qualität der Datengrundlage für die FIU und damit die Voraussetzungen wirksamer Analysen. Den Verpflichteten, die sich am Konsultationsverfahren beteiligt haben, gebührt Dank für ihre Beiträge zur praxistauglichen Ausgestaltung.

Der risikobasierte Ansatz hat sich im Berichtsjahr als Leitmotiv unserer Arbeit weiter verfestigt. Im Februar 2025 hat die Financial Action Task Force (FATF) die Bedeutung des Risk-Based Approach nochmals bestätigt. Die Schärfung unserer Analyse nach Maßgabe des Risikos verlagert den Schwerpunkt von Volumen auf Wirkung. Da wir diese Entwicklung auch mit europäischen Partner-FIUs abstimmen, berichtet die langjährige Leiterin der FIU der Niederlande, Hennie Verbeek-Kusters, im Kapitel zur internationalen Zusammenarbeit über die niederländischen Erfahrungen mit der risikobasierten Arbeitsweise.

Auch auf internationaler Ebene hat die FIU Deutschland eine neue Rolle übernommen. Bei der 31. Plenartagung der Egmont Group wurde ich zum Vizepräsidenten des Zusammenschlusses aller FIUs gewählt. Zugleich hat die europäische Anti-Geldwäschebehörde AMLA in Frankfurt am Main ihre operative Tätigkeit aufgenommen. Als Mitglied ihres Verwaltungsrats setze ich mich für eine starke Zusammenarbeit der europäischen FIUs ein.

Die Analyseeinheit »Sharks« hat im Projekt »Barakuda« gemeinsam mit dem Landeskriminalamt Sachsen und europäischen Partner-FIUs zur Bekämpfung eines international operierenden Callcenter-Betrugs mit einem Gesamtschaden von rund 8 Mio. Euro beigetragen.

Im Oktober 2025 haben wir erstmals einen FIU-Risikohinweis an die betroffenen Verpflichteten gesandt. Hiermit werden Verpflichtete ad hoc zu spezifischen Auffälligkeiten individualisiert sensibilisiert, um un-

mittelbar entsprechende Anpassungen für das eigene Meldeverhalten zu berücksichtigen. Damit erreicht die FIU die Verpflichteten gezielter als bisher und kann diese bei der Identifizierung von verdächtigen Transaktionen unterstützen. Diesen Weg werden wir fortsetzen.

Das Schwerpunktkapitel widmet sich dem Betrug als Vortat zur Geldwäsche, ein Risiko, das auch die FATF als prioritär einstuft. Am Beispiel der »Operation Chargeback«, einem der größten je aufgedeckten Fälle von Kreditkartenbetrug in Deutschland, wird gezeigt, wie Betrug und Geldwäsche in der digitalen Welt zunehmend verschmelzen.

Das Volumen der eingegangenen Verdachtsmeldungen ist im Berichtsjahr deutlich gestiegen, die Zahl der abgegebenen Analyseberichte demgegenüber zurückgegangen. Hierin schlägt sich die Schärfung des risikobasierten Ansatzes nieder: Bei wachsendem Eingang konzentriert die FIU ihre Analysekapazitäten auf Sachverhalte mit hohem Risikopotenzial. Dies führt auch zu einer Entlastung der Strafverfolgungsbehörden und schafft dort Kapazitäten für die Befassung mit Gewinnen aus schweren Straftaten. Damit leisten wir einen wichtigen Beitrag zum Ziel des GwG.

Im Berichtszeitraum wurden insgesamt 106 Sofortmaßnahmen in Form der vorübergehenden Untersagung der Durchführung auffälliger Transaktionen mit einem Gesamtvolumen von 751,8 Mio. Euro vorgenommen und damit das Eindringen potenziell inkriminierter Gelder in den legalen Wirtschaftskreislauf unterbunden.

Künftig werden wir uns noch stärker damit befassen, unsere Arbeitsabläufe zu optimieren, zu digitalisieren und Medienbrüche zu vermeiden. Wir setzen uns auch in den nächsten Jahren noch mehr für eine effektive nationale und internationale Zusammenarbeit ein.

All dies ist nur möglich dank unserer Beschäftigten, die sich tagtäglich mit großem Engagement und Fachwissen gegen Geldwäsche und Terrorismusfinanzierung einsetzen. Dafür bedanke ich mich im Namen der ganzen Leitung der FIU.

Ihr
Daniel Thelesklaf
Leiter der FIU Deutschland

Kennzahlen

1. FIU in Zahlen



Abb. 1: FIU in Zahlen 2025

Abgegebene Analyseberichte

Im Jahr 2025 hat die FIU 67.024 Analyseberichte an Empfängerbehörden abgegeben. Diese Entwicklung ist Ausdruck einer fortgesetzten Anwendung des risikobasierten Ansatzes innerhalb der FIU und einer stärkeren Konzentration auf Sachverhalte mit besonders hohem Risikopotenzial. Komplexere Sachverhalte erfordern größere Analysetiefe und einen breiteren Einsatz analytischer Werkzeuge. Daraus ergibt sich tendenziell eine geringere Anzahl von Berichten, in der Sache aber werthaltigere Übermittlungen für die Strafverfolgungsbehörden und weitere Empfänger. Dieser Prozess wird im Jahr 2026 fortgesetzt und weiter intensiviert.

Gesamtmeldeaufkommen

Nach dem Rückgang der Vorjahre ist das Gesamt-meldeaufkommen im Berichtsjahr wieder stark an-gestiegen. 374.693 Verdachtsmeldungen gingen bei der FIU ein. Bei rund 16 Prozent dieser Mel-dungen handelt es sich um sogenannte Nachmeldun-gen. Diese beziehen sich auf früher eingegangene Meldungen und liefern weitere Informationen zum Sachverhalt. Im Vergleich zu den Vorjahren blieb die Quote der Nachmeldungen konstant (2024: 16 %, 2023: 15 %). Die Zahl der im Gesamtmeldeaufkom-men enthaltenen Transaktionen stieg um rund 88 Prozent auf etwa 3,2 Millionen (2024: 1,7 Mio.).

Getragen wird der Zuwachs vor allem durch den Fi-nanzsektor. Allein aus dem Bereich der Kreditinstitute gingen 319.857 Verdachtsmeldungen ein und damit rund 49 Prozent mehr als im Vorjahr. Prägend für diese Entwicklung sind die Ausweitung von Geschäftsfel-dern und der Markteintritt neuer Verpflichteter. Knapp 60 Prozent des Zuwachses entfallen auf Verpflichtete, die zuvor nur wenige oder gar keine Meldungen ab-gegeben hatten. Hinzu kommen eine gestiegene Sen-sibilität gegenüber Geldwäscherisiken und die Weiter-entwicklung interner Monitoring-Verfahren. Innerhalb des Finanzsektors zeichnet sich zugleich eine strukturelle Verschiebung ab. Digitale Finanz-dienstleister haben ihren Anteil am Meldeaufkom-men deutlich erhöht.

Digitale Finanzdienstleister im Meldegesehehen

Digitale Finanzdienstleister werden teilweise auch als »Neobanken« bezeichnet, wobei dieser Begriff nicht gesetzlich definiert ist. Digitalen Finanzdienstleistern immanent sind eine weitgehend digitalisierte Kunden-beziehung, eine beschleunigte Kontoeröffnung sowie eine häufig grenzüberschreitende Ausrichtung. Die Zeitreihe der vergangenen vier Jahre zeigt einen deutlichen Wachstumstrend. Im Jahr 2022 entfielen rund 13 Prozent des Gesamtmeldeaufkommens auf Verpflichtete dieses Segments. Im Berichtsjahr 2025 waren es 29 Prozent. Die absolute Zahl der Verdachts-meldungen aus diesem Segment ist von rund 43.000 auf gut 108.000 angestiegen.

Jahr	Gesamtmelde-aufkommen	davon digitale Finanzdienst-leister	Anteil
2022	337.186	43.190	13 %
2023	322.590	52.289	16 %
2024	265.708	34.357	13 %
2025	374.693	108.158	29 %

Tabelle 1: Gesamtmeldeaufkommen und Anteil digitaler Finanzdienstleister 2022 – 2025

Innerhalb der 100 meldestärksten Verpflichteten des Berichtsjahres befanden sich 19 digitale Finanzdienst-leister. Diese gaben durchschnittlich mehr als doppelt so viele Meldungen pro Verpflichtetem pro Jahr ab wie

klassische Kreditinstitute in der Vergleichsgruppe. Trotz der deutlich geringeren Zahl der meldenden In-stitute tragen digitale Finanzdienstleister damit über-proportional zum Meldeaufkommen bei.

Meldegründe: Betrug und Kryptowerte prägen das Bild

Auf Vortaten und Branchen bezogen sind Betrug und Untreue bei digitalen Finanzdienstleistern der häufigste Meldungsgrund, die kryptowertbezoge-nen Auffälligkeiten folgen mit deutlichem Abstand. Glücksspiel- und Wettbezüge, bei klassischen Kredit-instituten bei dieser Betrachtung der zweithäufigste Meldungsgrund, treten bei digitalen Finanzdienst-leistern dagegen nur nachrangig auf. Die Bedeutung von Kryptowerten für das Meldewesen hatte der Jah-resbericht 2024 in seinem Schwerpunktkapitel »Im Fokus – Kryptowerte« ausführlich dargestellt. Diese ist weiterhin hoch.

Der Unterschied im Meldeprofil spiegelt die Ziel-gruppen- und Produktausrichtung der Institute wider. Digitale Finanzdienstleister sprechen in stärkerem Maße jüngere und technologieaffine Kundengruppen an, insbesondere durch die Ermöglichung krypto-wertbezogener Transaktionen. Digitalisierte Onboar-ding-Prozesse und eine hohe Dichte an Zahlungsvor-gängen machen das Segment zusätzlich anfällig für einen Missbrauch zu Betrugszwecken. Das überpro-portionale Meldeaufkommen ist vor diesem Hinter-grund nicht allein Ausdruck gestiegener Sensibilität auf Seiten der Verpflichteten. Es zeigt auch eine er-höhte Risikoexposition.

Einordnung

Es lässt sich festhalten, dass digitale Finanzdienst-leister innerhalb weniger Jahre von einem Nischen-segment des Meldegesehens zu einer tragenden Säule neben den klassischen Kreditinstituten gewor-den sind. Für die FIU ergibt sich daraus eine doppel-te Aufgabe. Erstens die risikogerechte Priorisierung eines Meldungsaufkommens, das in diesem Segment deutlich überdurchschnittlich wächst. Zweitens die Begleitung und Weiterentwicklung der Meldepraxis durch zielgerichtete Dialogformate mit den Ver-pflichteten.

»Digitale Finanzdienstleister sind innerhalb weniger Jahre von einem Nischensegment des Meldesgeschehens zu einer tragenden Säule neben den klassischen Kreditinstituten geworden.«

Nichtfinanzsektor

Gegen den Trend im Finanzsektor ist das Meldeaufkommen des Nichtfinanzsektors auf 9.006 Verdachtsmeldungen zurückgegangen und hat sich damit gegenüber dem Vorjahr um knapp 14 Prozent verringert. Niedrigere Meldezahlen verzeichnen vor allem Notare und Immobilienmakler. Ein wesentlicher Zusammenhang besteht mit der am 17. Februar 2025 in Kraft getretenen geänderten Fassung der Geldwäschegesetzmeldepflichtverordnung-Immobilien (GwGMeldV-Immobilien: vgl. 3.1.2). Die Änderung der Verordnung dient dazu, Geldwäsche im Immobiliensektor noch zielgerichteter zu bekämpfen. Neben der Erweiterung von meldepflichtigen Sachverhalten wurden hierfür Tatbestände durch klare Schwellenwerte konkretisiert und zu weit gefasste Tatbestände eingeschränkt. So sind Drittzahlungen erst ab 20.000 Euro und Verkehrswertabweichung in der Regel erst ab mehr als 25 Prozent meldepflichtig. Daneben wurde unter anderem der Schwellenwert für Vorabzahlungen auf 20.000 Euro angehoben und der Zeitraum für auffällige Weiterverkäufe von drei auf zwei Jahre reduziert. Hierdurch konnten Unsicherheiten bei der Meldepflicht deutlich reduziert und die Meldepflicht insoweit konturiert werden.

Sofortmaßnahmen

Anzahl und angehaltenes Gesamtvolumen der Sofortmaßnahmen haben im Berichtsjahr ihren Höchststand erreicht. Die Ursachen beider Entwicklungen sind jeweils eigener Natur. Der Anstieg bei der Zahl der Maßnahmen geht vorwiegend auf grenzüberschreitende Betrugsfälle zurück. 55 der insgesamt 106 Sofortmaßnahmen folgten internationalen Hin-

weisen und lösten jeweils eine Vielzahl von Einzelanordnungen bei mehreren Verpflichteten aus. Das außergewöhnlich hohe Gesamtvolumen geht vor allem auf eine einzelne Maßnahme zurück, mit der die Verfügung über 585 Mio. Euro untersagt wurde. Beide Entwicklungen stehen zugleich im Zusammenhang mit der zuvor beschriebenen größeren Analysetiefe, da die vertiefte Bearbeitung komplexer Sachverhalte vermehrt Ansatzpunkte für die Sicherung inkrimierter Vermögenswerte liefert.

Staatsanwaltschaftliche Rückmeldungen

In Strafverfahren, zu denen die FIU Informationen übermittelt hat, teilt die zuständige Staatsanwaltschaft der FIU die Erhebung der öffentlichen Klage und den Ausgang des Verfahrens einschließlich aller Einstellungsentscheidungen mit (§ 42 Absatz 1 GwG). Im Berichtsjahr gingen 41.743 solcher Rückmeldungen bei der FIU ein. Die Zahl bewegt sich damit auf dem Niveau des Vorjahres (41.821). Von den 41.743 Rückmeldungen betreffen 1.669 Urteile, Strafbefehle, Beschlüsse oder Anklageschriften. Einstellungsverfügungen bilden mit rund 96 Prozent weiterhin den größten Anteil. Dies bedeutet nicht, dass keine Ergebnisse erzielt wurden. Die Informationen der FIU werden regelmäßig zur Verfolgung der Vortat genutzt. Die Rückmeldungen bilden für die FIU eine maßgebliche Grundlage, um die Verwendungsbreite und den Mehrwert ihrer Analyseergebnisse nachzuhalten und die Analyseprozesse an den Bedarfen der Strafverfolgungsbehörden auszurichten.

Nationale Ersuchen

Im Rahmen der behördlichen Zusammenarbeit stellt die FIU Daten aus Finanzinformationen und Finanzanalysen zur Verfügung, sofern diese für die Aufgabenerfüllung der ersuchenden Behörde im Zusammenhang mit der Verhinderung und Verfolgung von Geldwäsche und Terrorismusfinanzierung erforderlich sind (§ 32 Absatz 3 GwG). Strafverfolgungsbehörden sowie das Bundesamt für Verfassungsschutz (BfV) sind nach § 32 Absatz 4 GwG zudem berechtigt, Daten zur Erfüllung ihrer Aufgaben automatisiert bei der FIU abzurufen. Eine entsprechende Schnittstelle steht seit 2022 zur Verfügung. Immer mehr abrufberechtigte Behörden schließen sich dem automatisierten Abruf

an. Im Berichtsjahr erreichte die Zahl der automatisierten Abrufe 51.756 und lag damit rund 58 Prozent über dem Vorjahreswert. Der automatisierte Abruf beschleunigt den behördlichen Informationsaustausch und entlastet sowohl die abrufenden Behörden als auch die FIU von manuellen Auskunftersuchen.

In der Folge ist die Zahl der schriftlich gestellten Auskunftersuchen weiter zurückgegangen. Sie belief sich im Berichtsjahr auf 3.607 Ersuchen. Der Rückgang entspricht dem Trend des Vorjahres und spiegelt den erreichten Automatisierungsgrad wider.

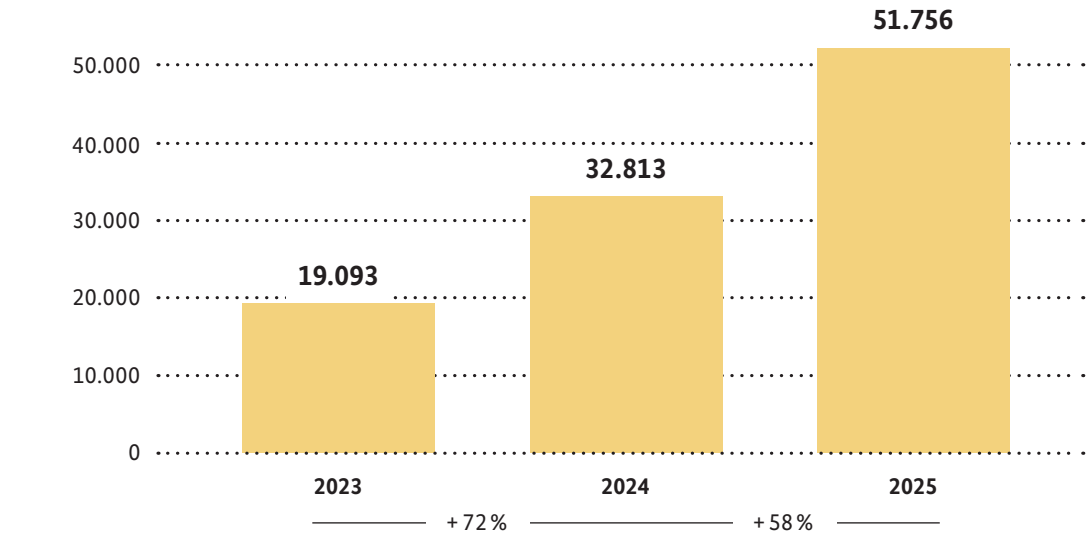


Abb. 2: Anzahl der automatisierten Abrufe (2023 – 2025)

Internationale Ersuchen

Bei der FIU gingen im Berichtsjahr 1.052 Ersuchen aus dem Ausland ein (Vorjahr: 1.029). Die Zahl der eingehenden Ersuchen bleibt damit auf dem Vorjahresniveau. Die Zahl der ausgehenden Ersuchen an Partner-FIUs ist mit 1.361 gegenüber dem Vorjahr (1.541) leicht zurückgegangen.

Neu registrierte und aktive Verpflichtete

Im Jahr 2025 haben sich 10.737 Verpflichtete neu bei der FIU registriert. Der deutliche Unterschied gegenüber dem Vorjahr (98.810) stand im Zusammenhang mit der ab dem 1. Januar 2024 geltenden verpflichtenden Registrierung bei der FIU (§ 45 Absatz 1 Satz 2 i.V.m. § 59 Absatz 6 Satz 1 GwG). Diese Nachholeffekte sind weitgehend abgeschlossen. Die Zahl der aktiven Verpflichteten lag im Berichtsjahr bei 4.062 und ist damit nahezu unverändert geblieben.

Im Fokus

2. Im Fokus: Betrug – »Operation Chargeback«

Betrug ist längst kein Randphänomen der Finanzkriminalität mehr. Laut der Financial Action Task Force (FATF) zählt cybergestützter Betrug inzwischen zu den verbreitetsten und schadensträchtigsten Formen gewinnorientierter Kriminalität weltweit. In 156 der von der FATF bewerteten Jurisdiktionen, also in rund 90 Prozent aller Fälle, wird Betrug als wesentliche Bedrohung eingestuft. Deshalb betrachtet die FATF das Thema mittlerweile als strategischen Schwerpunkt.

Diese Einordnung trifft auf eine Realität, die sich auch in der Analysearbeit der FIU abbildet. Betrugsnetzwerke operieren häufig grenzüberschreitend. Sie nutzen professionelle Infrastrukturen und verschleiern die Herkunft der Erlöse über komplexe Strukturen. Die Grenzen zwischen Vortat und Geldwäsche verschwimmen, insbesondere dort, wo Täter die Zahlungsinfrastruktur selbst als Instrument des Betrugs einsetzen.

Die folgende Fallkonstellation zeigt exemplarisch, wie sich diese Entwicklung in einem konkreten Sachverhalt mit Bezug zum Finanzplatz Deutschland darstellt. Die Operation Chargeback, die am 4. November 2025 in einem koordinierten internationalen Aktionstag mündete, gilt als einer der bedeutendsten je aufgedeckten Fälle von Kreditkartenbetrug in Deutschland. Geführt wird das Ermittlungsverfahren von der Landeszentralstelle Cybercrime (LZC) der Generalstaatsanwaltschaft (GenStA) Koblenz und dem Bundeskriminalamt (BKA). Die FIU hat die strukturellen Muster dieses Phänomenbereichs initial erkannt und über mehrere Jahre hinweg analytisch erschlossen sowie ihre Erkenntnisse in den Ermittlungskomplex eingebracht. Insgesamt hat die FIU in diesem Zusammenhang rund 14 Millionen Transaktionen analysiert.

Betrug in industriellem Ausmaß

Die kriminellen Netzwerke, die im Zentrum der Operation Chargeback standen, operierten zwischen 2016 und 2021. Ihr Geschäftsmodell war darauf ausgelegt, unter dem Radar klassischer Kontrollmechanismen zu bleiben. Anstatt große Einzelbeträge abzubuchen, erzeugten die Netzwerke rund 19 Millionen fingier-

te Online-Abonnements für Erwachsenenunterhaltung, Dating-Plattformen und Streaming-Dienste. Die monatlichen Abbuchungen bewegten sich typischerweise bis zu rund 50 Euro. Viele Karteninhaber bemerkten den Betrag nicht sofort oder ordneten ihn zunächst einem vergessenen Abonnement zu. Der Sachverhalt ist innerhalb der europäischen Betrugsermittlungen herauszuheben: Über 4,3 Millionen Kreditkarteninhaber in 193 Ländern sind betroffen. Der geschätzte Gesamtschaden übersteigt 300 Mio. Euro. Die versuchten Schäden, also Fälle, in denen die Täter Abonnements generierten, aber keine Belastung der Kreditkarte möglich war, weil die Karte z. B. abgelaufen war, belaufen sich auf rund 750 Mio. Euro. Aus durchgeführten und versuchten Transaktionen ergibt sich damit ein kumulierter Betrag von über einer Milliarde Euro.

Zur Verschleierung ihrer Aktivitäten nutzten die Netzwerke eine professionelle Infrastruktur. Zahlreiche Briefkastenfirmen, vornehmlich in Großbritannien und Zypern registriert, dienten dazu, die betrügerischen Transaktionen auf verschiedene Unternehmen zu verteilen und so das Risiko einer Entdeckung durch Chargeback-Verfahren der Kartenunternehmen zu minimieren. Diese Firmenstrukturen wurden über sogenannte Crime-as-a-Service-Anbieter bezogen, die komplette Unternehmensstrukturen einschließlich vorgeschobener Geschäftsführer und Know-Your-Customer-Dokumente lieferten.

Modus operandi

Die Geschäftsmodelle, die über die Scheinhändler abgewickelt wurden, folgten einem wiederkehrenden Muster. Nutzerinnen und Nutzer wurden auf Webseiten gelockt, die auf den ersten Blick ein konkretes Angebot versprachen und bei genauerer Betrachtung kaum Substanz aufwiesen. Beobachtet wurden unter anderem »Flatrate Photo Services«, sogenannte »Brain Train Games«, Streaming-Angebote unbekannter Herkunft sowie vage beschriebene »Budgetplaner«. Die Angebote folgten einem vergleichbaren Muster. Eine kurze Probemitgliedschaft von wenigen Tagen bis zu zwei Wochen für regelmäßig unter einem Euro ver-

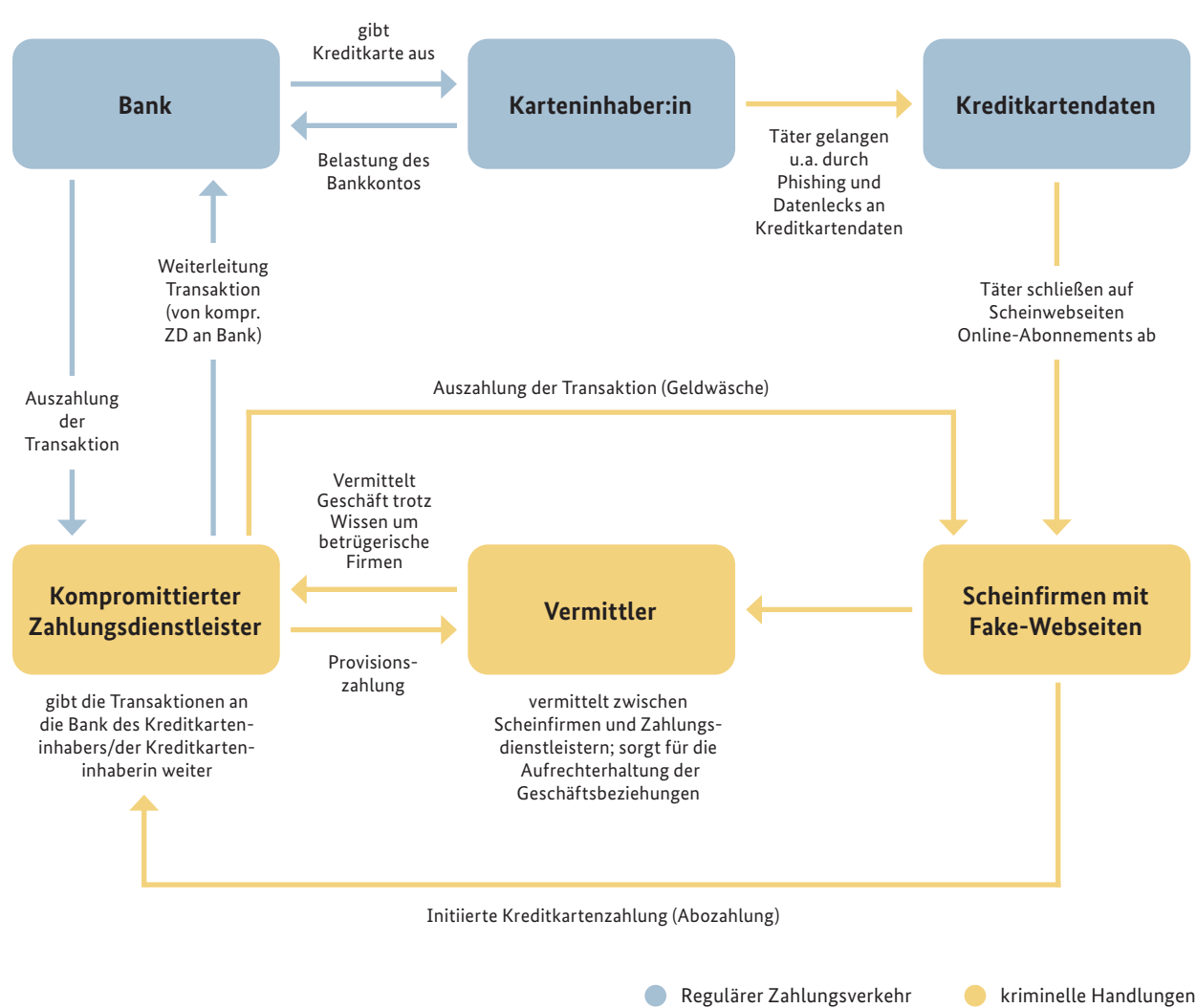


Abb. 3: Modus Operandi der Beschuldigten

längerte sich automatisch in ein kostenpflichtiges Monatsabonnement im mittleren zweistelligen Euro-Bereich, sofern der Nutzer nicht aktiv kündigte. Die Funktionalität der Webseiten beschränkte sich in der Regel auf die Registrierung und den Abschluss des Abonnements. Substanzielle Angaben zu Inhalten, Beispielmateriale oder Probeinhalten fehlten. Logos, Nutzerbewertungen und gelistete Gewinner waren auf unterschiedlichen Portalen identisch. Dieser Abrechnungsmechanismus ist in der Branche als »negative billing« bekannt. Die Kombination aus niedrigem Einstiegspreis, fehlender klarer Preiskommunikation und automatischer Verlängerung erhöht die Wahrscheinlichkeit, dass Abbuchungen über längere Zeit unbemerkt bleiben. Die Zuleitung auf diese Portale erfolgte häufig über

gezielte Täuschungen. Betroffene berichteten regelmäßig von Kurznachrichten, in denen eine angebliche Paketzustellung angekündigt und eine geringe Zustellgebühr verlangt wurde. Der in der Nachricht enthaltene Link führte auf eine Webseite, die den Auftritt bekannter Paketdienstleister nachbildete und am Ende die Eingabe der Kreditkartendaten verlangte. In anderen Fällen wurden Gewinnspiele im Namen bekannter Handelsmarken suggeriert, bei denen lediglich die Versandkosten für einen vermeintlichen Gewinn über die Kreditkarte zu zahlen waren. In beiden Varianten führte die Eingabe der Daten nicht zum angekündigten Vorgang, sondern zum versteckten Abschluss eines der beschriebenen Abonnements. Die Erlöse flossen anschließend in die regulierte Zahlungsinfrastruktur, über die sie weiterverteilt und abgebogen wurden.

Die Rolle der Zahlungsdienstleister

Ein strukturell aufschlussreiches Element des Sachverhalts war die mutmaßliche Beteiligung von Insidern aus dem Finanzsektor. Sechs Personen, darunter Führungskräfte und weitere Mitarbeiter von vier deutschen Zahlungsdienstleistern, stehen im Verdacht, den Netzwerken gegen finanzielle Gegenleistungen Zugang zur Zahlungsinfrastruktur verschafft zu haben. Der Umstand zeigt ein strukturelles Risiko. Wenn Kontrollinstanzen innerhalb des Finanzsektors kompromittiert werden, können klassische Präventionsmechanismen unterlaufen werden. Zugleich lässt sich dem Sachverhalt entnehmen, dass die Meldepflichten auf Seiten der Verpflichteten in Teilen gegriffen haben. Die beteiligten Zahlungsdienstleister hatten in den Jahren vor dem internationalen Zugriff bereits eine dreistellige Zahl von Verdachtsmeldungen zu einzelnen Händlern erstattet, ein Teil davon konzentriert in den Jahren 2021 und 2022. Parallel hat einer der beteiligten Dienstleister im Rahmen eigener interner Prüfungen die Geschäftsbeziehung zu einem Großteil der betroffenen Händler beendet. Die Fälle wurden sichtbar. Ihre systemische Dimension ließ sich jedoch erst erkennen, als die Einzelmeldungen in der FIU zu einem Gesamtbild zusammengeführt wurden. Genau an dieser Stelle liegt die Zentralstellenfunktion nach § 27 GWG.

Muster: Transaction Laundering

Über die Phasen der Bearbeitung hinweg verdichtete sich ein Muster, das international als »Transaction Laundering« bezeichnet wird. Im Kern werden dabei nicht oder nur eingeschränkt legale Zahlungsvorgänge über scheinbar legitime Händlerkonten abgewickelt und auf diese Weise in die regulierte Zahlungsinfrastruktur eingespeist. Anders als beim klassischen Geldwäschezyklus, der die Erlöse einer Vortat nachgelagert in den Finanzkreislauf überführt, liegen die betrügerische Abbuchung und die Einspeisung der Beträge in legal wirkende Handelsströme zeitlich und strukturell eng beieinander. Ein hiervon deutlich abgrenzbarer, nachgelagerter Schritt zur Verschleierung der Mittelherkunft kann dabei regelmäßig schwer feststellbar sein. Tragende Struktur dieses Modells innerhalb der Operation Chargeback waren »phony merchants«, also Scheinhändler, die nach außen eigenständige Ge-

schäftsmodelle vorgaben, tatsächlich aber als Durchlaufstationen für betrügerisch erlangte Zahlungen dienten. Charakteristisch waren Gesellschaften in britischer, zypriotischer oder maltesischer Rechtsform, überwiegend als Limited, mit Geschäftsleitungen aus Großbritannien, Zypern und osteuropäischen Staaten. Die eingetragenen Sitze lagen häufig an Privatadressen oder in virtuellen Büros. Mehrere Gesellschaften waren auf identische Gründungsadressen in virtuellen Büros zurückzuführen. Die Firmengründungen verliefen über spezialisierte Dienstleister nach dem Muster des »Crime-as-a-Service«. Vollmachten und Gesellschaftsverträge dienten zur Abschirmung der tatsächlich wirtschaftlich Berechtigten. Zwischen den Scheinhändlern und den Zahlungsdienstleistern agierten spezialisierte Vermittler, die als Acquisiteure von Händlerportfolios auftraten und für ihre Dienstleistung umsatzabhängige Provisionen erhielten. Gerade diese Zwischenebene erschwerte die risikobasierte Bewertung der Geschäftsbeziehung, weil die Zahlungsdienstleister die tatsächlichen wirtschaftlichen Hintergründe der einzelnen Händler häufig nur mittelbar erfassten.



Operation Chargeback auf einen Blick

- Tatzeit:** 2016 – 2021
- Aktionstag:** 4. November 2025
- Betroffene:** über 4,3 Millionen Kreditkarteninhaber in 193 Ländern
- Geschätzter Schaden:** über 300 Mio. Euro
- Beteiligte Länder am Aktionstag:** 10 (Deutschland, USA, Kanada, Singapur, Luxemburg, Zypern, Spanien, Italien, Niederlande, Großbritannien)
- Ermittlungsleitung:** Landeszentralstelle Cybercrime der GenStA Koblenz und BKA
- Festnahmen:** 21, davon 5 in Deutschland
- Durchsuchungen:** über 80
- Gesicherte Vermögenswerte:** über 75 Mio. Euro (Deutschland und Luxemburg)



Abb. 4: Typischer Ablauf einer Abofalle

Die analytische Vorarbeit der FIU

Der Operation Chargeback ging eine mehrjährige Analyse der FIU voraus. Ausgangspunkt waren im Jahr 2020 Verdachtsmeldungen eines deutschen Kreditinstituts zu auffälligen Transaktionen über die Sammeltreuhandkonten zweier inländischer Zahlungsdienstleister. Im Meldeaufkommen verdichteten sich rund 68.500 Transaktionen mit einem Gesamtvolumen von mehr als 77 Mio. Euro, die sich auf rund 280 Empfängerkonten bei drei Bankinstituten verteilten und mehr als 600 Entitäten betrafen. Was als isolierter Ankerpunkt begann, entwickelte sich in mehreren Analysephasen zu einem der umfangreichsten Analysekomplexe der FIU der vergangenen Jahre. Ein entscheidender Schritt war die intensive Kooperation mit der FIU Luxemburg, mit der die deutsche FIU Zahlungsströme bilateral abglich, bereits identifizierte Scheinhändler austauschte und einen stetigen Austausch etablierte. Parallel dazu bearbei-

tete die FIU eine Vielzahl eingehender Ersuchen aus weiteren Jurisdiktionen zu Personen und Zahlungsflüssen aus diesem Kontext und stimmte sich eng mit der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ab. Die quantitative Dimension der Analyse verdeutlicht die Anforderungen, die ein solcher Sachverhalt an eine zentrale Meldestelle stellt. Aus der Gesamtmenge der erkannten Entitäten bildete die FIU eine Stichprobe von 29 Gesellschaften für die Vertiefung. Mehr als 400 Konten bei den involvierten Bankinstituten wurden in die Auswertung einbezogen, rund 14 Millionen Einzeltransaktionen, darunter umfangreiche Kreditkartenumsätze, wurden systematisch ausgewertet. Die FIU richtete Auskunftersuchen an 19 ausländische Partner-FIUs und beantwortete selbst eine Vielzahl von Ersuchen aus dem internationalen Egmont-Netzwerk. Die 29 Gesellschaften betrieben insgesamt rund 280 Webseiten, überwiegend Dating- und Erwachsenenplattformen.



Glossar zum Fall:

Briefkastenfirma	Gesellschaft ohne eigene operative Substanz, in der Regel ohne eigenes Personal und eingetragen an der gleichen Adresse wie viele andere Gesellschaften. Im Kontext von Transaction Laundering dient sie häufig als Vehikel für betrügerische Zahlungsabwicklung.
Chargeback	Rückbuchung einer Kreditkartenzahlung, die ein Karteninhaber nach unberechtigter Abbuchung oder nicht erbrachter Leistung beim kartenausgebenden Institut geltend machen kann.
Crime-as-a-Service (CaaS)	Kriminelles Dienstleistungsmodell, bei dem spezialisierte Anbieter Bausteine krimineller Geschäftsmodelle, etwa vorkonfektionierte Gesellschaften, gefälschte Identitätsdokumente oder Zugänge zu Zahlungsinfrastrukturen, gegen Entgelt bereitstellen. Das Modell senkt die Einstiegshürden für Finanzkriminalität und erschwert die Zuordnung von Taten zu ihren Urhebern.
High Risk Merchant	Händlerkategorie mit statistisch erhöhtem Risiko von Rückbuchungen und betrügerischen Vorgängen, häufig aus Branchen wie Adult Entertainment, Dating, Gaming oder ausgewählten Gesundheitsprodukten.
Know Your Customer (KYC)	Kundensorgfaltspflichten, die Verpflichtete zum Beispiel zur Identifizierung und Überprüfung ihrer Kunden durchführen müssen. Im vorliegenden Fall wurden KYC-Dokumente verfälscht, um Briefkastenfirmen als legitime Unternehmen erscheinen zu lassen.
OSINT (Open Source Intelligence)	Systematische Erhebung und Auswertung öffentlich zugänglicher Informationen, etwa aus Webseiten, Registern und sozialen Medien. Im vorliegenden Fall diente sie der Untersuchung der Schein-Webseiten und der dahinterstehenden Gesellschaften.
Negative Billing	Vertragsgestaltung, bei der eine günstige Probemitgliedschaft automatisch in ein kostenpflichtiges Abonnement übergeht, sofern der Nutzer nicht aktiv kündigt.
Phony Merchant	Scheinhändler ohne reale wirtschaftliche Tätigkeit, dessen Händlerkonto ausschließlich der Abwicklung betrügerischer oder anderweitig illegaler Zahlungen dient.
Transaction Laundering	Abwicklung von Zahlungen über scheinbar legitime Händlerkonten unter Verschleierung des tatsächlichen Verkäufers oder des wahren Geschäftszwecks. Die einzelnen Zahlungsvorgänge können dabei für sich genommen legal sein.
Zahlungsdienstleister (Payment Service Provider)	Im vorliegenden Fall Unternehmen, die Zahlungstransaktionen zwischen Händlern und Karteninhabern abwickeln. Der gesetzliche Begriff des Zahlungsdienstleisters nach § 1 ZAG ist weiter gefasst.

Neben der Auswertung der Bank- und Kreditkartendaten stützte sich die Analyse auf systematische OSINT-Recherchen (Open Source Intelligence, die systematische Auswertung öffentlich zugänglicher Quellen) zu den Webseiten und Gesellschaften. Auffällig waren wiederkehrende technische Gestaltungsmerkmale. Die Webseiten wiesen weitgehend identische Menüführungen und Textinhalte auf, die in Webseiten-Programmierung hinterlegten Anweisungen verhinderten die Indexierung durch Suchmaschinen, Gewinnerlisten und Nutzerbewertungen waren portalübergreifend identisch. Typologisch wies dies auf statische, nicht tatsächlich betriebene Angebote hin, deren einzige wirtschaftliche Funktion im Betrieb des Abonnementabrechnungssystems bestand.

Strafverfolgung und aufsichtsrechtliche Folgemaßnahmen

Im Jahr 2022 übergab die FIU den Analysekomplex an die LZC der GenStA Koblenz und unterstützte die anschließenden Ermittlungen fortlaufend mit Finanzinformationen und Folgeauswertungen. Parallel dazu prüfte die Bafin die beteiligten inländischen Zahlungsdienstleister im Rahmen von Sonderprüfungen. Die aufsichtsrechtlichen Maßnahmen reichten vom Neukundenverbot über die Bestellung von Sonderbeauftragten bis zu einem Transaktionsverbot im Hochrisikogeschäftsbereich. In Folge der Einstellung der betroffenen Geschäfte durch die beteiligten Zahlungsdienstleister wurden keine weiteren Verdachtsmeldungen mehr notwendig, wodurch der fortlaufende Zustrom weiterer Verdachtsmeldungen aus diesem Phänomenbereich unterblieb.

Internationaler Zugriff

Am 4. November 2025 führten Ermittlungsbehörden in zehn Ländern koordinierte Maßnahmen durch. Die Operation wurde von der LZC der GenStA Koblenz und dem BKA geleitet und durch Europol und Eurojust unterstützt. Mehr als 80 Durchsuchungen wurden durchgeführt und 21 Haftbefehle vollstreckt, darunter fünf in Deutschland. Im Vorfeld waren über 90 Rechtshilfeersuchen an 30 Länder gestellt worden. In Deutschland und Luxemburg wurden Vermögenswerte in Höhe von über 75 Mio. Euro gesichert. Die Beschuldigten werden unter anderem des gewerbsmäßigen Computerbetrugs, der Mitgliedschaft

in einer kriminellen Vereinigung und der Geldwäsche beschuldigt.

Erkenntnisse für die Geldwäschebekämpfung

Die Operation Chargeback steht exemplarisch für eine Entwicklung zur Industrialisierung des Betrugs und seine Verschränkung mit Geldwäsche. Der Fall zeigt, dass Betrugserlöse in erheblichem Umfang über regulierte Zahlungskanäle fließen. Diese Kanäle dienten nicht der Verschleierung der Mittelherkunft, sondern unmittelbar der Begehung des Betrugs. Die Täter nutzten keine Parallelstrukturen, sondern die bestehende Zahlungsinfrastruktur, einschließlich regulierter deutscher Zahlungsdienstleister. Wirksame interne Kontrollen bei den Verpflichteten und gezielte Maßnahmen gegen Schwachstellen in der Compliance bleiben zentral. Dabei ist die Rolle der Zwischenebene aus Vermittlern und Portfolio-Anbietern von besonderer Bedeutung, insbesondere dort, wo Händlerbeziehungen nicht direkt, sondern über spezialisierte Vertriebsstrukturen begründet werden. Der Sachverhalt bestätigt zudem die Relevanz des Crime-as-a-Service-Modells für die Geldwäschebekämpfung. Die Beschaffung von Firmenmänteln, formal eingesetzten Strohpersonen (sogenannten Nominees) und Zahlungsdienstleistungen über spezialisierte Anbieter erschwert die Zuordnung von Transaktionen zu den eigentlichen Tätern. Klassische Risikoindikatoren wie Unternehmenssitz, Gesellschaftsform oder eingetragene Geschäftsführung verlieren an Aussagekraft, wenn diese Merkmale industriell erzeugt werden. Die mehrjährige Bearbeitung in der FIU unterstreicht schließlich, dass Sachverhalte dieses Zuschnitts nicht aus einer einzelnen Verdachtsmeldung, sondern nur durch die systematische Zusammenführung von Informationen aus verschiedenen Quellen sichtbar werden. Meldungen mehrerer Verpflichteter, behördliche Hinweise, Spontaninformationen ausländischer Partner-FIUs und Open-Source-Recherchen greifen ineinander. Gerade bei Betrugsschemata, die gezielt unterhalb der Aufmerksamkeitsschwelle operieren, entsteht das Gesamtbild erst im Zusammenspiel dieser Informationsstränge. Die internationale Kooperation, zuerst im bilateralen Austausch mit der FIU Luxemburg und später im erweiterten Kreis von



FIU-Analyse in Zahlen

- Bearbeitungszeitraum:** 2020–2023
- Analysephasen:** 5 (Ankerpunkt, aufsichtsrechtliche Signale, Kooperation FIU Luxemburg, vertiefte Analyse, Übergabe Strafverfolgung)
- Ausgewertete Entitäten (Stichprobe):** 29
- Ausgewertete Konten:** über 400
- Ausgewertete Einzeltransaktionen:** rund 14 Millionen
- Beteiligte Partner-FIUs:** 19
- Betroffene Webseiten:** rund 280

Perspektive

»Cyber-enabled Fraud« wird die Geldwäschebekämpfung über die kommenden Jahre prägen. Die FATF hat das Thema zu einem strategischen Schwerpunkt erhoben. Internationale Partnerinstitutionen haben ihre analytischen Kapazitäten in diesem Bereich sichtbar ausgebaut. Für die FIU folgen daraus mehrere Linien der Weiterentwicklung. Zum einen gewinnt die systematische Zusammenführung von Transaktionsdaten, Kreditkartenumsätzen und Kryptotransaktionen in einem gemeinsamen Analysezugang weiter an Bedeutung. Zum anderen werden Sachverhalte mit industriell erzeugten Firmenstrukturen zukünftig stärker in strategischen Auswertungen abgebildet, die über den Einzelfall hinaus typisierte Muster beschreiben. Die internationale Zusammenarbeit im Egmont-Netzwerk und im Rahmen der AMLA sorgt künftig verstärkt dafür, dass grenzüberschreitende Betrugsnetzwerke sichtbar werden.

19 beteiligten Jurisdiktionen, war für den analytischen Durchbruch ebenso entscheidend wie die anschließende Zusammenarbeit mit den Ermittlungsbehörden.

Betrug im Fokus der internationalen Gemeinschaft

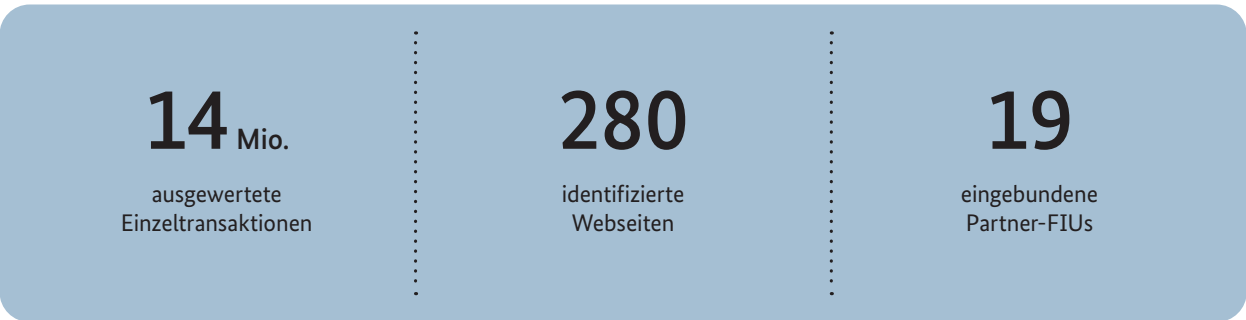
Die Operation Chargeback steht nicht isoliert. Sie fügt sich in eine Reihe internationaler Initiativen ein, die Betrug als eigenständiges und wachsendes Risiko für die Integrität des Finanzsystems adressieren. Die FATF hat im Februar 2026 mit ihrem Bericht zu cybergestütztem Betrug erstmals umfassend dargelegt, wie die bestehenden FATF-Standards zur Bekämpfung dieser Kriminalitätsform eingesetzt werden können. Der Bericht identifiziert drei prioritäre Handlungsfelder, nämlich die Stärkung der innerstaatlichen Koordination zwischen öffentlichem und privatem Sektor, den Ausbau der multilateralen internationalen Zusammenarbeit sowie die Verbesserung von Erkennung und Prävention. Die FATF hebt dabei die Rolle der FIUs hervor. Einige FIUs haben bereits Verfahren des maschinellen Lernens auf Transaktionsdatensätze angewandt, um Anomalien im Zusammenhang mit Betrug zu erkennen. Die FIU Deutschland hat mit dem Aufbau datenbasierter Analyseverfahren (vgl. 4.2) frühzeitig ein Instrument aufgebaut, das in diese Richtung weist. Flankierend sensibilisiert die FIU die Verpflichteten mit dem neu eingeführten FIU-Risikohinweis (vgl. 5.3) gezielt für aktuelle Typologien, einschließlich Betrugsmuster.

Operation Chargeback in Zahlen

Schaden und Reichweite



FIU-Analyse 2020 – 2023



Aktionstag 4. November 2025



Abb. 5: Kennzahlen der Operation Chargeback

Entwicklungen

3. Entwicklungen

Die FIU nimmt gemäß § 27 Absatz 1 GwG die Rolle der nationalen Zentralstelle für die Verhinderung, Aufdeckung und Unterstützung bei der Bekämpfung der Geldwäsche und Terrorismusfinanzierung wahr. Sie führt im Vorfeld eines strafrechtlichen Anfangsverdachts operative und strategische Finanzanalysen durch. Dies umfasst auch qualifizierte, eigenständige strategische Auswertungen zu aktuellen Phänomenen.

Das Berichtsjahr 2025 war von Weichenstellungen auf mehreren Feldern geprägt: von der Schaffung eines bundeseinheitlichen Rechtsrahmens für das Meldewesen (3.1) über eine neue Qualität des Dialogs mit Verpflichteten und Partnerbehörden im Inland (3.2) bis zur deutlich vertieften internationalen Zusammenarbeit mit dem operativen Start der AMLA und der Vizepräsidentschaft in der Egmont Group (3.3). Die beschleunigte technologische Weiterentwicklung der FIU wird in Kapitel 4 (Digitalisierung und Technologie) im Zusammenhang mit den datengestützten Analyseverfahren dargestellt.

3.1 Rechtlicher Rahmen und Meldewesen

Das Berichtsjahr 2025 war von einer Reihe regulatorischer Weichenstellungen geprägt, die den rechtlichen Rahmen für das Meldewesen und die Analysearbeit der FIU wesentlich weiterentwickelt haben. Im Zentrum stand der Erlass der Verordnung über die Form und die erforderlichen Angaben bei der Meldung von Sachverhalten nach dem Geldwäschegesetz (GwGMeldV), mit der bundeseinheitliche Standards für Form und Inhalt von Verdachtsmeldungen an die FIU geschaffen wurden. Flankiert wurde diese Entwicklung durch eine Änderung der Geldwäschegesetzmeldepflichtverordnung-Immobilien sowie durch mehrfache Aktualisierungen der Auslegungs- und Anwendungshinweise der Bafin. Die gemeinsame Fortschreibung der Orientierungshilfe zu den Begriffen der »Unverzüglichkeit« und »Vollständigkeit« einer Verdachtsmeldung nach § 43 GwG ist

ausführlich unter 3.2.4 dargestellt. Parallel haben auf europäischer und internationaler Ebene die EU-Geldwäscheverordnung (EU-AMLR) und die FATF-Standards zum risikobasierten Ansatz das Arbeitsumfeld der FIU und der Verpflichteten mitgeprägt. Die FIU hat diese Prozesse aktiv mitgestaltet. Leitgedanke war die Verbesserung der Qualität der Datengrundlage und damit die Schaffung der Voraussetzungen für wirksamere Analysen.

3.1.1 GwG-Meldeverordnung

Die Übermittlung von Verdachtsmeldungen an die FIU erfolgte bereits vor Erlass der Verordnung elektronisch über das von ihr im Internet bereitgestellte IT-Verfahren goAML. Verbindliche und detaillierte Vorgaben zu Form und Inhalt der elektronischen Meldung bestanden bis dahin jedoch nicht. Die Meldungsqualität hing im Wesentlichen von den internen Standards der jeweiligen Verpflichteten ab. Dies führte zu deutlichen Qualitätsunterschieden bei den gegenüber der FIU erstatteten Verdachtsmeldungen.

Bundeseinheitliche Standards für das Meldewesen

§ 45 Absatz 5 GwG ermächtigt das Bundesministerium der Finanzen (BMF), durch Rechtsverordnung nähere Bestimmungen über die Form der Meldung und über mögliche weitere zulässige Übertragungswege zu erlassen. Mit dem Finanzmarktdigitalisierungsgesetz (FinmadiG) trat am 31. Dezember 2024 eine Ergänzung der Ermächtigung in Kraft (§ 45 Absatz 5 GwG), die klarstellt, dass neben Vorgaben zur Form auch Bestimmungen zu den erforderlichen Angaben einer Meldung getroffen werden können. Auf diesen Grundlagen wurde zwischen Januar und März 2025 ein Verordnungsentwurf erarbeitet. Im April 2025 führte das BMF ein Konsultationsverfahren durch, das die Anhörung der Länder und die Beteiligung der Verbände umfasste. 40 Stellungnahmen gingen ein, deren Hinweise vielfach berücksichtigt werden konnten. Die GwGMeldV wurde am 1. Sep-

tember 2025 im Bundesgesetzblatt verkündet (BGBl. 2025 I Nr. 200) und ist am 1. März 2026 in Kraft getreten.

Die Verordnung regelt verbindlich und im Detail, in welcher Form und mit welchen Angaben Verdachtsmeldungen an die FIU zu übermitteln sind. Kernelement ist die elektronische Übermittlung über goAML im XML-Format. Die Verordnung setzt inhaltliche Mindestanforderungen an die Meldung, insbesondere zu Meldegründen, Sachverhaltsdarstellung und Dokumentation, und schreibt detaillierte Angabepflichten für bestimmte Sachbereiche fest, sofern derlei Informationen im Zeitpunkt der Meldeerstattung beim Verpflichteten vorliegen und für die Sachverhaltsdarstellung erforderlich sind. Bemerkenswert sind etwa die Pflicht zur Angabe der Blockchain-Transaction-ID bei kryptowertbezogenen Sachverhalten und die Angabe von Gemarkung, Flur und Flurstück bei Immobilientransaktionen. Die vollständige Aufstellung der seit dem 1. März 2026 geltenden Pflichtangaben ergibt sich aus den Anhängen zur GwGMeldV und den zugehörigen Anwendungshinweisen. Eine unterbliebene oder nicht vollständige Befüllung der Pflichtfelder führt dazu, dass die Meldung nicht übermittelt werden kann und eine technische Zurückweisung erfolgt. Bei Nichteinhaltung der Vorgaben kann die FIU den Meldenden zur Nachbesserung auffordern. Insbesondere bei wiederholten, systematischen oder vorsätzlichen Verstößen gegen die Vorgaben der Verordnung kommt die Verhängung von aufsichtsrechtlichen Maßnahmen über die zuständige Aufsichtsbehörde in Betracht. Am 20. Oktober 2025 veröffentlichte die FIU, abgestimmt mit der Bafin, Anwendungshinweise zur GwGMeldV. Diese stehen den Verpflichteten im geschützten Bereich der FIU-Website zum Abruf bereit und enthalten ergänzende Hinweise zur Umsetzung der Verordnung und ihrer Anlagen.

Etappen bis zur GwGMeldV (2017 – 2026)



Abb. 6: Der Weg bis zur GwGMeldV (2017 – 2026)

Datengrundlage verbessern

Mit den Neuregelungen wurden bundeseinheitliche Standards geschaffen, wodurch die FIU in ihrer gesetzlichen Aufgabenwahrnehmung gestärkt wird. Sie trägt zu einer Verbesserung der Meldungsqualität und der Einheitlichkeit der Meldungen bei. Durch diese Vorgaben ist die Meldungsverarbeitung bei der FIU vereinfacht und beschleunigt und die Analysearbeit operativ wie strategisch weiter gestärkt worden. Zugleich wurde vorgehend den Vorgaben aus dem im Sommer 2027 in Kraft tretenden und europaweit geltenden AML-Paket bereits Rechnung getragen. Für die strategische Auswertung bedeuten die neuen Standards, dass mit allgemein besser durchsetzbaren Regeln eine über den gesamten Datenbestand höhere Datenqualität einhergeht. Korrekt erfasste Transaktionsdaten ermöglichen es, länderspezifische Risiken zuverlässiger zu erkennen, sowohl im strategischen Risikomonitoring als auch bei der Auswertung einzelner Länder. Auch für die Verpflichteten bringt die GwGMeldV Vorteile. Die verbindliche Definition der erforderlichen Angaben schafft Klarheit über die Anforderungen an eine Verdachtsmeldung und reduziert Unsicherheiten in der Meldepraxis. Die strukturierten Pflichtfelder erleichtern die interne Qualitätssicherung und ermöglichen eine systematischere Bearbeitung von Verdachtsfällen.

3.1.2 Änderung der GwGMeldV-Immobilien

Im Februar 2025 trat eine Änderung der Geldwäschegesetzmeldepflichtverordnung-Immobilien in Kraft. Die Verordnung ergänzt das Barzahlungsverbot beim Immobilienerwerb gemäß § 16a GwG und definiert neue Meldetatbestände, die auf die Erkennung von Umgehungsstrategien ausgerichtet sind. In der Praxis fielen nach Einführung des Barzahlungsverbots Umgehungsversuche auf, etwa durch die Aufteilung von Zahlungen auf mehrere Tranchen unterhalb der Schwellenwerte oder durch den Einsatz zwischengeschalteter Dritter. Die Änderungsverordnung adressiert solche Konstellationen gezielt, indem sie zusätzliche meldepflichtige Sachverhalte definiert, die auf typische Umgehungsmuster abgestellt sind. Betroffen sind insbesondere Verpflichtete



GwGMeldV auf einen Blick

Rechtsgrundlage: § 45 Absatz 5 GwG
Verkündung: 1. September 2025 (BGBl. 2025 I Nr. 200)
Inkrafttreten: 1. März 2026
Kernelemente: elektronische Übermittlung über goAML (XML-Format), inhaltliche Mindestanforderungen, detaillierte Angabepflichten (u. a. Kryptowerte, Immobilien)
Anwendungshinweise: veröffentlicht am 20. Oktober 2025, abgestimmt mit Bafin
Konsultation: 40 Stellungnahmen im Rahmen der Verbändeanhörung

aus dem Immobiliensektor, darunter Notare, Immobilienmakler und Rechtsanwälte, die an Immobilien-transaktionen mitwirken. Die GwGMeldV-Immobilien und die GwGMeldV stellen zwei eigenständige, sich jedoch ergänzende Regelungswerke dar. Während die GwGMeldV den allgemeinen Rahmen für Form und Inhalt aller Verdachtsmeldungen setzt, konkretisiert die GwGMeldV-Immobilien die spezifischen Meldepflichten im Zusammenhang mit dem Barzahlungsverbot beim Immobilienerwerb. Die Wirkung der Änderungsverordnung ist in der Meldestatistik bereits sichtbar. Notare und Immobilienmakler verzeichnen im Berichtsjahr niedrigere Meldzahlen als im Vorjahr, dafür stieg aber die Relevanz an. Besonders deutlich zeigt sich der Rückgang bei den Notaren, die den Großteil der Meldungen in diesem Bereich abgeben. Die Meldungszahlen sanken hier von 7.739 im Jahr 2024 auf 6.612 im Berichtsjahr.

3.1.3 Auslegungs- und Anwendungshinweise der Bafin

Im Berichtsjahr hat die Bafin unter Beteiligung der FIU ihre Auslegungs- und Anwendungshinweise (AuA) zum GwG mehrfach aktualisiert. Im Februar 2025 wurde eine Neufassung der AuA

(Allgemeiner Teil) veröffentlicht, die unter anderem klarstellende Hinweise zur Anwendung der Sorgfaltspflichten bei grenzüberschreitenden Geschäftsbeziehungen und zur Dokumentation des Risikomanagementsystems enthielt. Im März 2025 folgte eine Aktualisierung, die auf das FinmadiG zurückging und insbesondere die Anforderungen an den Umgang mit Self-Hosted Wallets im Bereich der Kryptowertedienstleistungen präziserte. Eine weitere Konkretisierung im Juli 2025 betraf das Meldewesen und ergänzte die AuA um praxisbezogene Hinweise zur Abgabe von Verdachtsmeldungen, die auf die Harmonisierung mit den Anforderungen der GwGMeldV abgestimmt waren.

3.2 Nationale Zusammenarbeit

Die Zusammenarbeit und der Informationsaustausch mit Partnerbehörden und Verpflichteten zählen zu den zentralen Aufgaben der FIU. Im Fokus stehen dabei vor allem die Verbesserung der Kommunikation zwischen allen beteiligten Akteuren und die Förderung eines gemeinsamen Erkenntnisprozesses. Im Jahr 2025 hat die FIU die in den Vorjahren angestoßenen Maßnahmen zur Stärkung der Verpflichtetenkommunikation deutlich ausgebaut. Insgesamt führte die FIU im Berichtsjahr über 110 Informationsaustausche mit Verpflichteten und Aufsichtsbehörden des Finanzsektors durch und erreichte dabei über 330 externe Teilnehmende. Ergänzend fanden vier Veranstaltungen für den Nichtfinanzsektor mit insgesamt 254 Teilnehmenden statt. Neben bilateralen und multilateralen Austauschformaten stellt die FIU auch über ihre Website regelmäßig aktualisierte Informationen bereit. Diese richten sich sowohl an die Verpflichteten als auch an Behörden mit Aufgaben im Kontext der Bekämpfung von Geldwäsche und Terrorismusfinanzierung.

3.2.1 Anti Financial Crime Alliance (AFCA)

Ein zentrales Instrument der sektorübergreifenden Zusammenarbeit ist die im September 2019 gegründete und von der FIU geleitete Anti Financial Crime Alliance (AFCA). Die Public-Private-Partnership ver-

bindet Akteure aus Behörden und Privatwirtschaft mit Blick auf eine dauerhafte strategische Kooperation im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Seit ihrer Gründung im September 2019 hat die AFCA über 30 Analyse- und Whitepaper veröffentlicht, fünf Arbeitsgruppen etabliert und zählt zum Ende des Berichtsjahres 59 Mitgliedsinstitutionen. Das AFCA-Board führt die Allianz auf strategischer Ebene. Es setzt sich aus der FIU, der Bafin, dem BKA, der Deutschen Bank, der Commerzbank und der DZ BANK zusammen. Den Vorsitz führt die FIU. Auf operativer Ebene arbeiten fünf Arbeitsgruppen, nämlich zu den Grundsätzen der Zusammenarbeit, zu Risiken und Trends im Finanzsektor, zu Geldwäsche im Immobiliensektor, zu Steuerdelikten und zu Glücksspiel. Hinzu kommt das projektbezogene Format zur Umweltkriminalität. Das Management Office und der Expertenstab begleiten die Gremienarbeit fachlich.

➔ Projekt Umweltkriminalität

Die AFCA hat ihre Aktivitäten im Berichtsjahr weiter konsolidiert. Im Rahmen des Projekts Umweltkriminalität mit dem Arbeitstitel »Illegale Abfallentsorgung« widmet sich eine Arbeitsgruppe speziell diesem Phänomenbereich. Teilnehmer sind Banken, eine Nichtregierungsorganisation (NGO), das BKA und die FIU. Der Projektabschluss ist für das zweite Quartal 2026 vorgesehen. Eine Fortführung zum Thema illegaler Holzhandel ist ebenfalls für 2026 geplant.

➔ Artikel 75 EU-AMLR

Einen neuen Impuls erhielt die AFCA durch die Auseinandersetzung mit Artikel 75 der Verordnung (EU) 2024/1624 zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung (EU-AMLR). Der Artikel richtet sich primär an den Privatsektor, der im Rahmen von Partnerschaften künftig auch Operativ-Informationen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung austauschen soll. Die Wirksamkeit solcher Partnerschaften hängt maßgeblich von der aktiven Einbindung der zuständigen Behörden ab. Innerhalb der AFCA befassen sich zwei Gremien mit dem Thema, die Arbeitsgruppe 1 zu den Grundsätzen der Zusammenarbeit sowie der Expertenstab, der den Kontakt zu der im Dezember 2025 ins Leben gerufenen Artikel 75 Contact Group der Euro-

pol Financial Intelligence Public-Private Partnership (EFIPPP) aufgenommen hat und daran arbeitet, die Möglichkeiten eines operativen Austauschs innerhalb der AFCA zu formulieren.

→ **AFCA-Forum 2025**

Das AFCA-Forum fand im Berichtsjahr in München statt, ausgerichtet bei der HypoVereinsbank - UniCredit Deutschland. Im Mittelpunkt standen die Fortentwicklung der Allianz, die Weiterentwicklung der Zusammenarbeit zwischen öffentlichem und privatem Sektor sowie ein Erfahrungsaustausch mit Public-Private-Partnerships aus Österreich und Dänemark. Juan Manuel Vega-Serrano, stellvertretender Vorsitzender der AMLA, ordnete in einem Impulsbeitrag die künftige Rolle der europäischen Geldwäscheaufsichtsbehörde ein. Vorgestellt wurde zudem ein im Berichtsjahr von AFCA-Mitgliedern erarbeitetes Whitepaper.

3.2.2 Umsetzung der gesetzlichen Anpassungen zur Stärkung der FIU

→ **Fortentwicklung des Risikobewertungssystems**

Die FIU hat die im Jahr 2024 eingeführten Risikobewertungssysteme gemäß § 30 Absatz 2 GwG im Berichtsjahr weiterentwickelt. Das automatisierte Filtersystem, dessen Kriterien im Benehmen mit Strafverfolgungsbehörden und den Nachrichtendiensten des Bundes festgelegt werden, wurde einer umfassenden Evaluation unterzogen und auf dieser Grundlage angepasst.

→ **Weiterführung der Fristfall-Kriterien und typisierten Transaktionen**

Die im November 2024 begonnene behördenübergreifende Abstimmung zu den Kriterien für die risikobasierte Auswahl von Fristfällen gemäß § 46 Absatz 1 Satz 3 bis 5 GwG wurde im Berichtsjahr fortgeführt. Ebenso wurde die Festlegung sogenannter Negativtypologien vorangetrieben. Unter diesem Begriff werden Transaktionsmuster verstanden, die gerade nicht von der Meldepflicht nach § 43 Absatz 1 GwG erfasst sind. Beide Prozesse erfolgen im Benehmen mit Strafverfolgungs- und Aufsichtsbehörden.

3.2.3 Neues Rückmeldeverfahren nach § 41 Absatz 2 und 3 GwG

Ein zentrales Anliegen der Verpflichteten sind Rückmeldungen zu erstatteten Verdachtsmeldungen. Mit dem im Jahr 2025 eingeführten neuen Rückmeldeverfahren hat die FIU dieses Anliegen aufgegriffen und das bisherige Verfahren grundlegend überarbeitet.

In der Vergangenheit erhielten Verpflichtete quartalsweise zusammenfassende Rückmeldeberichte. Diese enthielten zwar verschiedene Statistiken, waren jedoch nicht auf den konkreten Einzelfall bezogen. Die Erstellung dieser Berichte war zudem mit erheblichem manuellem Aufwand verbunden, sodass die Rückmeldungen häufig erst mit einem Verzug von über einem Jahr bei den Verpflichteten eingingen. Die FIU hat das Verfahren daher unter Berücksichtigung der seitens der Kammern und Verbände geäußerten Vorschläge und Anregungen neu konzipiert. Im Fokus steht nunmehr eine automatisierte Rückmeldung über die goAML-Mailbox zu einzelnen Verdachtsmeldungen, die durch die angewandten Filter (Risikobewertungssysteme gemäß § 30 Absatz 2 GwG) erfasst wurden. Der Versand erfolgt wöchentlich und bezieht sich grundsätzlich auf Meldungen der vorangegangenen Kalenderwoche. Sofern nach 21 Werktagen, gerechnet ab dem Zeitpunkt der Übermittlung der Verdachtsmeldung an die FIU, keine Rückmeldung erfolgte, dürfte die/der Verpflichtete davon ausgehen, dass diese Verdachtsmeldung im Zeitpunkt ihres Eingangs bei der FIU zunächst keine weitere operative Analyse ausgelöst hat.

Dieser Sachstand bedeutet jedoch nicht, dass derlei Verdachtsmeldungen künftig nicht die Meldepflicht nach § 43 bzw. § 44 GwG oder § 31b Absatz 2 AO auslösen; die Prüfung der Meldepflicht wird hierdurch nicht berührt.

Ergänzend erfolgen einzelfallbezogene Rückmeldungen, sofern die FIU Mängel in der Meldequalität feststellt. Im Bedarfsfall gibt die FIU ein ausführliches, individuelles Feedback, das gezielt auf Besonderheiten des meldenden Verpflichteten eingeht, beispielsweise zur korrekten Erfassung von Konten, zur Beifügung von Legitimationsdokumenten oder zur vollständigen Angabe beteiligter Personen und Organisationen. Nach Abschluss der erforderlichen technischen Vor-

bereitungen wurde das Rückmeldeverfahren zum 1. August 2025 rückwirkend zum Jahresbeginn 2025 auch auf Meldungen von Aufsichtsbehörden gemäß § 44 GwG und Mitteilungen von Finanzbehörden gemäß § 31b Absatz 2 AO ausgeweitet. Die Ausweitung trägt dem Umstand Rechnung, dass auch behördliche Meldungen und Mitteilungen einer konsistenten Rückmeldung bedürfen.

Im Rahmen zahlreicher Gesprächsformate erhielt die FIU positive Rückmeldungen zum neuen Konzept. Verpflichtete berichteten, dass ihnen die einzelfallbezogenen Rückmeldungen ermöglichen, Anpassungen an ihren internen Monitoring-Systemen vorzunehmen. Insgesamt zeigt das neue Verfahren, dass ein Dialog auf Augenhöhe zwischen FIU und Verpflichteten möglich und gewünscht ist.



Abb. 7: Informationsaustausch mit Verpflichteten und Aufsichtsbehörden 2025

3.2.4 Aktualisierung der gemeinsamen Orientierungshilfe von Bafin und FIU

Die im November 2024 veröffentlichte gemeinsame Orientierungshilfe zur Auslegung der Begriffe »Unverzüglichkeit« und »Vollständigkeit« einer Verdachtsmeldung nach § 43 GwG wurde im Berichtsjahr aktualisiert. Die überarbeitete Fassung wurde am 1. Dezember 2025 im öffentlichen Bereich der Websites von Bafin und FIU publiziert.

Grundlage der Überarbeitung war ein strukturierter Konsultationsprozess mit dem Privatsektor. Im Juli 2025 hatte die FIU Kammern und Verbände eingeladen, Anmerkungen und Ergänzungsvorschläge einzureichen. Die eingegangenen Stellungnahmen wurden systematisch ausgewertet und im weitestmöglichen Umfang berücksichtigt. Darüber hinaus flossen Erkenntnisse aus einem Workshop anlässlich der 9. Geldwäschetagung im April 2025 ein, in dem erste Erfahrungen im Umgang mit der Orientierungshilfe erörtert wurden.

Wesentliche Änderungen betreffen drei Bereiche. Erstens wurde die Orientierungshilfe um vier praxisnahe Fallbeispiele ergänzt, die den Verpflichteten eine konkretere Anwendung der Tatbestandsvoraussetzungen der Meldepflicht ermöglichen. Dieser Wunsch war sowohl im Rahmen der Konsultation als auch anlässlich der Geldwäschetagung vorgetragen worden. Zweitens wurde ein Hinweis ergänzt, der darauf gerichtet ist, sogenanntes »defensive reporting« zu vermeiden, also die vorsorgliche Abgabe von Meldungen ohne hinreichende Anhaltspunkte. Drittens wurde ein Leitfaden zur Dokumentation des Entscheidungsprozesses aufgenommen.

Die Aktualisierung zeigt, dass FIU und Bafin das Feedback der Verpflichteten ernst nehmen und den Dialog über die Auslegung zentraler Begriffe des Geldwäschegesetzes aktiv fortführen. Die GwGMeldV (vgl. 3.1.1) untermauert die Inhalte der Orientierungshilfe nunmehr auch regulatorisch.

3.2.5 Dialogformate mit Verpflichteten und Aufsichtsbehörden

Am 9. April 2025 führte die FIU die 9. Geldwäschetagung für Verpflichtete und Verbände des Finanz-



Orientierungshilfe:
Vom Feedback zur Aktualisierung

- April 2025:** Workshop auf der 9. Geldwäschetagung, erste Erfahrungen
- Juli 2025:** Konsultation mit Kammern und Verbänden
- Dezember 2025:** Aktualisierte Fassung veröffentlicht
- Wesentliche Ergänzungen:** 4 neue Praxisfälle, Hinweis zur Vermeidung von defensive reporting, Dokumentationsleitfaden

sektors in Köln durch. Rund 90 Vertreterinnen und Vertreter aus dem Privatsektor nahmen an der Veranstaltung teil, die aus Vorträgen, Workshops und Podiumsdiskussionen zu aktuellen Themen der Prävention von Geldwäsche und Terrorismusfinanzierung bestand. Aktive Beiträge erfolgten unter anderem von der Bafin, dem BKA sowie von Verpflichteten selbst.

Ein Workshop widmete sich den ersten Erfahrungen im Umgang mit der gemeinsamen Orientierungshilfe zur Unverzüglichkeit und Vollständigkeit einer Verdachtsmeldung. FIU und Bafin wiesen in diesem Rahmen darauf hin, dass beide Begriffe gleichwertig zu verstehen seien. Fragestellungen und Anmerkungen der Verpflichteten aus diesem Workshop wurden in die anschließende Konsultation und Aktualisierung der Orientierungshilfe übernommen (vgl. 3.2.4). Darüber hinaus führte die FIU im Berichtsjahr 15 Workshops mit 13 verschiedenen Verpflichteten durch. Acht dieser Institute gehörten zu den 20 meiststärksten Verpflichteten. Ergänzend fanden 81 telefonische Sensibilisierungsgespräche mit 27 Verpflichteten statt. Thematische Schwerpunkte waren die Meldequalität, die Umsetzung der GwGMeldV (vgl. 3.1.1) sowie sektorspezifische Fragestellungen. Die Gespräche zeigten, dass die Verpflichteten den direkten Kontakt mit der FIU schätzen und großen Wert auf eine gute Zusammenarbeit legen. Durch die einzelfallbezogene Erörterung individueller Meldequalitätsmängel konnten zielgerichtete Verbesserungen angeregt werden.

3.3 Europäische und internationale Zusammenarbeit

Geldwäsche und Terrorismusfinanzierung sind sehr häufig grenzüberschreitende Phänomene. Die Methoden der Täter werden zunehmend ausgefeilter, die Konstrukte zum Verschleiern illegal erlangter Vermögenswerte komplexer. Die Vernetzung der globalen Wirtschaft erleichtert es Kriminellen, Gelder über Ländergrenzen hinweg zu transferieren und Spuren gezielt zu verwischen.

Nur durch einen ganzheitlichen Ansatz auf internationaler Ebene lassen sich Geldwäsche und Terrorismusfinanzierung wirksam bekämpfen. Die Intensivierung der operativen und strategischen Zusammenarbeit mit ihren internationalen Partner-FIUs bildet daher einen Schwerpunkt in der Tätigkeit der FIU Deutschland. Sie ist Mitglied der Egmont Group of FIUs sowie der FIU Plattform der EU.

Im Jahr 2025 hat die internationale Dimension der Arbeit der FIU Deutschland erheblich an Gewicht gewonnen. Das Berichtsjahr war international vor allem durch die Wahl von Daniel Thelesklaf, Leiter der FIU Deutschland, zum Vizepräsidenten der Egmont Group geprägt. Hinzu kamen der operative Start der europäischen Anti-Geldwäschebehörde AMLA in Frankfurt am Main und die fortgesetzte aktive Mitwirkung in den Gremien der FATF. Das Bild wird durch ein dichtes Programm bilateraler und multilateraler Besuche abgerundet.

3.3.1 Egmont Group of FIUs

→ **31. Plenartagung und Vizepräsidentenwahl**

Die Egmont Group feierte im Berichtsjahr ihr 30-jähriges Bestehen. Bei der 31. Plenartagung vom 6. bis 11. Juli 2025 in Luxemburg kamen Vertreterinnen und Vertreter der mittlerweile 182 Mitglieds-FIUs zusammen. Fast 600 Delegierte nahmen teil. Während der Plenarwoche wurden 47 Memoranda of Understanding zwischen FIUs unterzeichnet.

Im Rahmen der Plenartagung wurde FIU-Leiter Daniel Thelesklaf für eine zweijährige Amtszeit zum Vizepräsidenten der Egmont Group gewählt. Die Wahl zeigt das Vertrauen der internationalen Gemeinschaft in die Arbeit der deutschen FIU und eröffnet die

Möglichkeit, die strategische Ausrichtung des weltweiten FIU-Netzwerks aktiv mitzugestalten.

→ Internationaler Tag der FIU

Die Plenartagung beschloss zudem die Einführung eines »Internationalen Tags der FIU« am 9. Juni. Das Datum erinnert an die Gründung der Egmont Group im Egmont-Palast in Brüssel im Jahr 1995.

→ Operative Unabhängigkeit als verbindlicher Standard

Ein weitreichender Beschluss der Plenartagung 2025 betrifft die operative Autonomie und Unabhängigkeit der FIUs. Die Egmont Group hat 18 Kriterien der Unabhängigkeit in ihre Charta aufgenommen und damit zu verbindlichen Mitgliedschaftsanforderungen erhoben.

3.3.2 Start der AMLA

Am 1. Juli 2025 hat die Anti-Money Laundering Authority (AMLA) in Frankfurt am Main ihre operative Tätigkeit aufgenommen. Die AMLA ist die neue europäische Geldwäschaufsichtsbehörde und unterstützt FIUs in der Wahrnehmung ihrer Aufgaben. Sie wird ab 2028 direkte Aufsicht über die risikoreichsten Finanzunternehmen ausüben, als Drehscheibe für die nationalen Aufsichtsbehörden fungieren und in bestimmten Bereichen die Zusammenarbeit der EU-FIUs koordinieren.

Die FIU Deutschland hat sich von Beginn an aktiv in den Aufbauprozess der AMLA eingebracht, sowohl durch die Mitwirkung in zentralen Arbeitsgruppen als auch durch die Aufnahme eines regelmäßigen bilateralen Austauschs mit der AMLA-Führungsebene.

→ Mitwirkung im Verwaltungsrat

Daniel Thelesklaf ist als Leiter der FIU Deutschland zugleich Mitglied des Verwaltungsrats der AMLA in FIU-Zusammensetzung (General Board). Dr. Thora Funken, stellvertretende Leiterin der FIU, ist »alternate member«. Dieses Gremium fasst auch die Beschlüsse, die zur Erfüllung der entsprechenden Unterstützungs- und Koordinierungsaufgaben der AMLA betreffend die FIUs erforderlich sind.



Egmont Group of FIUs

Die Egmont Group ist der weltweite Zusammenschluss der Financial Intelligence Units. Sie wurde 1995 gegründet und zählt zum Ende des Berichtsjahres 182 Mitglieder. Die Mitglieds-FIUs tauschen auf operativer Ebene Finanzinformationen aus und arbeiten auf strategischer Ebene in Gremien eng zusammen, um Rahmenparameter für die Bekämpfung der Geldwäsche und Terrorismusfinanzierung mitzugestalten.

→ Arbeitsgruppen und operative Zusammenarbeit

Die Zusammenarbeit mit der AMLA konzentrierte sich im Berichtsjahr auf die Mitwirkung in mehreren Arbeitsgruppen sowie auf den direkten Austausch mit Vertreterinnen und Vertretern der AMLA.

Im März 2025 richtete die AMLA die Arbeitsgruppe »Building up AMLA« ein, an der sich die FIU von Beginn an beteiligte. Der für die FIU relevante Workstream bereitete zentrale Dokumente für den Unterstützungs- und Koordinierungsmechanismus gemäß Abschnitt 6 der 6. EU-Geldwäscherichtlinie (AMLD6) vor und legte diese dem Verwaltungsrat bis Ende 2025 vor.

In weiteren Arbeitsgruppen wirkte die FIU Deutschland an der Erarbeitung technischer Durchführungsstandards mit, unter anderem zu Format von Verdachtsmeldungen und Bereitstellung von Transaktionsdaten (Artikel 69 Absatz 3 EU-AMLR), zu Relevanz- und Selektionskriterien für die grenzüberschreitende Weiterleitung von Verdachtsmeldungen (Artikel 31 Absatz 3 EU-AMLR), zum Format für den Informationsaustausch zwischen FIUs (Artikel 31 Absatz 2 EU-AMLR) sowie zum Format für die Informationsübermittlung an die Europäische Staatsanwaltschaft (Artikel 81 Absatz 1 EU-AMLR).

→ Besuche

Der direkte Austausch mit der AMLA-Führungsebene wurde im Berichtsjahr durch mehrere Besuche intensiviert. Unter anderem begrüßte die FIU am 3. September den AMLA-Vizevorsitzenden Juan Manuel Vega-Serrano in Köln. Am 11. Dezember fand ein Country Visit der AMLA-Vorsitzenden Bruna Szego in

den Räumlichkeiten der Bafin in Frankfurt am Main statt, an dem das BMF, die Bafin, die FIU sowie Vertreter des Privatsektors teilnahmen. Die frühe und direkte Einbindung der AMLA-Führungsebene zeigt die Bereitschaft aller Beteiligten, die Zusammenarbeit von Beginn an bestmöglich auszurichten.

3.3.3 FATF

Die FATF ist das zentrale internationale Gremium zur Festlegung globaler Standards gegen Geldwäsche und Terrorismusfinanzierung. Gleichzeitig prüft die FATF deren Mitglieder hinsichtlich der effektiven Umsetzung dieser Standards. Die FIU bringt sich im Rahmen der deutschen Delegation aktiv in die Gremienarbeit ein.

→ Plenarsitzungen und Standards

Bei der Plenarsitzung im Februar 2025 beschloss die FATF neue Standards zum risikobasierten Ansatz (Risk-Based Approach). Die FIU brachte praxisrelevante Perspektiven aus der operativen Analysearbeit ein und unterstützte die deutsche Delegation bei der Positionierung zu den Entwürfen.

→ »Graue Liste«

Die FATF aktualisiert die Liste der Jurisdiktionen mit strategischen Defiziten bei der Bekämpfung der Geldwäsche und Terrorismusfinanzierung regelmäßig im Rahmen ihrer Plenarsitzungen. Die Anpassungen haben Auswirkungen auf das Risikomonitoring der Verpflichteten.

→ Projektarbeit

Die FIU Deutschland war im Berichtsjahr am FATF-Projekt »Comprehensive Update on Terrorist Financing Risks« beteiligt, das im Zeitraum Juni 2024 bis Juni 2025 durchgeführt wurde. Parallel dazu wurde im März 2025 die Studie »Online Child Sexual Exploitation« veröffentlicht, an deren Entwicklung die FIU mitgewirkt hatte.

3.3.4 Zusammenarbeit mit der Europäischen Staatsanwaltschaft

Die FIU arbeitet eng mit der Europäischen Staatsanwaltschaft (EUSTa) zusammen. Die Zusammenarbeit stützt sich auf die gesetzlichen Grundlagen, insbesondere § 32 GwG und die Verordnung (EU) 2017/1939 des Rates der Europäischen Union. Der Austausch umfasst fallspezifische Anfragen, vertiefte Analysen und gemeinsame Abstimmungen zu laufenden Sachverhalten. Schwerpunkt der bisherigen Kooperation sind grenzüberschreitende Umsatzsteuerkarusselle. Im Berichtsjahr kooperierte die FIU in mehreren Verfahren unmittelbar mit der EUSTa oder mit beauftragten Strafverfolgungsbehörden. Aktuell besteht Kenntnis über fünf laufende EUSTa-Verfahren im Zusammenhang mit europaweiten Umsatzsteuerbetrugssystemen. Die Zusammenarbeit hat sich als wirksames Instrument erwiesen. Die EUSTa bündelt die Verfahrensführung bei einem zentralen Ansprechpartner und kann bundesweit sowie in anderen Mitgliedstaaten Maßnahmen koordinieren. Eine Fallkonstellation aus dem Berichtsjahr illustriert die Zusammenarbeit aus der operativen Perspektive.

EXKURS

Im Gespräch – Hennie Verbeek-Kusters

Langjährige Leiterin der FIU der Niederlande

Die FIU der Niederlande zählt europaweit zu den Vorreiterinnen in der risikobasierten Priorisierung von Verdachtsmeldungen. Bereits seit dem Jahr 2008 arbeitet sie konsequent risikoorientiert. In der FATF-Länderprüfung von 2022 wurde die niederländische Nutzung von Finanzinformationen als eine der besten aller geprüften Staaten bewertet.



Hennie Verbeek-Kusters

FIU Deutschland:

Die FIU der Niederlande erhält eine sehr große Zahl unterschiedlicher Meldungen. Ab wann wurde der risikobasierte Ansatz zu einem zentralen Arbeitsprinzip Ihrer Organisation und was hat diesen Schritt ausgelöst?

Verbeek-Kusters:

Der Schritt zu einem risikobasierten Ansatz wurde tatsächlich bereits im Jahr 2008 eingeleitet. Bis dahin arbeitete die FIU überwiegend reaktiv. Schon damals gingen über 100.000 Meldungen bei der FIU ein, bei einer Personalstärke von 56 Beschäftigten. Wir hatten deshalb nie eine andere Wahl, als zu priorisieren. Einen verlässlichen und objektiven Weg dafür zu finden, war und ist eine zentrale Aufgabe. Der gesamte Datenbestand muss so sorgfältig wie möglich erschlossen werden, und nicht jede einzelne Meldung nacheinander abgearbeitet. Wir sind in diesem Punkt immer sehr transparent gewesen. Seit meinem Amtsantritt als Leiterin der FIU der Niederlande war der risikobasierte Ansatz fundamental für unsere Arbeit.

FIU Deutschland:

Welche Rolle spielen datengetriebene Analysemethoden bei dieser Priorisierung, und wo stößt Technologie an Grenzen, an denen menschliche Urteilskraft erforderlich ist?

Verbeek-Kusters:

Wir haben Abfragen entwickelt, die auf verschiedenen Perspektiven basieren. Die identifizierten Risiken stützen sich auf die Nationale Risikoanalyse; spezifischere Prioritäten werden in Zusammenarbeit mit den Strafverfolgungsbehörden gesetzt. Eine weitere Perspektive ergibt sich aus den Zielen der öffentlich-privaten Partnerschaften, an denen wir mitwirken. Nicht zuletzt führen wir datengetriebene explorative strategische Analysen aus kriminologischer Perspektive zu Phänomenen und Trends durch. Zugleich nutzen wir die Daten zunehmend so, dass sie für sich selbst sprechen können. Die menschliche Urteilskraft kommt ins Spiel, sobald die Ergebnisse einer Abfrage auf dem Tisch liegen. An dieser Stelle müssen die FIU-Analystinnen und -Analysten die relevantesten Daten identifizieren, um aus ihnen Fälle aufzubauen.

FIU Deutschland:

In der Länderprüfung von 2022 hat die FATF die Nutzung von Financial Intelligence in den Niederlanden als eine der besten aller geprüften Staaten bewertet. Sehen Sie dieses Ergebnis als unmittelbare Bestätigung des risikobasierten Ansatzes, und gab es Aspekte der Evaluation, die Sie zu weiteren Anpassungen veranlasst haben?

Verbeek-Kusters:

Ja, ich halte das für das Ergebnis unseres risikobasierten Ansatzes. Unsere enge Zusammenarbeit mit den Partnerbehörden zielt darauf ab, wertvolle Fälle zu identifizieren, aus denen sich Interventionsmöglichkeiten und neue Erkenntnisse zu Trends und Phänomenen ergeben. Wir arbeiten derzeit an einem stärker strukturierten Rückmeldesystem. Die Ermittlerinnen und Ermittler werden darin verpflichtet, der FIU Rückmeldung zur Nutzbarkeit und zum Mehrwert der übermittelten Informationen zu geben. Der Rückmeldeprozess entwickelt sich noch weiter, und wir bauen eine neue IT-Infrastruktur auf, die ihn tragen soll. Damit werden wir besser und gezielter an die meldenden Einrichtungen zurückmelden können. Zugleich ermöglicht es uns, unsere internen Prozesse anzupassen und den risikobasierten Ansatz weiter zu verfeinern.

FIU Deutschland:

Ein risikobasierter Ansatz bedeutet auch, bestimmten Meldungen bewusst weniger Ressourcen zu widmen. Wie stellt die FIU der Niederlande sicher, dass dabei keine relevanten Informationen übersehen werden?

Verbeek-Kusters:

Wir haben verschiedene Wege, den Meldungsbestand zu erschließen. Wenn eine Meldung aber die definierten Abfragen nicht trifft, wird sie nicht individuell durch eine Analystin oder einen Analysten bearbeitet. Wir arbeiten derzeit an Methoden, mit denen sich genau diejenigen Meldungen identifizieren lassen, die keinen Treffer ausgelöst haben. Dieses »Reverse Querying« lässt sich mit intelligenten Text- und Stichwort-basierten Suchen nach bestimmten Merkmalen umsetzen. Es wird uns langfristig ermöglichen, alle eingegangenen Meldungen auf ihre Qualität und ihren Wert hin zu bewerten.

FIU Deutschland:

Welche Rolle erwarten Sie für den risikobasierten Ansatz auf europäischer Ebene, mit AMLA und dem europäischen AML-Paket?

Verbeek-Kusters:

Das gesamte europäische AML-Paket basiert auf einem risikobasierten Ansatz. Wenn wir eine Methode entwickeln, mit der sich Risiken stärker harmonisiert identifizieren lassen, wird dies die Diskussionen darüber, wo und worauf sich die Aufsicht konzentrieren soll, erheblich erleichtern. Zugleich sehen wir hier wichtige Anknüpfungspunkte für die Zusammenarbeit zwischen FIUs und den Austausch von Erkenntnissen. Auf diese Weise werden wir eine gemeinsame »Sprache« für Risiken und den risikobasierten Ansatz entwickeln können.

Vom Fristfall zum europäischen Ermittlungsverfahren

Ende Februar 2025 ging bei der FIU ein Fristfall ein. Ein Verpflichteter hatte zwei Auslandsüberweisungen in Höhe von insgesamt rund 120.000 Euro angehalten. Die erste Analyse zeigte ein Konto mit reinem Durchlaufcharakter, gespeist durch Eigenüberträge und Rechnungseingänge, ohne erkennbare gewerbetypische Umsätze. Zu den gemeldeten Transaktionspartnern lagen bereits weitere Verdachtsmeldungen vor.

Der Bankkunde versuchte, Gelder auf ein weiteres Konto zu transferieren. Vor Ablauf der Dreitagesfrist ordnete die FIU die erste Sofortmaßnahme an und untersagte alle ausgehenden Transaktionen. Als am Folgetag bei einer Drittbank nur noch 22.000 Euro gesichert werden konnten, weil der Kunde kurz zuvor fast 300.000 Euro in mehrere EU-Mitgliedstaaten überwiesen hatte, folgte eine zweite Sofortmaßnahme. Die Steuerfahndung wurde umgehend informiert und leitete eigene Pfändungsmaßnahmen ein.

Am fünften Tag der Analyse übernahm die EUSTa die Ermittlungen. Ausschlaggebend waren neue Erkenntnisse der Steuerfahndung, die auf ein grenzüberschreitendes Umsatzsteuer-Betrugssystem mit einem Schaden in zweistelliger Millionenhöhe hindeuteten. Die FIU weitete ihre Analyse auf die Transaktionspartner aus und ordnete in Abstimmung mit Steuerfahndung und EUSTa insgesamt neun Sofortmaßnahmen bei fünf Verpflichteten an. Eingehende Zahlungen blieben dabei zulässig, ausgehende Transfers wurden untersagt. So konnten bis zur Aufhebung der Maßnahmen über 4,7 Mio. Euro gesichert werden. Parallel analysierte die FIU die beteiligten Firmen unter Geldwäsche Gesichtspunkten und leitete erweiterte Meldungen nach § 32 GwG an die Strafverfolgungsbehörden weiter. Über den Ersuchensbereich wurden zudem 190 ausländische Konten in 22 Ländern abgefragt. Diese Erkenntnisse bildeten die Grundlage für die Ermittlungsmaßnahmen der EUSTa.

Die EUSTa konnte bundesübergreifend innerhalb von drei Wochen Durchsuchungsbeschlüsse erwirken. Ende März 2025 durchsuchten Ermittlungskräfte der Steuerfahndung Leipzig, Berlin und München sowie der Kriminalpolizeiinspektion Leipzig und der Polizei München koordiniert 28 Standorte. Im Juni folgten weitere Maßnahmen im europäischen Ausland. Ins-

gesamt wurden sechs Haftbefehle in Deutschland und Portugal vollstreckt. Die Anklage wegen bandenmäßiger Umsatzsteuerhinterziehung ist vor dem Landgericht anhängig.

Die enge Abstimmung zwischen FIU, Steuerfahndung und EUSTa ermöglichte in diesem Fall eine Verzahnung von Geldwäscheanalyse, steuerlichen Sicherungsmaßnahmen und strafrechtlichen Ermittlungen, die in dieser Geschwindigkeit und Reichweite ein Novum war.

»4,7 Mio. Euro gesichert durch 9 Sofortmaßnahmen bei 5 Verpflichteten, in Abstimmung mit Steuerfahndung und EUSTa.«

Fallbeispiel Fristfall 2025



Abb. 8: Sechs Tage vom Fristfall zur EUSTa-Übernahme

3.3.5 Weitere europäische und internationale Formate

→ EU FIUs Platform und FIU.net

Im Berichtsjahr wurde die europäische Zusammenarbeit auch im Rahmen der EU FIUs Platform fortgesetzt. Es handelt sich um eine im Jahr 2006 durch die Europäische Kommission eingesetzte Expertengruppe zum Austausch und zur Kooperation zwischen FIUs in der Europäischen Union. Bis zur im Juli 2027 geplanten Übernahme durch die AMLA hat die EU FIUs Platform auch maßgeblich zur Fortentwicklung von FIU.net NG (Next Generation) beigetragen. Bei FIU.net NG handelt es sich um das zentrale Kommunikationsnetzwerk zum sicheren Austausch von Informationen zwischen FIUs der Europäischen Union einschließlich der drei Staaten der Europäischen Freihandelsassoziation (EFTA), Norwegen, Island und Liechtenstein. Auf der 64. EU FIUs Platform am 25. Juni 2025 in Brüssel informierte die von der Platform eingesetzte FIU.net Advisory Group über die Stabilität der Anwendung, den Ausbau der Schulungsmaßnahmen sowie das Nutzerfeedback zu der Entwicklung von FIU.net NG und der Ablösung von FIU.net Legacy. Optionen für neue Funktionen und künftige Prioritäten von FIU.net NG wurden diskutiert. Für das derzeit verwendete FIU.net NG wurde eine Optimierungsstudie erstellt. Sie schreibt unter anderem das Prinzip der nationalen Datenhoheit und

*i***EFIPPP**

Die Europol Financial Intelligence Public Private Partnership ist eine länderübergreifende öffentlich-private Partnerschaft für den Informationsaustausch im Bereich der Geldwäsche- und Terrorismusfinanzierungsbekämpfung. Seit 2017 bietet EFIPPP ein Umfeld für die grenzüberschreitende Zusammenarbeit und den Informationsaustausch zwischen Europol, den zuständigen Behörden (einschließlich Finanzermittlungsstellen und Strafverfolgungsbehörden) und regulierten Finanzdienstleistern wie Banken. Gegenwärtig hat EFIPPP 103 Mitglieder und Beobachter.

Kontrolle fest und umfasst Verbesserungspotenziale sowie mögliche zukünftige Entwicklungsrichtungen zur Stärkung der EU-weiten Datenanalysemöglichkeiten.

→ Europol Financial Intelligence Public Private Partnership (EFIPPP)

Die FIU Deutschland hat ihr Engagement in der EFIPPP auch im Jahr 2025 weiter gestärkt. Der Workstream »Trafficking in Human Beings, Phase II«, den die FIU Deutschland bis Anfang des Jahres 2025 geleitet hatte, wurde weiter vorangetrieben. Im Workstream »Child Sexual Abuse and Exploitation« (CSAE) leitet die FIU eine Unterarbeitsgruppe. Darüber hinaus beteiligt sich die FIU an Arbeitsgruppen zu Investment Fraud, Krypto-Assets und Terrorismusfinanzierung sowie an den Plenarsitzungen der EFIPPP. Dort brachte sich die FIU auch mit eigenen Vorträgen und der Leitung von Workshops ein.

→ Internationale Initiativen: CTFTI und RRIFS

Die FIU Deutschland setzte im Jahr 2025 ihr Engagement in den internationalen Initiativen CTFTI und RRIFS fort. Die Counter Terrorist Financing Taskforce Israel (CTFTI) wurde kurz nach dem Terrorangriff der Hamas auf Israel am 7. Oktober 2023 auf Initiative der FIUs der Niederlande, der USA, Israels und Deutschlands gegründet. FIUs aus 18 Nationen teilen und analysieren gemeinsam Erkenntnisse zu den Finanzströmen von Terrororganisationen. Die Zusammenarbeit wurde im Berichtsjahr fortgesetzt. Die Arbeitsgruppe »Russia-Related Illicit Finance and Sanctions« (RRIFS), die von den FIUs der G7-Staaten sowie von Australien, Neuseeland und den Niederlanden im Zusammenhang mit den nach dem russischen Angriff auf die Ukraine im Jahr 2022 erheblich ausgeweiteten Sanktionen gegen Russland gegründet wurde, setzte ihre etablierte Zusammenarbeit auch 2025 fort und dient dem Austausch zu sanktionsrelevanten Finanzströmen.

3.3.6 Bilaterale und multilaterale Zusammenarbeit

Im Jahr 2025 empfing die FIU eine Vielzahl internationaler Delegationen und war selbst bei Ver-

anstaltungen im Ausland vertreten. Das Spektrum reichte von Studienbesuchen, die vom Europarat oder der Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) organisiert wurden, über operative Fachaustausche bis hin zum jährlichen Treffen der deutschsprachigen Heads of FIU, das erstmals in Deutschland stattfand. Das Treffen der deutschsprachigen Heads of FIU am 26. und 27. November in Dresden vereinte Delegationen aus der Schweiz, Liechtenstein, Luxemburg, Österreich und den Niederlanden. Im Mittelpunkt standen strategische und operative Themen, die Nutzung von goAML, die Zusammenarbeit mit Strafverfolgungsbehörden und aktuelle Entwicklungen im Bereich Kryptowerte.

3.3.7 Vorbereitung auf das EU-AML-Paket

Mit dem AML-Paket hat die EU die Vorschriften zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung umfassend harmonisiert. Zentraler Baustein ist die Anti-Money Laundering Directive (AMLD6), die ab dem 10. Juli 2027 weite Teile des GwG ersetzen wird. Die FIU bereitet sich auf diese Veränderungen umfassend vor. Besondere Aufmerksamkeit gilt der mit Artikel 80 Absatz 4 AMLD6 einhergehenden Verpflichtung zur Abgabe schwellenwertbasierter, verdachtsunabhängiger Meldungen. Für Deutschland ist dieser Meldungstyp neu. Die FIU erarbeitet im Austausch mit den Verpflichteten Prognosen zum erwarteten Meldevolumen und bereitet die Strukturen und Abläufe für Aufnahme und Verarbeitung gezielt vor.

Global

Egmont Group of Financial Intelligence Units

Weltweiter FIU-Verbund, 182 Mitglieder

Europäisch

EU FIUs Platform

FIUs der EU-Mitgliedsstaaten

Anti-Money Laundering Authority – AMLA

EU-Anti-Geldwäschebehörde, Sitz Frankfurt am Main

Partnerschaften und Initiativen

EFIPPP

Europol-PPP, 100+ Mitglieder

AFCA

Deutsche-PPP, Vorsitz FIU

CTFTI

Taskforce, 18 Nationen

RRIFS

G7 und weitere Partner

Abb. 9: Internationale Formate und Mitgliedschaften der FIU

Digitalisierung und Technologie

4. Digitalisierung und Technologie

Die technologische Weiterentwicklung der FIU hat sich im Berichtsjahr weiter beschleunigt. Mit einer Low-Code-Plattform kann die FIU benötigte Fachanwendungen schnell bereitstellen; erste auf der Plattform entwickelte Anwendungen wurden im Jahr 2025 in den operativen Betrieb überführt (4.1). Daneben fanden die im Vorjahr begonnenen datenbasierten Analyseverfahren, insbesondere Anomalieerkennung und Netzwerkanalyse, zunehmend Eingang in die laufende Analysearbeit (4.2).

4.1 Beschleunigte Digitalisierung durch Low-Code-Entwicklung

Die Fachprozesse der FIU sind stark datengetrieben. Neue Geldwäschemethoden, veränderte Meldeformate und aktualisierte regulatorische Vorgaben erfordern eine hohe Anpassungsfähigkeit der eingesetzten digitalen Werkzeuge. Um auf veränderte operative Bedarfe schneller reagieren zu können, setzt die FIU ergänzend auf den Einsatz einer Low-Code-Plattform. Der Low-Code-Ansatz reduziert den Programmieraufwand bei der Erstellung von Fachanwendungen. Visuelle Werkzeuge, wiederverwendbare Komponenten und vorkonfigurierte Dienste verkürzen den Weg von der Anforderung zum funktionsfähigen Prototyp. Für die FIU ist das besonders relevant. In den Analyse- und Auswertungseinheiten arbeiten zahlreiche technisch versierte Beschäftigte, die fachliche Anforderungen unmittelbar in digitale Lösungen überführen können.

Offene Technologie, kontrollierte Umgebung
Die FIU nutzt eine eigenentwickelte Open-Source-Plattform auf Basis der Programmiersprache Python. Es bestehen keine Abhängigkeiten von kommerziellen Anbietern. Die Plattform wird als containerbasierte Lösung bereitgestellt und lässt sich sowohl lokal als auch in skalierbaren Umgebungen betreiben. Zentrale Dienste wie Datenbanken, eine Nutzerverwaltung und eine Versionsverwaltung sind integriert. Für die Benutzer-

oberflächen der Anwendungen kommt das Python-Framework Streamlit zum Einsatz, das eine schnelle Umsetzung interaktiver Web-Oberflächen ermöglicht, ohne dass dafür Kenntnisse in der Web-Entwicklung erforderlich sind. Wesentliche Anforderungen an Datenschutz und IT-Sicherheit werden dabei bereits im Systemdesign abgebildet. Ein mehrstufiger Zugriffsmechanismus steuert die Berechtigungen auf Ebene einzelner Anwendungen. Die Anbindung an die zentrale Nutzerverwaltung der Generalzolldirektion stellt sicher, dass Rollen und Zugriffsrechte einheitlich administriert werden. Schreibende Zugriffe auf Datenbanken des Informationsverbundes erfolgen ausschließlich über abgesicherte Schnittstellen mit zusätzlichen Integritätsprüfungen.

i

Was ist Low-Code?

Low-Code-Plattformen ermöglichen die Erstellung von Software-Anwendungen mit deutlich reduziertem Programmieraufwand. Anstelle umfangreicher Programmierung in klassischen Entwicklungsumgebungen werden visuelle Werkzeuge, vorgefertigte Bausteine und standardisierte Schnittstellen genutzt. Der Ansatz richtet sich ausdrücklich auch an fachlich versierte Beschäftigte, sogenannte Citizen Developer, die Anwendungen für den eigenen Arbeitsbereich erstellen. Die FIU nutzt eine eigenentwickelte Open-Source-Plattform auf Basis der Programmiersprache Python.

»Citizen Development«
Beim Citizen-Development-Ansatz erstellen Beschäftigte der Fachbereiche eigenständig Anwendungen. Sie agieren als fachlich versierte Anwenderinnen und Anwender, die ihre operativen Anforderungen am besten kennen. Die IT-Organisation stellt hierfür die Plattform bereit und begleitet den Prozess durch klare und weitestgehend automatisierte Governance-Strukturen. Dazu zählen ein definierter Frei-

gabeprozess, Dokumentationsanforderungen und Regeln für den Lebenszyklus jeder Anwendung. Risiken, die mit einer dezentralen Entwicklung verbunden sein können, etwa eine Fragmentierung der Systemlandschaft, werden durch diese Einbettung adressiert. Der Ansatz ermöglicht kurze Reaktionszeiten auf veränderte fachliche Bedarfe und entlastet zugleich den IT-Fachbereich. »Die Einführung der Low-Code-Plattform verändert die Arbeitsweise der FIU grundlegend. Die Analytistinnen und Analysten sind nun in der Lage, eigenständig Werkzeuge zu bauen. Diese lassen sich exakt ihre fachlichen Fragestellungen zuschneiden und innerhalb von Tagen statt Monaten bereitstellen.«

Zwei Wege zur Fachanwendung Klassischer Entwicklungs- gegenüber Low-Code-Ansatz

Klassisch	Low-Code
Monate	Tage
bis zur produktiven Anwendung	bis zum funktionsfähigen Prototyp
1 Anforderungsaufnahme durch IT	1 Fachbereich formuliert Bedarf und baut Prototyp
2 Spezifikation und Freigabe	2 Governance-Freigabe, Qualitätssicherung und Dokumentation
3 Programmierung und Entwicklungsumgebung	3 Bereitstellung über Plattform
4 Test und Qualitätssicherung	
5 Deployment und Abnahme	

Abb. 10: Klassische Entwicklung und Low-Code-Ansatz im Vergleich

4.2 Neue Wege der Datenanalyse

Die im Vorjahr begonnene Weiterentwicklung datenbasierter Analyseverfahren wurde im Jahr 2025 fortgeführt. Anomalieerkennung und Netzwerkanalyse werden in der laufenden Analysearbeit der FIU zunehmend genutzt, insbesondere in den Projekten der Analyseeinheit »Sharks« (vgl. 5.2). Die Low-Code-Plattform der FIU unterstützt die schnellere Bereitstellung der hierfür erforderlichen Werkzeuge (vgl. 4.1). Maßgeblich für die Leistungsfähigkeit datenbasierter

Erste Anwendungen im operativen Einsatz
Im Jahr 2025 wurden erste Anwendungen auf Basis der Plattform in den operativen Betrieb überführt. Dazu zählt ein Konvertierungswerkzeug, das eingehende Informationen verschiedener Fachverfahren automatisiert in das jeweils erforderliche Format überführt. Die Anwendung arbeitet ohne Verbindung zu weiteren Komponenten des Informationsverbundes und lässt sich über eine administrative Oberfläche aktualisieren, ohne dass ein erneutes Deployment der Plattform erforderlich ist. Die Beispiele zeigen, wie sich wiederkehrende, datenintensive Arbeitsschritte durch gezielte Automatisierung beschleunigen lassen.

Verfahren bleibt die Qualität der verfügbaren Eingangsdaten. Die mit der GwGMeldV geschaffenen einheitlichen Meldeanforderungen (vgl. 3.1.1) verbessern diese Grundlage strukturell. Bei einem Gesamtmeldeaufkommen von 374.693 Verdachtsmeldungen mit rund 3,2 Millionen enthaltenen Transaktionen gewinnt die maschinelle Verarbeitbarkeit der Daten weiter an Bedeutung. Die Anwendung technischer Verfahren erfolgt ausschließlich innerhalb eines rechtsstaatlich abgesicherten Rahmens. Die Bewertung sensibler Sachverhalte bleibt Aufgabe der menschlichen Analyse.

Strategische Auswertung

5. Strategische Auswertung

Das im Vorjahr erarbeitete Konzept für die Strategische Auswertung hat sich im Jahr 2025 in der Praxis bewährt und wurde weiter konsolidiert. Der Reformprozess hat mit der Aufnahme der operativen Tätigkeit der Analyseeinheit »Sharks«, der Einführung des neuen Kommunikationsinstruments »FIU-Risikohinweis« und einer deutlich ausgeweiteten Produktpalette strategischer Berichte eine neue Qualitätsstufe erreicht.

5.1 Strategische Berichte und Analysen

Neben der operativen Analyse führt die FIU strategische Auswertungen und Analysen durch und erstellt entsprechende Berichte (§ 28 Absatz 1 Satz 4 Nr. 8 GwG). Die Arbeit dient der Feststellung von Trends und Entwicklungen sowie neuen Methoden im Bereich der Geldwäsche und Terrorismusfinanzierung. Die gewonnenen Erkenntnisse werden anschließend adressatengerecht aufbereitet. Die Auswertungen und Analysen der FIU fließen zudem in die Arbeiten des BMF zur Erstellung der Nationalen Risikoanalyse ein.

Im Jahr 2025 hat die Strategische Auswertung ihr Produktportfolio deutlich ausgebaut. Insgesamt wurden im Berichtsjahr über 50 strategische Produkte erstellt und an Partnerbehörden sowie Verpflichtete übermittelt. Diese gliedern sich in vier Produktkategorien.

Regelmäßiges Monitoring

Das monatliche Reporting zum Meldeaufkommen ist seit vielen Jahren fester Bestandteil der strategischen Produktpalette und wurde im Berichtsjahr fortgeführt. Es dient den Empfängern als Grundlage für die Beobachtung von Entwicklungen und als Ausgangsbasis für weiterführende Anfragen. Ergänzend wurden quartalsweise Sonderauswertungen zu Kryptowerten sowie zum grenzüberschreitenden Barmittelverkehr

erstellt. Darüber hinaus erfolgte eine monatliche regionale Auswertung der abgegebenen Analysekomplexe nach Bundesländern sowie eine jährliche Gesamtchau.

Erstmals wurde zudem ein fortlaufendes, strategisches Risikomonitoring eingeführt, das monatlich aktuelle Entwicklungen anhand von Veränderungen in den Meldungsströmen im Bereich der Geldwäsche abbildet und sowohl im In- als auch im Ausland auf positives Feedback stieß.

Anhaltspunktepapiere

Im Jahr 2025 wurden Papiere zu den Themen handelsbasierte Geldwäsche sowie Handel mit CO₂-Emissionszertifikaten erstellt. Das Anhaltspunktepapier zur handelsbasierten Geldwäsche wurde in einem neu entwickelten Format erarbeitet, das als Muster für kommende Publikationen dient. Das BKA nutzt in Abstimmung mit der FIU das Anhaltspunktepapier zu Emissionszertifikaten im Rahmen des Europol-EMPACT-Schwerpunktthemas Umweltkriminalität¹ gemeinsam mit entsprechenden Teilnehmerstaaten. Die Deutsche Emissionshandelsstelle des Umweltbundesamtes hat das Dokument im Register des nationalen Brennstoffemissionshandels eingestellt. Darüber hinaus wurde das bestehende Anhaltspunktepapier zu Transaktionen mit Bezug zu Kryptowerten und Kryptoverwahrgeschäften aktualisiert.

Auswertebereichte

Vertiefende Auswertebereichte wurden unter anderem zu Themenfeldern wie Umweltkriminalität und Emissionshandel erstellt und mitunter zuständigen Partnerbehörden zur Verfügung gestellt.

FIU-Risikohinweise

Als neues Produktformat wurden im Berichtsjahr erstmals FIU-Risikohinweise herausgegeben. Die ausführliche Darstellung findet sich in 5.3.

5.2 Die Analyseeinheit »Sharks« im ersten operativen Jahr

Im Jahresbericht 2024 wurde die Einrichtung der neuen Analyseeinheit »Sharks« vorgestellt. Die Einheit hat im Sommer 2024 ihre Arbeit aufgenommen und bereits mit dem Projekt »Barrakuda« ein erstes Ermittlungsverfahren unterstützt. Im Jahr 2025 hat sie den Übergang von der Aufbauphase in den regulären operativen Betrieb vollzogen und eine breitere Produktpalette bearbeitet.

Mit den »Sharks« greift die FIU wesentliche Empfehlungen der FATF aus der Deutschlandprüfung 2021/2022 auf. Sie richten ihre Analysen bedarfspezifisch auf die Strafverfolgungsbehörden aus und wenden den »Follow-the-Money-Ansatz« an. Hierfür nutzen sie die Befugnis der FIU zu sogenannten anlasslosen Analysen gemäß § 30 Absatz 2a GwG, um unabhängig vom Vorliegen einer Verdachtsmeldung Sonderauswertungen in Bezug auf den Datenbestand der FIU durchzuführen.

Projekt »Barrakuda«

Ein erstes bedeutendes Projekt der Sharks war die Unterstützung des Landeskriminalamt (LKA) Sachsen in einem Ermittlungsverfahren wegen gewerbsmäßigen Bandenbetrugs im Bereich Callcenter-Kriminalität (Projekt »Barrakuda«). Das LKA führte seit Februar 2022 Ermittlungen gegen eine Tätergruppierung, deren Betrugshandlungen Bezüge zu mehreren europäischen Ländern aufwiesen. Die Tätergruppe stand in Verbindung mit Strukturen der organisierten Kriminalität.

Ausgehend von über 1.000 Konto- und über 100 Personendaten, die das LKA zur Verfügung gestellt hatte, führten die Sharks umfangreiche Analysen im Datenbestand der FIU durch. Dabei zeigte sich einer der wesentlichen Vorteile der FIU. Der umfangreiche Datenpool aus Verdachtsmeldungen, Transaktionsdaten und beigefügten Informationen wie KYC-Daten und Kontoumsätzen ermöglicht es, personelle Verbindungen, finanzielle Verflechtungen und dahinter liegende Netzwerke sichtbar zu machen.

Ein weiterer Vorteil war der direkte Austausch mit zwei europäischen Partner-FIUs, wodurch Erkenntnisse zeitnah ausgetauscht sowie Maßnahmen wie Kontosperrungen ad hoc veranlasst werden konnten.

Im Ergebnis konnten die Sharks bei diesem Komplex, bei dem ein Schaden von rund 8 Millionen Euro durch über 30.000 Betrugsfälle entstand, insgesamt 110 relevante Verdachtsmeldungen, 35 bislang unbekannte Personen, 5 neue Konten und 10 Scheinfirmen identifizieren. Darüber hinaus konnten 66 Prozent der Konto- und Personendaten, zu denen zuvor keine hinreichenden Erkenntnisse vorlagen, durch die Analysen der Sharks ergänzt und verifiziert werden. Diese Erkenntnisse trugen dazu bei, bestehende Ermittlungslücken zu schließen.

Im Juni 2025 wurde zu diesem Komplex ein Action Day in fünf europäischen Ländern durchgeführt, bei dem drei Haftbefehle vollstreckt und zahlreiche Beweismittel gesichert werden konnten.

In einem Schreiben an die FIU würdigte die damalige Präsidentin des LKA Sachsen, Sonja Penzel, den wesentlichen Beitrag der Sharks zum Erfolg der Maßnahmen und dankte ausdrücklich für die »hohe Einsatzbereitschaft und die professionelle Unterstützung«.

»8 Mio. Euro Gesamtschaden durch über 30.000 Betrugsfälle. 110 relevante Verdachtsmeldungen und 35 bislang unbekannte Personen identifiziert.«

Projekt Barrakuda, 2025

¹ EMPACT (European Multidisciplinary Platform Against Criminal Threats) ist das ständige EU-Instrument für die behördenübergreifende operative Zusammenarbeit bei der Bekämpfung der organisierten und schweren internationalen Kriminalität; Europol unterstützt und koordiniert die Umsetzung. Weiterführende Informationen: www.europol.europa.eu/how-we-work/empact.

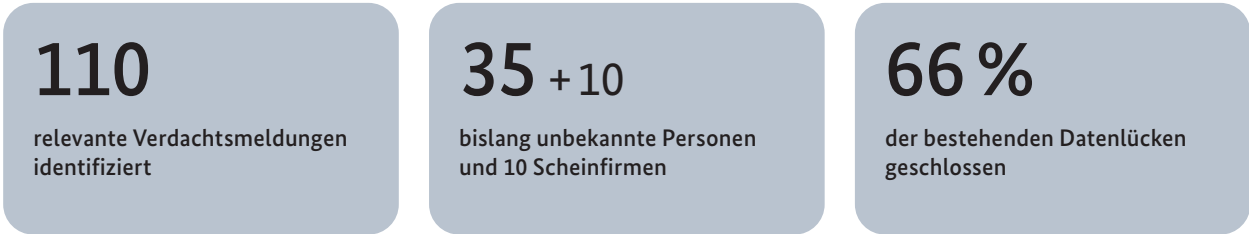


Abb. 11: Projekt »Barrakuda« in Zahlen

Internationales Projekt »TRACE«

Im Rahmen des Projekts »TRACE«, an dem mehrere internationale FIUs beteiligt sind und bei dem die Sharks eine Co-Lead-Rolle innehaben, wird Geldwäsche im Zusammenhang mit Kokainhandel betrachtet. Neben Analysen strategischer Art werden in der Projektgruppe auch konkrete gemeinsame operative Fallanalysen durchgeführt. Das Projekt steht exemplarisch für die verstärkte internationale Ausrichtung der strategischen Analysearbeit der FIU.

5.3 Der FIU-Risikohinweis als neues Instrument der externen Kommunikation

Im Jahr 2025 hat die FIU mit dem FIU-Risikohinweis ein neues Informationsinstrument eingeführt, das aktuelle Erkenntnisse zu Geldwäschetypologien und Modi Operandi gezielt an betroffene Verpflichtetengruppen und Behörden adressiert. Das Instrument soll Verpflichtete proaktiv auf erkannte Risiken hinweisen, damit Monitoring-Systeme frühzeitig angepasst und verdächtige Muster gezielter erkannt werden können. Der FIU-Risikohinweis umfasst eine kompakte Beschreibung der jeweiligen Typologie sowie prägnante Erkennungsmerkmale und wird auf maximal zwei Seiten begrenzt. Die Veröffentlichung erfolgt anlassbezogen und adressatenspezifisch. Erkennt ein Verpflichteter den beschriebenen Modus Operandi, ergänzt er die Verdachtsmeldung um einen entsprechenden Hashtag, der eine gezielte Auswertung durch die FIU ermöglicht. Bei Bedarf erfolgt zu einem festgelegten Zeitpunkt eine Aktualisierung des Risikohinweises.

Der erste FIU-Risikohinweis wurde im Oktober 2025 veröffentlicht und betraf auffällige Zahlungsmuster mit Bezug zu einem Drittland. Erste Erfahrungen zeigen, dass der FIU-Risikohinweis von den Empfängern positiv aufgenommen wird. Das relevante Meldungsaufkommen zu dem beschriebenen Modus Operandi ist nach Veröffentlichung des Risikohinweises deutlich angestiegen. Bei den Behörden trug der Risikohinweis dazu bei, Einzelfälle in einen Gesamtzusammenhang einzuordnen und laufenden Ermittlungen mitunter eine neue Dynamik zu verleihen. Der FIU-Risikohinweis ergänzt damit die Kommunikation zwischen FIU und Verpflichteten und behördlichen Partnern. Während Anhaltspunktepapiere einen grundlegenden analytischen Überblick bieten, ermöglicht der Risikohinweis eine zeitnahe, fallbasierte Warnung vor konkreten aktuellen Bedrohungen.

5.4 Ausgewählte Phänomenbereiche 2025

Die regelmäßige Beobachtung und Einordnung ausgewählter Phänomenbereiche ist ein wesentlicher Bestandteil der strategischen Analysearbeit der FIU. Für das Berichtsjahr wird im Folgenden der Bereich des informellen Werttransfers (Geldtransfer, Hawala und Underground Banking) zusammenfassend dargestellt. Der im Schwerpunktkapitel dieses Berichts behandelte Komplex des cybergestützten Betrugs (Operation Chargeback) bildet den übergreifenden thematischen Rahmen und wird an dieser Stelle nicht erneut aufgegriffen.

Funktionsweise des FIU-Risikohinweises

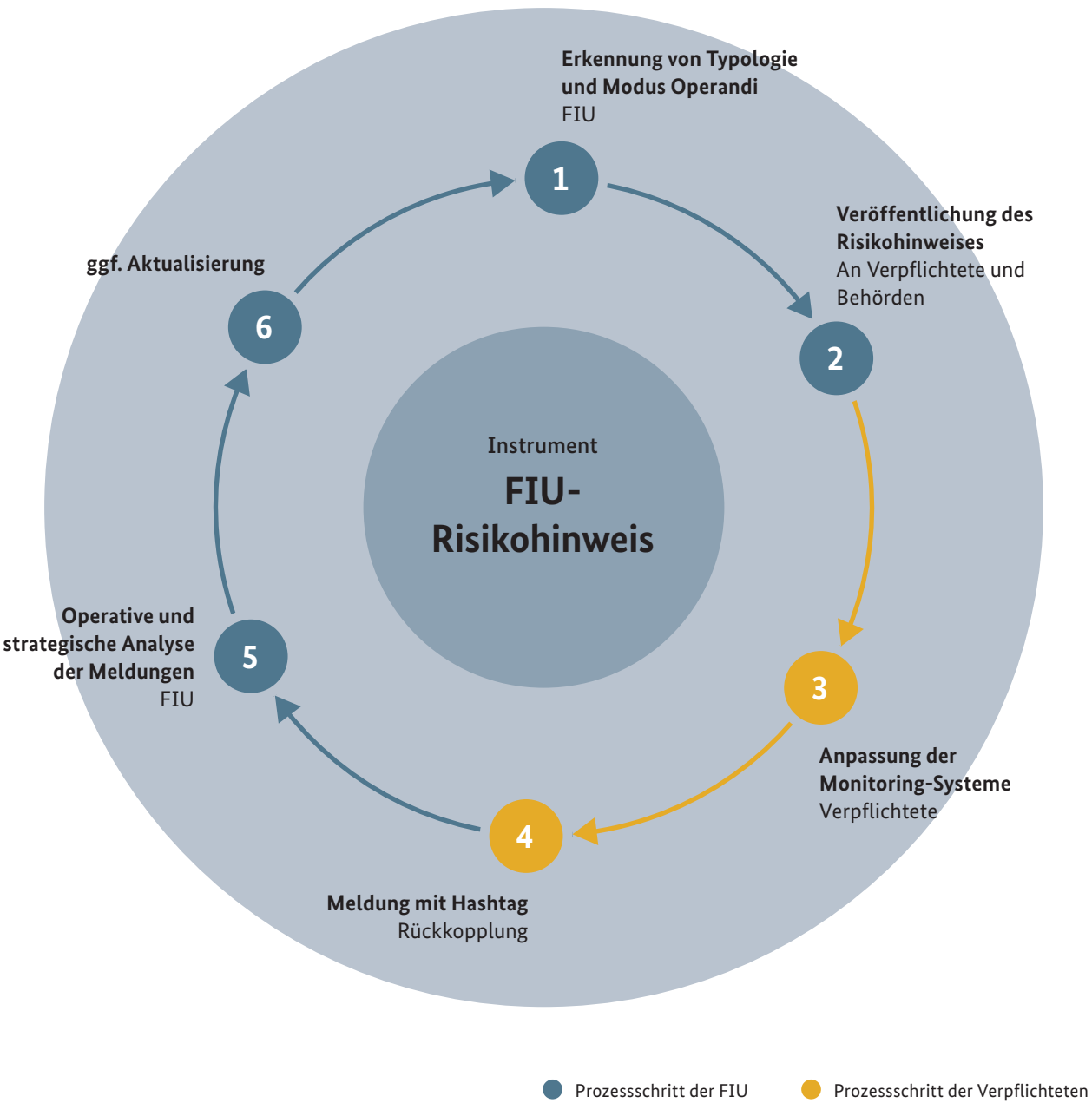


Abb. 12: Der FIU-Risikohinweis in sechs Schritten

Geldtransfer, Hawala und Underground Banking

Als Hawala wird ein informelles System zur Übertragung von Geldwerten bezeichnet, das außerhalb des beaufsichtigten Finanzsektors arbeitet und auf dem Vertrauen zwischen den beteiligten Vermittlern beruht. Ein Kunde zahlt einen Betrag bei einem Vermittler ein und nennt dem Empfänger ein Kennwort, gegen dessen Vorlage ein zweiter Vermittler am Zielort den Betrag auszahlt. Das Geld selbst wird dabei in der Regel nicht unmittelbar bewegt. Die entstehenden Forderungen halten die Vermittler fest und gleichen sie zu einem späteren Zeitpunkt untereinander aus, etwa durch gegenläufige Transfers, Warenlieferungen oder Bargeldkuriere. Die FATF unterscheidet rein traditionelle Anbieter, die legitime Überweisungen etwa für Wanderarbeiter abwickeln, hybride Anbieter, die zugleich legale und illegale Zwecke bedienen, und kriminelle Anbieter, die ihr Geschäft gezielt auf die Bedürfnisse krimineller Auftraggeber ausrichten. Für diese letzte Ausprägung wird auch der Begriff Criminal Underground Banking (CUB) verwendet. In Deutschland unterliegt der Betrieb von Finanztransfergeschäften nach dem Zahlungsdiensteaufsichtsgesetz einem Erlaubnisvorbehalt. Wer sie ohne die erforderliche Erlaubnis erbringt, macht sich strafbar. Das Phänomen verändert sich. Nach den Feststellungen der FATF ist der Missbrauch solcher Systeme längst nicht mehr auf klassische, bargeldintensive Vortaten wie den Betäubungsmittelhandel begrenzt. Die Anbieter arbeiten zunehmend professionell. Ihre Kundenstruktur ist breiter geworden, und die Systeme verzahnen sich enger mit dem regulären Finanzsektor. Hinzu tritt eine digitale Komponente. Traditionelle Verrechnungsmechanismen werden mit digitalen Mitteln kombiniert, etwa mit Kryptowerten zur Abwicklung oder Verschleierung der Werttransfers. Die Übergänge zwischen organisierter Kriminalität, der Nutzung von Kryptowerten und dem informellen Werttransfer sind dabei fließend.

Eine derzeit international besonders beachtete Ausprägung des CUB sind professionell organisierte Netzwerke, die grenzüberschreitend als Vermittler eines informellen Werttransfersystems auftreten. Sie verschieben Vermögenswerte außerhalb des regulierten Finanzsektors und nutzen dazu unter anderem die handelsbasierte Geldwäsche, Bargeldtransporte, so-

genannte Mirror-Transaktionen, bei denen sich gegenläufige Zahlungen in verschiedenen Ländern wertmäßig ausgleichen, und zunehmend Kryptowerte. Ein Teil der zugrunde liegenden Nachfrage entsteht dort, wo staatliche Kapitalausfuhrbeschränkungen einen Markt für den Transfer von Vermögenswerten außerhalb des regulierten Systems schaffen. Solche Netzwerke erbringen ihre Dienstleistungen für unterschiedliche kriminelle Auftraggeber, unter anderem für Drogenhandelsorganisationen, und wurden von internationalen Partnern zuletzt als bedeutende Geldwäschebedrohung eingestuft. Dabei lassen sich legale und kriminelle Nutzung nicht immer trennscharf unterscheiden, da in diesem Umfeld auch legitime Überweisungen und der Auslandseinkauf hochwertiger Waren vorkommen. Entsprechende Strukturen wurden auch in Europa festgestellt.

Die fortgesetzte Relevanz dieses Themenfeldes zeigt sich an zwei im Berichtsjahr abgeschlossenen Projekten. Das Projekt einer Arbeitsgruppe der AFCA und das durch das LKA Nordrhein-Westfalen koordinierte Projekt HAIFINS (Hawala Informal Financial Systems) haben zur Sensibilisierung gegenüber den besonderen Erscheinungsformen des informellen Zahlungsverkehrs beigetragen.

Die FIU beobachtet laufend das Meldeaufkommen im Hinblick auf Vorgänge mit Bezügen zu unerlaubt betriebenen Finanzdienstleistungen, CUB und Hawala-Banking. Mit den Partnerbehörden besteht ein fortlaufender Austausch. Die Identifizierung entsprechender Betreiber durch die Verpflichteten ist strukturell erschwert. Das Meldeaufkommen mit eindeutigen Bezügen zu diesem Phänomenbereich bleibt dementsprechend auf einem relativ niedrigen Niveau. Gleichwohl gelingt es im Rahmen der laufenden Überwachung wiederholt, Sachverhalte zu identifizieren, die eine vertiefte operative Analyse rechtfertigen.

Anhang

A.1 Aktuelle Zahlen

A.1.1 Abgegebene Analyseberichte



Abb. 13: Anzahl abgegebener Analyseberichte an Empfängerbehörden in den Jahren 2023 – 2025

- Die Zahl der im Jahr 2025 abgegebenen Analyseberichte ist im Vergleich zum Vorjahr um rund 24 % gesunken.
- Dies ist unter anderem auf die weitere Schärfung des risikobasierten Ansatzes mit Fokus auf Sachverhalte mit besonders hohem Risikopotenzial zurückzuführen.
- Komplexere Fälle erfordern tiefere Analysen und mehr analytische Werkzeuge, was zu weniger aber qualitativ werthaltigeren Übermittlungen führt.
- Dieser Prozess wird im Jahr 2026 fortgesetzt und weiter intensiviert.

A.1.2 Sofortmaßnahmen



Abb. 14: Sofortmaßnahmen (2023 – 2025)

- Anzahl und angehaltenes Gesamtvolumen der Sofortmaßnahmen haben im Berichtsjahr ihren Höchststand erreicht. Die Ursachen beider Entwicklungen sind jeweils eigener Natur.
- Der Anstieg bei der Zahl der Maßnahmen geht vorwiegend auf grenzüberschreitende Betrugsfälle zurück. 55 der insgesamt 106 Sofortmaßnahmen folgten internationalen Hinweisen und lösten jeweils eine Vielzahl von Einzelanordnungen bei mehreren Verpflichteten aus.
- Das außergewöhnlich hohe Gesamtvolumen geht vor allem auf eine einzelne Maßnahme zurück, mit der die Verfügung über 585 Mio. Euro untersagt wurde.

A.1.3 Anzahl der staatsanwaltschaftlichen Rückmeldungen

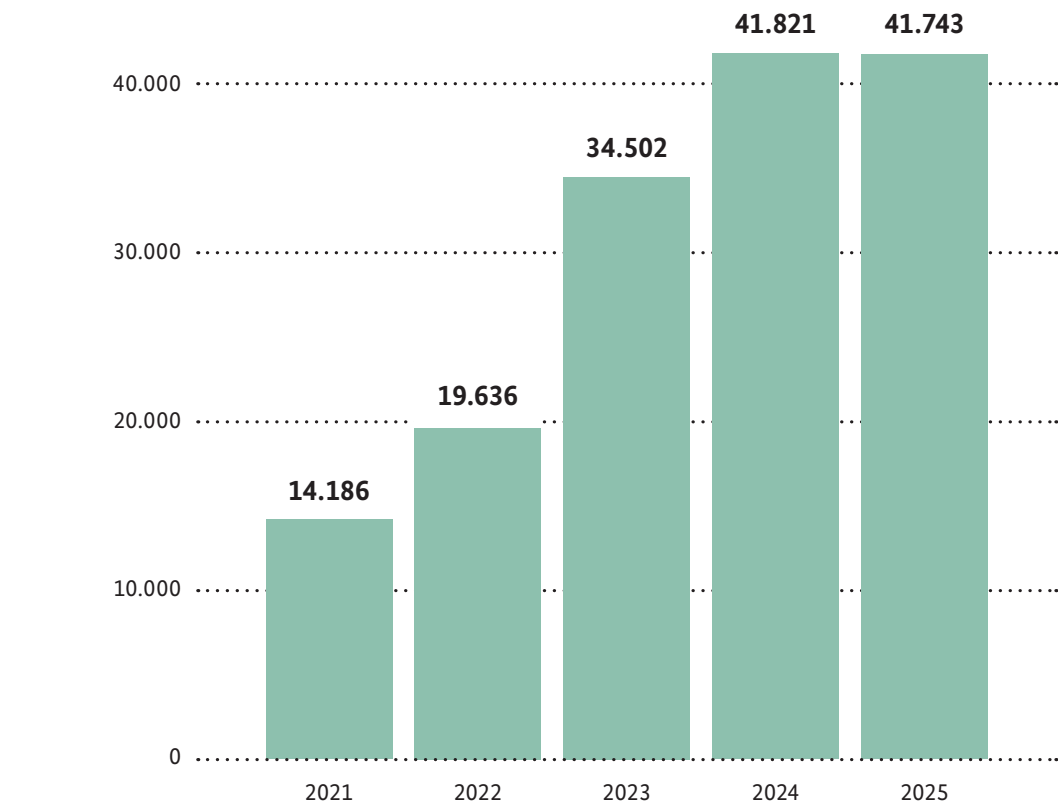


Abb. 15: Entwicklung Anzahl der staatsanwaltschaftlichen Rückmeldungen (2021 – 2025)

- In Strafverfahren, zu denen die FIU Informationen übermittelt hat, teilt die zuständige Staatsanwaltschaft der FIU die Erhebung der öffentlichen Klage und den Ausgang des Verfahrens einschließlich aller Einstellungsentscheidungen mit (§ 42 Absatz 1 GwG).
- Im Berichtsjahr gingen 41.743 solcher Rückmeldungen bei der FIU ein. Die Zahl bewegt sich damit auf dem Niveau des Vorjahres.

A.1.4 Staatsanwaltschaftlichen Rückmeldungen: Übersicht der Urteile, Strafbefehle, Beschlüsse und Anklageschriften

	2023	2024	2025	Veränderung 2024/2025
Urteile	202	256	247	↘
Strafbefehle	692	843	841	→
Beschlüsse	26	44	38	↘
Anklageschriften	434	482	543	↗
Gesamt	1.354	1.625	1.669	↗

Tabelle 2: Übersicht der Urteile, Strafbefehle, Beschlüsse und Anklageschriften (2023 – 2025)

- Bei insgesamt 1.669 Rückmeldungen handelt es sich um Urteile, Strafbefehle, Beschlüsse und Anklageschriften. Somit bilden Einstellungsverfügungen mit rund 96 % weiterhin den größten Anteil der staatsanwaltschaftlichen Rückmeldungen.
- Dies bedeutet nicht, dass keine Ergebnisse erzielt wurden. Die Informationen der FIU können auch für andere Zwecke genutzt werden, etwa zur Verfolgung der Vortat.

A.1.5 Eingegangene Verdachtsmeldungen nach dem GwG

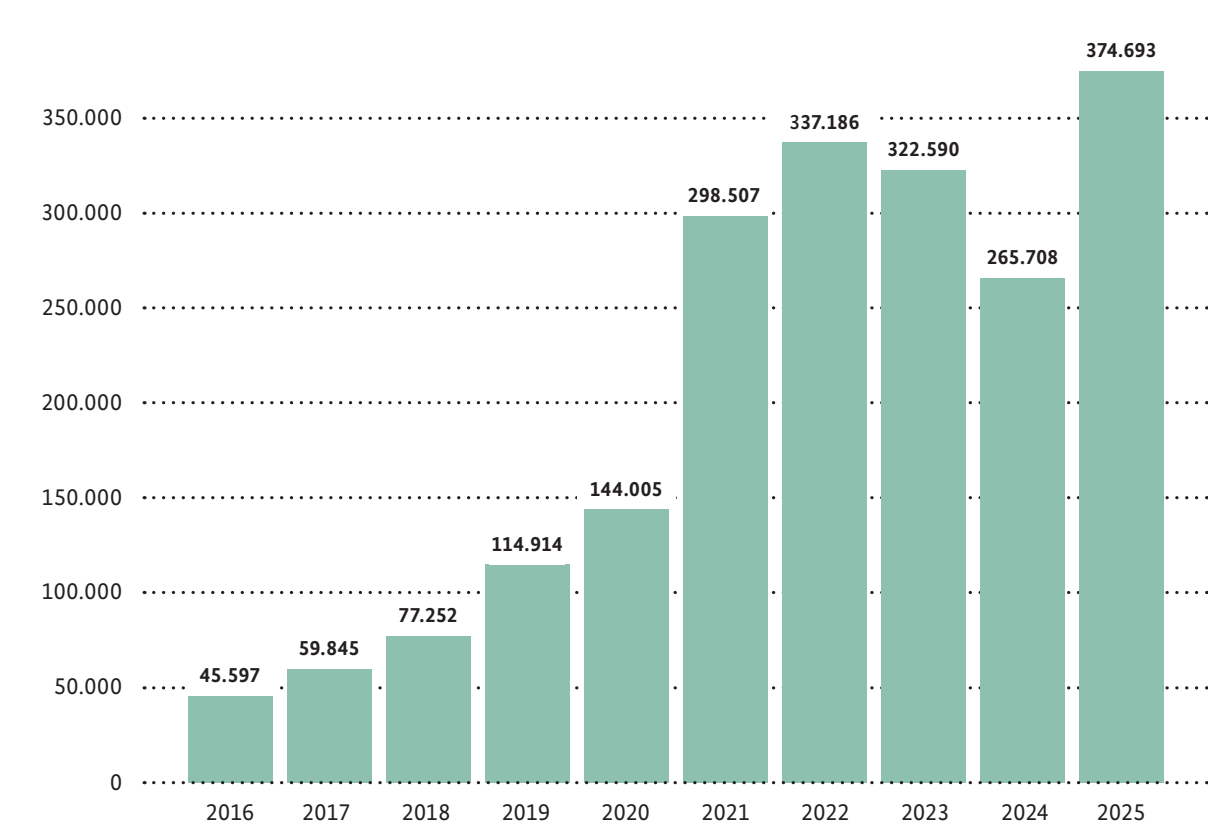


Abb. 16: Entwicklung der eingegangenen Verdachtsmeldungen nach dem GwG (2016–2025)

- Im Jahr 2025 ist nach den rückläufigen Entwicklungen der Vorjahre ein deutlicher Anstieg der eingehenden Verdachtsmeldungen um 41 % gegenüber dem Vorjahr auf 374.693 Meldungen zu verzeichnen.
- Der starke Anstieg des Gesamteldeaufkommens ist maßgeblich durch die Ausweitung von Geschäftsfeldern und den Markteintritt neuer Verpflichteter im Finanzsektor geprägt.
- Innerhalb des Finanzsektors haben digitale Finanzdienstleister, im Marktsprachgebrauch teilweise als Neo-banken bezeichnet, ihren Anteil am Meldeaufkommen deutlich erhöht.
- Bei rund 16 % aller im Jahr 2025 eingegangenen Verdachtsmeldungen handelte es sich um sogenannte Nach-meldungen. Diese beziehen sich auf früher eingegangene Meldungen und liefern weitere Informationen zum Sachverhalt. Im Vergleich zu den Vorjahren blieb die Quote der Nachmeldungen konstant (2024: 16 %, 2023: 15 %).

A.1.6 Verdachtsmeldungen mit potenziellem Bezug zu Terrorismusfinanzierung, Staatsschutz, Sanktionen

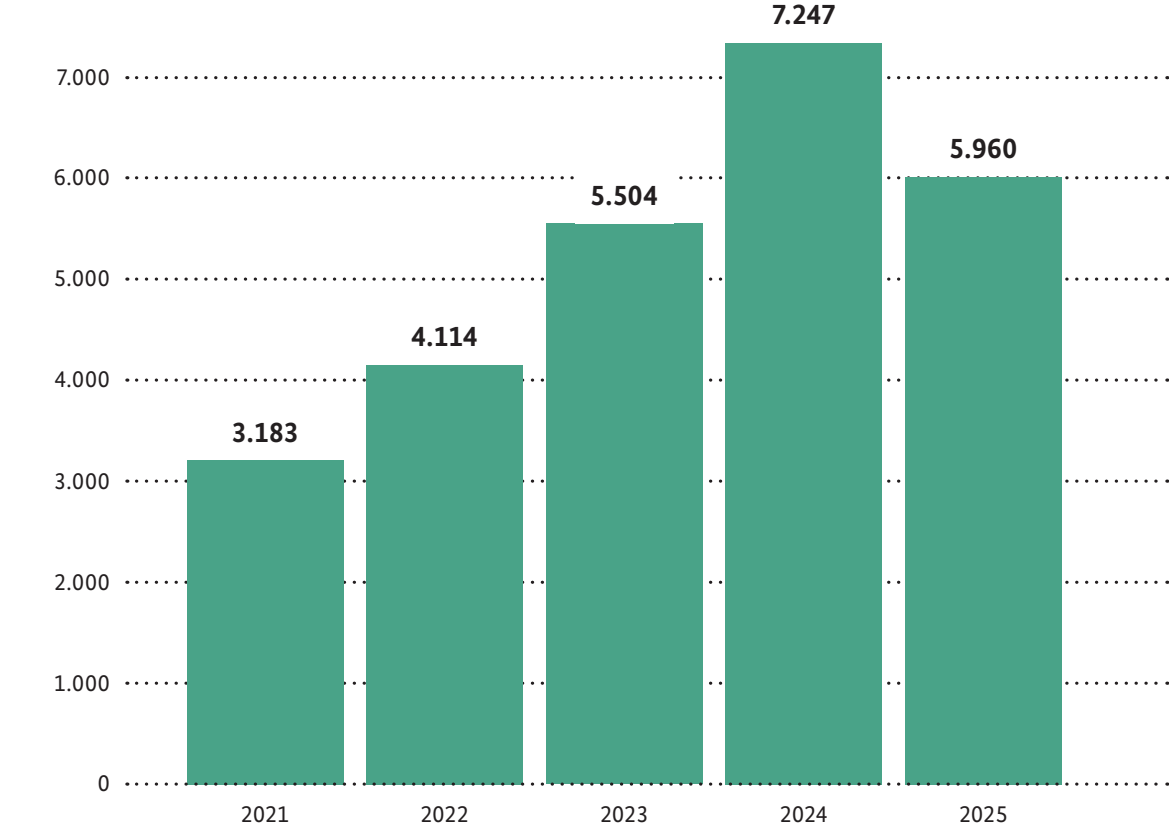


Abb. 17: Verdachtsmeldungen mit potenziellem Bezug zu Terrorismusfinanzierung, Staatsschutz, Sanktionen (2021 – 2025)

- Im Gegensatz zum steigenden Gesamtaufkommen ist die Zahl der Verdachtsmeldungen mit Bezug zu Terro-rismusfinanzierung, Staatsschutz, Sanktionen gegenüber dem Vorjahr zurückgegangen, bewegt sich jedoch weiterhin über dem Niveau von 2023.

A.1.7 Eingegangene Verdachtsmeldungen nach dem GwG nach Verpflichtetengruppen

	Verpflichtete	2023	2024	2025	Veränderung 2024/2025
Finanzsektor	Kreditinstitute	217.657	214.607	319.857	↗
	Finanzdienstleistungsinstitute	28.494	27.650	33.982	↗
	Zahlungsinstitute und E-Geld-Institute	63.764	10.152	9.217	↘
	Agenten	723	1.131	838	↘
	Selbstständige Gewerbetreibende	0	0	0	→
	Versicherungsunternehmen	269	271	298	↗
	Kapitalverwaltungsgesellschaften	49	36	40	↗
	Summe Verdachtsmeldungen Finanzsektor	310.956	253.847	364.232	↗
Nichtfinanzsektor	Finanzunternehmen	359	19	19	→
	Versicherungsvermittler	17	22	16	↘
	Rechtsanwälte	160	223	206	↘
	Kammerrechtsbeistände	0	0	0	→
	Patentanwälte	0	0	0	→
	Notare	7.305	7.739	6.612	↘
	Rechtsbeistände	0	2	1	↘

- Im Jahr 2025 ist ein deutlicher Anstieg der eingehenden Verdachtsmeldungen von verpflichteten Kreditinstituten zu verzeichnen.
- Der starke Anstieg ist maßgeblich durch die Ausweitung von Geschäftsfeldern und dem Markteintritt neuer Verpflichteter im Finanzsektor geprägt.
- Entgegen dem Trend im Finanzsektor ist die Zahl der Verdachtsmeldungen des Nichtfinanzsektors um rund 14 % zurückgegangen.
- Insbesondere bei der Gruppe der Notare und Immobilienmakler ist ein Rückgang erkennbar. Grund hierfür sind die am 17. Februar 2025 in Kraft getretenen Änderungen der Geldwäschegesetzmeldepflichtverordnung-Immobilien (GwGMeldV-Immobilien).

	Verpflichtete	2023	2024	2025	Veränderung 2024/2025
Nichtfinanzsektor	Wirtschaftsprüfer und vereidigte Buchprüfer	31	44	68	↗
	Steuerberater und Steuerbevollmächtigte	57	64	79	↗
	Treuhänder, Dienstleister für Treuhandgeschäfte	6	7	2	↘
	Lohnsteuerhilfeverein	0	0	0	→
	Immobilienmakler	260	270	193	↘
	Veranstalter und Vermittler von Glücksspielen	429	372	503	↗
	Dienstleister für Gesellschaften und für Treuhandvermögen (außer: Bürodienstleister/Business-Center)	1	3	6	↗
	Dienstleister i.S. von Bürodienstleister/Business-Center	3	9	7	↘
	Güterhändler	1.746	1.690	1.294	↘
	Summe Verdachtsmeldungen Nichtfinanzsektor	10.374	10.464	9.006	↘
Weitere	Aufsichtsbehörde	121	165	145	↘
	Finanzbehörden	956	1.097	1.230	↗
	Sonstige Verdachtsmeldungen	183	135	80	↘
	Gesamtsumme	322.590	265.708	374.693	↗

Tabelle 3: Anzahl der Verdachtsmeldungen, differenziert nach Verpflichtetengruppen (2023 – 2025)

- Die Gesetzesänderung zielt darauf ab Geldwäsche im Immobiliensektor noch effektiver zu bekämpfen. Neben der Erweiterung von meldepflichtigen Sachverhalten wurden hierfür Verdachtstatbestände durch klare Schwellwerte konkretisiert und zu weit gefasste Verdachtstatbestände eingeschränkt. Hierdurch konnten Unsicherheiten bei der Meldepflicht deutlich reduziert und zahlreiche nicht werthaltige Verdachtsmeldungen ausgeschlossen werden.
- Die bei den verpflichteten Güterhändlern erkennbare Verringerung des Meldeaufkommens ist maßgeblich durch das Meldeverhalten einzelner Verpflichteter geprägt.

A.1.8 Anzahl neu registrierter Verpflichteter

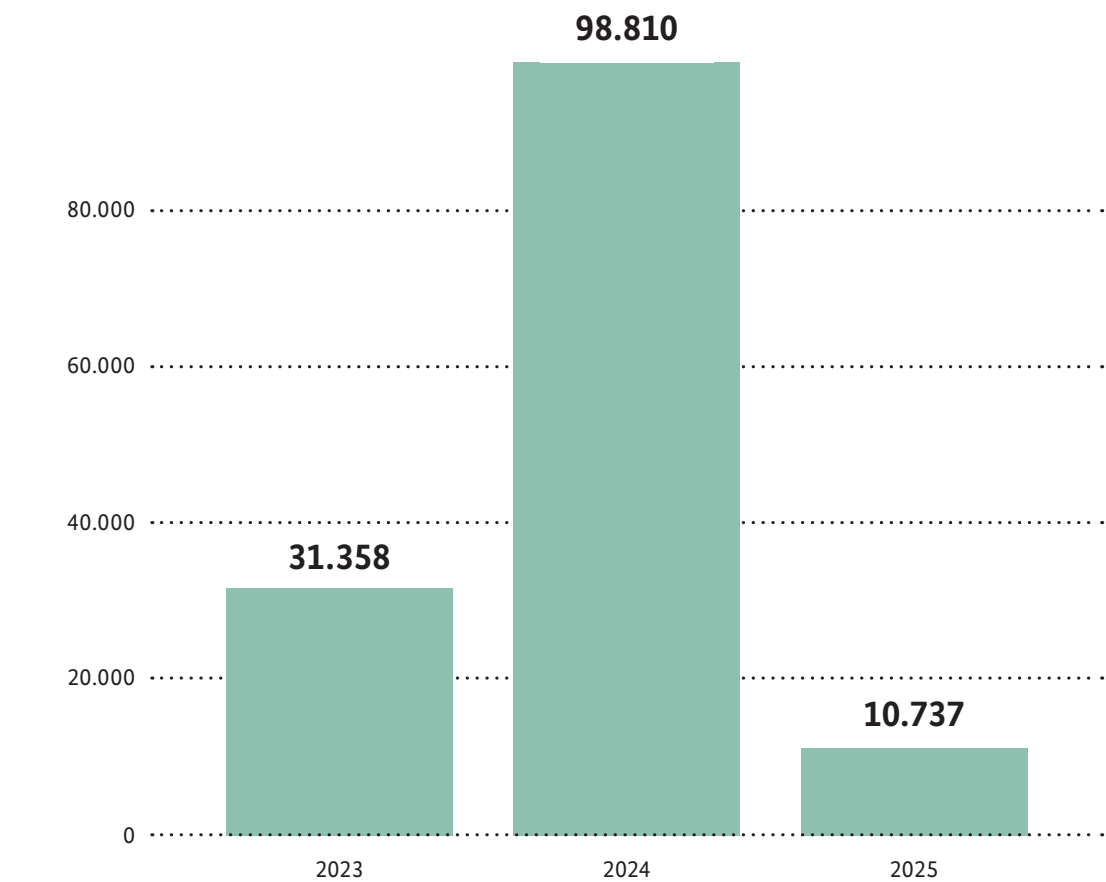


Abb. 18: Anzahl neu registrierter Verpflichteter (2023 – 2025)

- Im Jahr 2025 ist die Zahl der bei der FIU neu registrierten Verpflichteten im Vergleich zum Vorjahr deutlich zurückgegangen.
- Der in den Jahren 2023 und 2024 verzeichnete außergewöhnlich starke Anstieg stand insbesondere im Zusammenhang mit der ab dem 1. Januar 2024 geltenden verpflichtenden Registrierung von Verpflichteten bei der FIU (§ 45 Absatz 1 Satz 2 i.V.m. § 59 Absatz 6 Satz 1 GwG), infolge derer zahlreiche Verpflichtete ihre Registrierung erstmals vornahmen.

A.1.9 Anzahl automatisierter Datenabfragen bei der FIU gemäß § 32 Absatz 4 GwG



Abb. 19: Anzahl automatisierter Datenabfragen bei der FIU gemäß § 32 Absatz 4 GwG (2023 – 2025)

- Strafverfolgungsbehörden, das BKA sowie das BfV sind gemäß § 32 Absatz 4 GwG berechtigt, die Daten zur Erfüllung ihrer Aufgaben auch automatisiert bei der FIU abzurufen.
- Hierfür hat die FIU bereits im Jahr 2022 eine entsprechende Schnittstelle bereitgestellt, über die sich zunehmend mehr abrufberechtigte Behörden an den automatisierten Abruf anbinden.
- Entsprechend ist die Zahl der automatisierten Abrufe im Berichtsjahr deutlich gestiegen und liegt rund 58 % über dem Vorjahreswert.

A.1.10 Eingehende Ersuchen inländischer Behörden

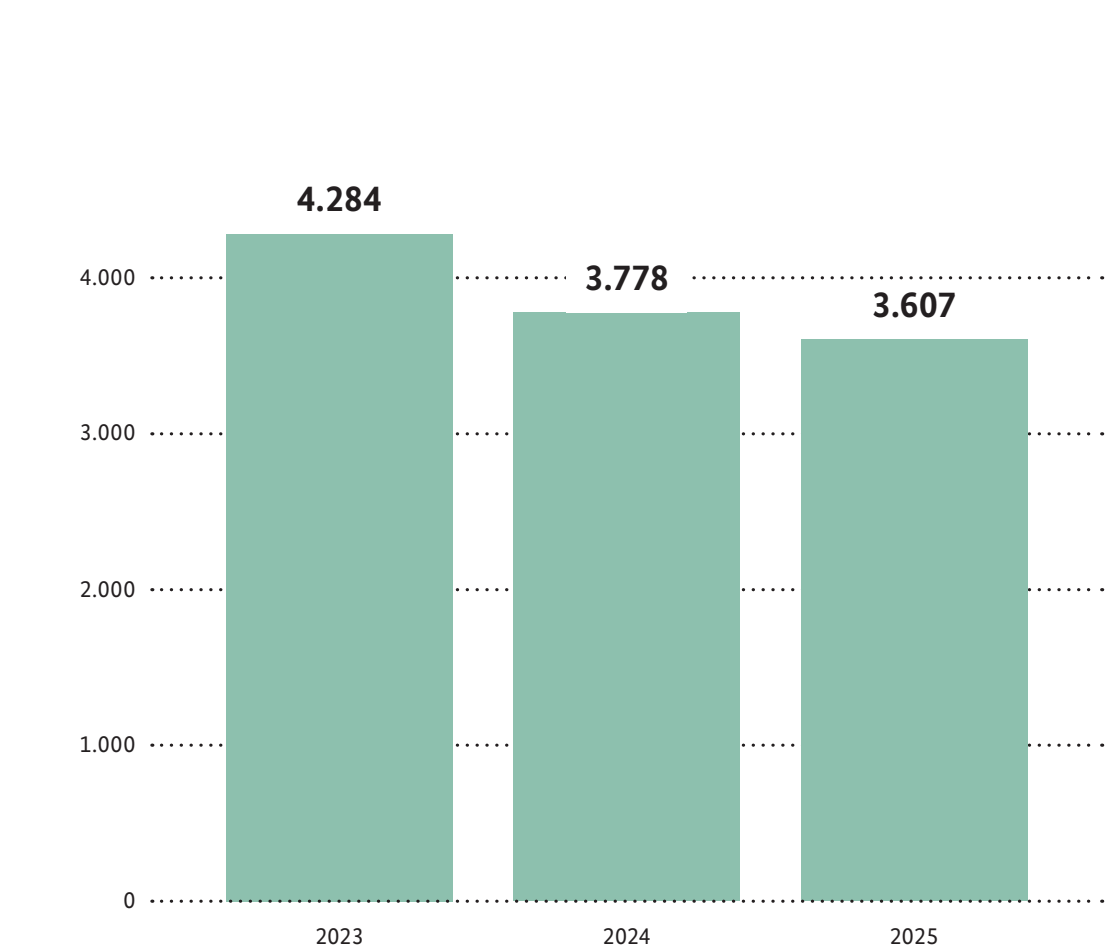


Abb. 20: Eingehende Ersuchen inländischer Behörden gesamt (2023 – 2025)

- Im Rahmen der behördlichen Zusammenarbeit stellt die FIU Daten aus Finanzinformationen und Finanzanalysen zur Verfügung, sofern diese zur Aufgabenerfüllung der ersuchenden Behörde im Zusammenhang mit der Verhinderung und Verfolgung von Geldwäsche und Terrorismusfinanzierung erforderlich sind (§ 32 Absatz 3 GwG).
- Die Zahl der entsprechenden Auskunftersuchen ist im Berichtsjahr wie bereits im Vorjahr leicht rückläufig.
- Gleichzeitig ist ein deutlicher Anstieg der Zahl automatisierter Datenabrufe gemäß § 32 Absatz 4 GwG zu verzeichnen, die die manuellen Auskunftersuchen ergänzen und mitunter ersetzen.

A.1.11 Verteilung ersuchende inländische Behörden

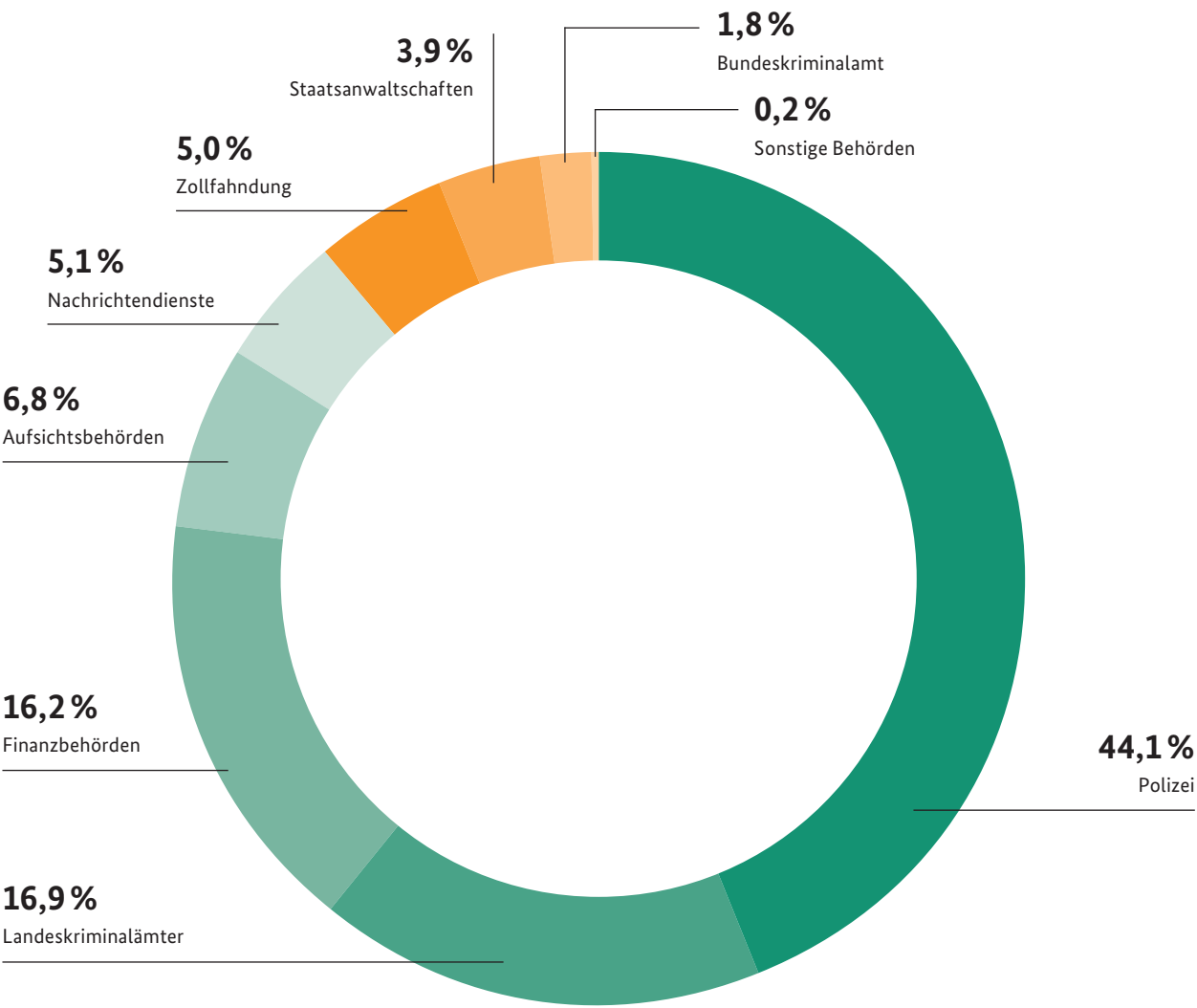


Abb. 21: Verteilung ersuchende inländische Behörden gesamt (2025)

A.1.12 Eingehende Ersuchen inländischer Behörden im Bereich Terrorismusfinanzierung, Staatsschutz, Sanktionen

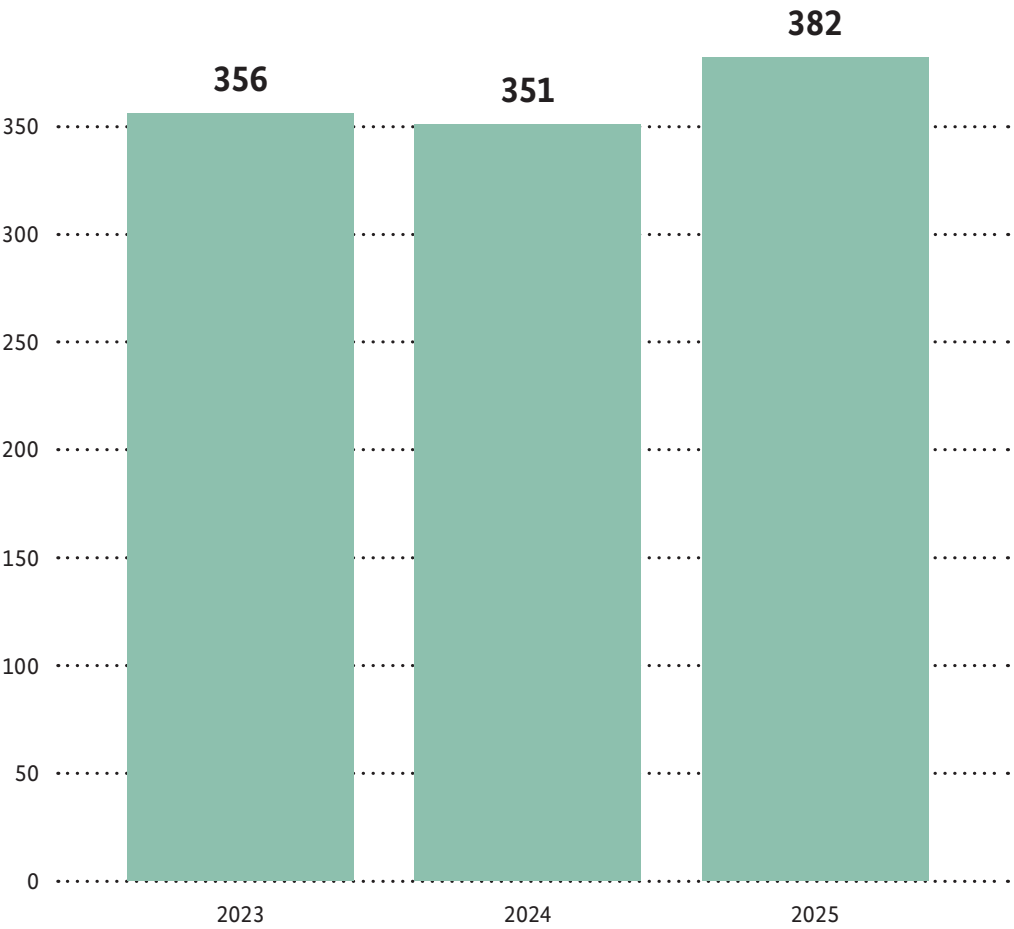


Abb. 22: Eingehende Ersuchen inländischer Behörden im Bereich Terrorismusfinanzierung, Staatsschutz, Sanktionen (2023 – 2025)

A.1.13 Verteilung ersuchende inländische Behörden im Bereich Terrorismusfinanzierung, Staatsschutz, Sanktionen

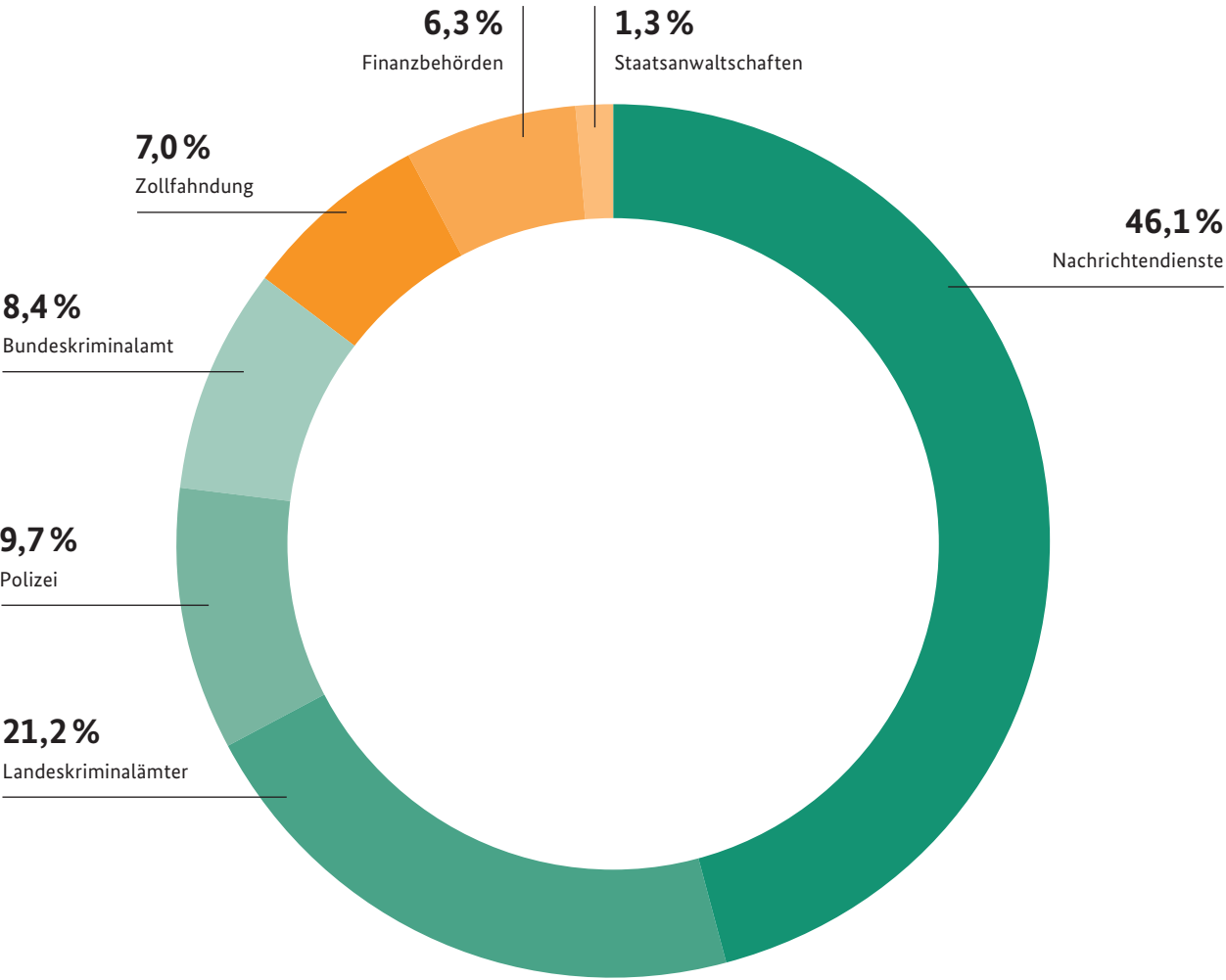


Abb. 23: Verteilung ersuchende inländische Behörden im Bereich Terrorismusfinanzierung, Staatsschutz, Sanktionen nach Absender (2025)

A.1.14 Internationale Ersuchen im Überblick

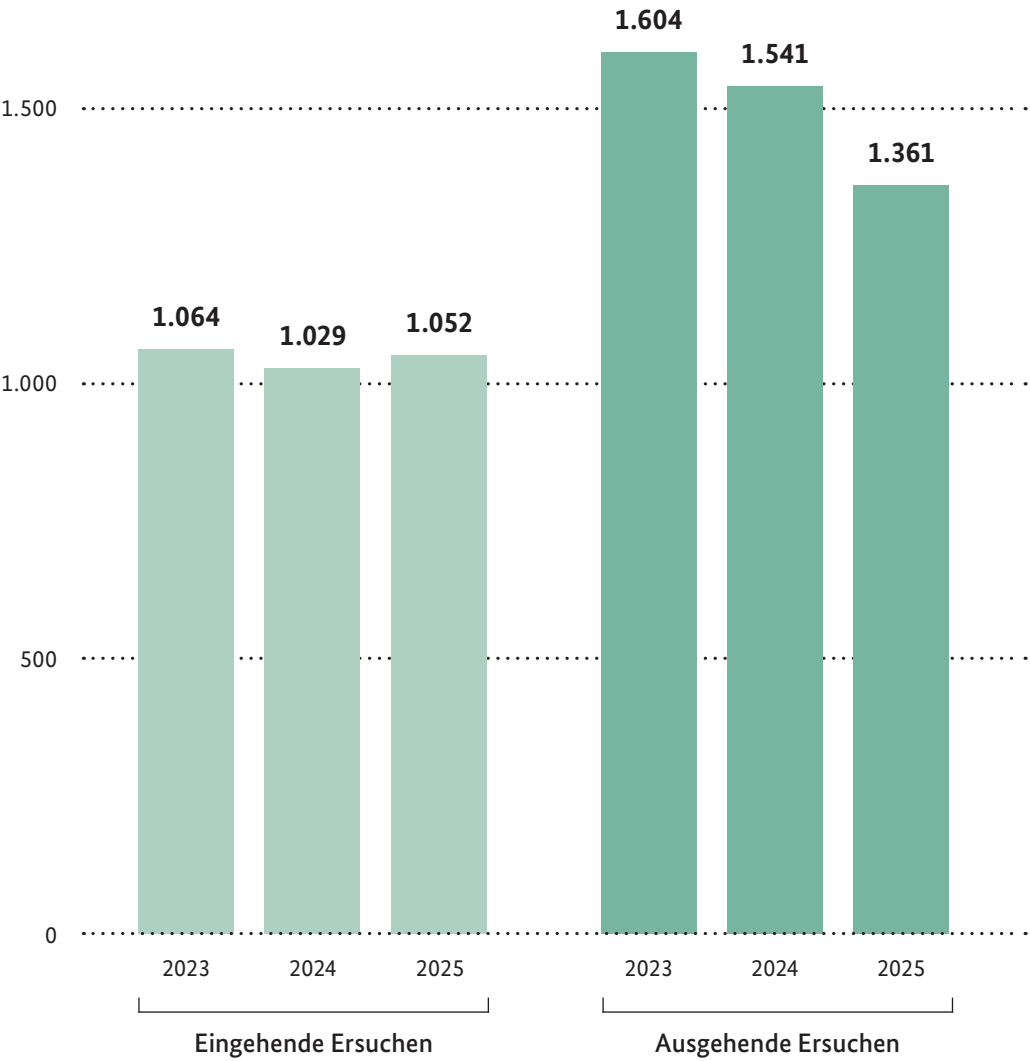


Abb. 24: Internationale Ersuchen im Jahresvergleich gesamt (2023 – 2025)

- Bei der FIU gingen im Berichtsjahr 1.052 Ersuchen aus dem Ausland ein. Die Zahl der eingehenden Ersuchen bleibt damit auf dem Vorjahresniveau.
- Zugleich richtete die FIU im Berichtsjahr 1.361 internationale Ersuchen an Partner-FIUs, nach 1.541 im Vorjahr.

A.1.15 Internationale Ersuchen mit Bezug zu Terrorismusfinanzierung, Staatsschutz, Sanktionen

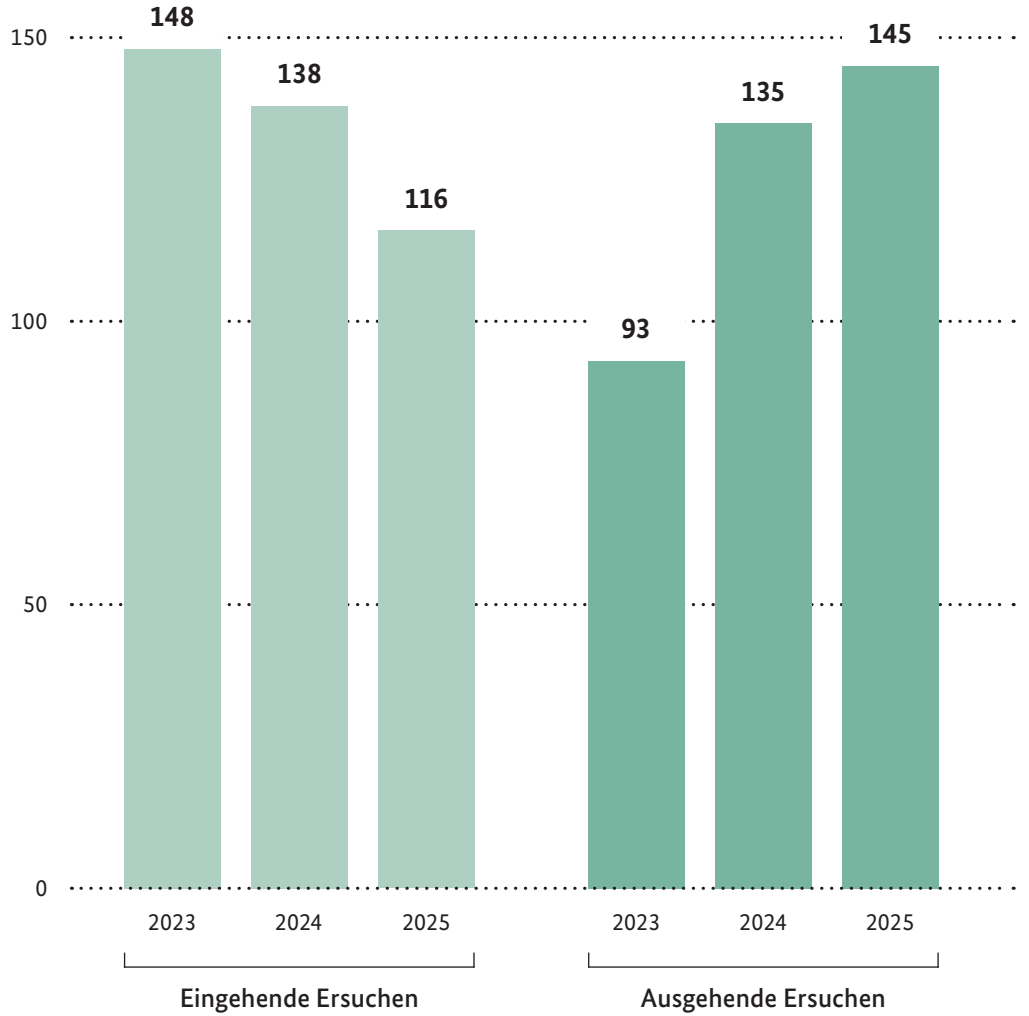


Abb. 25: Internationale Ersuchen mit Bezug zu Terrorismusfinanzierung, Staatsschutz, Sanktionen im Jahresvergleich (2023 – 2025)

A.1.16 Von den Zollbehörden gemäß Artikel 9 der Verordnung (EU) 2018/1672 (BarmittelVO) übermittelte Daten zu grenzüberschreitenden physischen Barmitteltransfers

	Verbringen von Barmitteln bei der Einreise aus einem Drittland		Verbringen von Barmitteln bei der Ausreise in ein Drittland	
	Anzahl	in Mio. €	Anzahl	in Mio. €
Ordnungsgemäß abgegebene Barmittelanmelde- erklärungen BarmittelVO Artikel 3	8.434	23.077	12.355	17.405
davon mit Annahmegründen Geldwäsche/Terrorismusfinanzierung BarmittelVO Artikel 10 Absatz 1 Buchstabe c	19	1,1	16	0,8
Von Amts wegen erstellte Barmittelanmeldeerklärungen BarmittelVO Artikel 5 Abs. 3 und Artikel 6 Absatz 1	666	11,7	2.210	38,1
davon mit Annahmegründen Geldwäsche/Terrorismusfinanzierung BarmittelVO Artikel 10 Absatz 1 Buchstabe b und c	88	0,2	608	10,8
Von Amts wegen erstellte Offenlegungserklärungen BarmittelVO Artikel 5 Absatz 3 und Artikel 6 Absatz 2	1	0,006	2	0,00
davon mit Annahmegründen Geldwäsche/Terrorismusfinanzierung BarmittelVO Artikel 10 Absatz 1 Buchstabe b und c	1	0,006	2	0,005

Tabelle 4: Barmittelanmeldeerklärungen und Offenlegungserklärungen gemäß Artikel 9 BarmittelVO (2025)

- Als nationale zentrale Meldestelle erhält die FIU Informationen aus der Überwachung des grenzüberschreitenden Barmittelverkehrs, § 30 Absatz 1 Nr. 3 a und b GwG. Eine Ausweisung der Statistiken erfolgt erstmalig mit diesem Jahresbericht.
- Für das Berichtsjahr 2025 wurden, zum Datenstand 23. März 2026, insgesamt 23.665 Barmittelanmeldeerklärungen (begleiteter Barmitteltransfer) und 3 Offenlegungserklärungen (unbegleiteter Barmitteltransfer) gemäß Artikel 9 der Verordnung (EU) 2018/1672 (BarmittelVO) im Zollinformationssystem (ZIS) erfasst.
- Bei rund 7 % der Barmittelanmeldeerklärungen wurde ein Betrag über 1.000.000 Euro angegeben; diese Barmittel werden vornehmlich durch gewerbsmäßige Geldkuriere angemeldet und transportiert. Der Hauptanteil der Barmitteltransfers, rund 56 %, weist einen Betrag zwischen 10.000 und 30.000 Euro auf.
- Bei rund 3,1 % der Barmittelanmeldeerklärungen und Offenlegungserklärungen liegen Annahmegründe für Geldwäsche oder Terrorismusfinanzierung vor. Etwa 47 % dieser Barmitteltransfers umfassen einen Betrag von weniger als 10.000 Euro und liegen damit unterhalb des Schwellwerts. Weitere 24 % entfallen auf Beträge ab 10.000 Euro bis 15.000 Euro. Etwa 29 % dieser Barmitteltransfers umfassen Beträge über 15.000 Euro.
- Betreffende Informationen nutzt die FIU einzelfallspezifisch im Rahmen ihrer Analysearbeit; seit 2019 hat die FIU in Übereinstimmung mit den Ergebnissen der Nationalen Risikoanalyse und in Abstimmung mit Strafverfolgungsbehörden unter anderem zum Einsatz von Bargeld einen spezifischen Risikoschwerpunkt gebildet.

A.1.17 Anzahl der Stammbeschäftigten der FIU



Abb. 26: Anzahl der Stammbeschäftigten der FIU zum 31. Dezember 2025

Verzeichnisse

Abbildungsverzeichnis

Abbildung	Titel	Seite
1	FIU in Zahlen 2025	12
2	Anzahl der automatisierten Abrufe (2023 – 2025)	15
3	Modus Operandi der Beschuldigten	19
4	Typischer Ablauf einer Abofalle	21
5	Kennzahlen der Operation Chargeback	25
6	Der Weg bis zur GwGMeldV (2017 – 2026)	29
7	Informationsaustausch mit Verpflichteten und Aufsichtsbehörden 2025	33
8	Sechs Tage vom Fristfall zur EUStA-Übernahme	41
9	Internationale Formate und Mitgliedschaften der FIU	43
10	Klassische Entwicklung und Low-Code-Ansatz im Vergleich	47
11	Projekt »Barrakuda« in Zahlen	52
12	Der FIU-Risikohinweis in sechs Schritten	53
13	Anzahl abgegebener Analyseberichte an Empfängerbehörden in den Jahren 2023 – 2025	58
14	Sofortmaßnahmen (2023 – 2025)	59
15	Entwicklung Anzahl der staatsanwaltschaftlichen Rückmeldungen (2021 – 2024)	60
16	Entwicklung der eingegangenen Verdachtsmeldungen nach dem GwG (2016 – 2025)	62
17	Verdachtsmeldungen mit potenziellem Bezug zu Terrorismusfinanzierung, Staatsschutz, Sanktionen (2021 – 2025)	63
18	Anzahl neu registrierter Verpflichteter (2023 – 2025)	66
19	Anzahl automatisierter Datenabfragen bei der FIU gemäß § 32 Absatz 4 GwG (2023 – 2025)	67

20	Eingehende Ersuchen inländischer Behörden gesamt (2023 – 2025)	68
21	Verteilung ersuchende inländische Behörden gesamt (2025)	69
22	Eingehende Ersuchen inländischer Behörden im Bereich Terrorismusfinanzierung, Staatsschutz, Sanktionen (2023 – 2025)	70
23	Verteilung ersuchende inländische Behörden im Bereich Terrorismusfinanzierung, Staatsschutz, Sanktionen nach Absender (2025)	71
24	Internationale Ersuchen im Jahresvergleich gesamt (2023 – 2025)	72
25	Internationale Ersuchen mit Bezug zu Terrorismusfinanzierung, Staatsschutz, Sanktionen im Jahresvergleich (2023 – 2025)	73
26	Anzahl der Stammbeschäftigten der FIU zum 31. Dezember 2025	75

Tabellenverzeichnis

Tabelle	Titel	Seite
1	Gesamtmeldeaufkommen und Anteil digitaler Finanzdienstleister 2022 – 2025	13
2	Übersicht der Urteile, Strafbefehle, Beschlüsse und Anklageschriften (2023 – 2025)	61
3	Anzahl der Verdachtsmeldungen, differenziert nach Verpflichtetengruppen (2023 – 2025)	64/65
4	Barmittelanmeldeerklärungen und Offenlegungserklärungen gemäß Artikel 9 BarmittelVO (2025)	74

Abkürzungsverzeichnis

AFCA	Anti Financial Crime Alliance
AML	Anti-Money Laundering (Geldwäschebekämpfung)
AMLA	Anti-Money Laundering Authority
AMLD6	Anti-Money Laundering Directive (6. EU-Geldwäscherichtlinie)
AO	Abgabenordnung
AuA	Auslegungs- und Anwendungshinweise
Bafin	Bundesanstalt für Finanzdienstleistungsaufsicht
BarmittelVO	Verordnung (EU) 2018/1672 über die Überwachung von Barmitteln, die in die Union oder aus der Union verbracht werden
BGBL	Bundesgesetzblatt
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BMF	Bundesministerium der Finanzen
CaaS	Crime-as-a-Service
CSAE	Child Sexual Abuse and Exploitation
CTFTI	Counter Terrorist Financing Taskforce Israel
CUB	Criminal Underground Banking
EFIPPP	Europol Financial Intelligence Public Private Partnership
EFTA	Europäische Freihandelsassoziation
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EU	Europäische Union
EU-AMLR	Anti-Money Laundering Regulation (EU-Geldwäscheverordnung; Verordnung (EU) 2024/1624)
EUStA	Europäische Staatsanwaltschaft

FATF	Financial Action Task Force
FinmadiG	Finanzmarktdigitalisierungsgesetz
FIU.net	Kommunikationsnetzwerk zum sicheren Austausch von Informationen zwischen FIUs der Europäischen Union und der EFTA-Staaten Norwegen, Island und Liechtenstein
GenStA	Generalstaatsanwaltschaft
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
goAML	System zur elektronischen Abgabe von Verdachtsmeldungen
GwG	Geldwäschegesetz, zuletzt geändert durch Artikel 53 des Gesetzes vom 4. Februar 2026 (BGBl. 2026 I Nr. 33)
GwGMeldV	GwG-Meldeverordnung
GwGMeldV-Immobilien	Verordnung zu den nach dem Geldwäschegesetz meldepflichtigen Sachverhalten im Immobilienbereich
HAIFINS	Hawala Informal Financial Systems
IT	Informationstechnik
KYC	Know Your Customer
LKA	Landeskriminalamt
LZC	Landeszentralstelle Cybercrime
NFS	Nichtfinanzsektor
OSINT	Open Source Intelligence
PPP	Public Private Partnership
RRIFS	Russia-Related Illicit Finance and Sanctions
ZAG	Zahlungsdiensteaufsichtsgesetz
ZIS	Zollinformationssystem

Impressum

Herausgeber

Generalzolldirektion
Financial Intelligence Unit (FIU)
Postfach 85 05 55
51030 Köln

Redaktion

Financial Intelligence Unit (FIU)

Gestaltung und Herstellung

Generalzolldirektion
Bildungs- und Wissenschaftszentrum
der Bundesfinanzverwaltung
Reg.-Nr.: SAB 272

Köln, Juli 2026

www.fiu.bund.de

