Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Meldestelle für Geldwäscherei (MROS)

Jahresbericht 2023

Mai 2024

Meldestelle für Geldwäscherei (MROS)

Jahresbericht 2023

Mai 2024

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol
Meldestelle für Geldwäscherei
3003 Bern

Telefon: (+41) 58 463 40 40
E-Mail: *meldestelle-geldwaescherei@fedpol.admin.ch*

Internet: *www.fedpol.admin.ch*

Inhaltsverzeichnis

1. Vorwort

Im letzten Jahrzehnt sind die Verdachtsmeldungen im Durchschnitt jährlich um 20–30 % angestiegen. Dieser Trend setzte sich 2023 fort – der Anstieg war jedoch erheblich steiler, als dies zu erwarten war. Per Ende des Jahres 2023 verzeichnete die Meldestelle für Geldwäscherei (MROS[1]) gesamthaft 11 876 Meldungen; dies entspricht geschätzten 21 500 Geschäftsbeziehungen und im Durchschnitt 47 Verdachtsmeldungen pro Werktag. Im Vergleich zum Vorjahr stellt dies eine Zunahme von 56 % dar.

Generell hat das gesamte Reporting- und Datenvolumen zugenommen. Bei der MROS sind im Jahr 2023 gesamthaft 21 375 Reportings eingegangen: Verdachtsmeldungen, Antworten der Finanzintermediäre auf Anfragen der MROS (Art. 11*a* GwG[2]), Abbruchsmitteilungen (Art. 9*b* GwG), internationale Anfragen von anderen Financial Intelligence Units (FIUs) sowie Spontaninformationen nationaler und internationaler Behörden (vgl. Kap. 4). Die Kommunikation mit den Finanzintermediären erfolgt fast ausschliesslich über das Informationssystem goAML. Die Daten werden von den Finanzintermediären mehrheitlich strukturiert eingereicht. Diese Entwicklung ist erfreulich. Indessen besteht auf Behördenseite noch Potenzial – der Anteil an unstrukturierten Daten ist hier nach wie vor sehr hoch und macht derzeit einen Anteil von knapp 30 % des gesamten Datenvolumens aus (vgl. Kap. 3).

Im Jahr 2023 hat die MROS insgesamt 866 Anzeigen an die Strafverfolgungsbehörden getätigt. Dies entspricht einem Rückgang von knapp 30 % gegenüber dem Vorjahr. Ursache ist unter anderem die Strategie der MROS, risikobasiert zu agieren und sich auf Schwerstkriminalität zu fokussieren. Die von der MROS erstellten Analysen in diesem Bereich gehen tiefer und sind aufwändiger. So übermittelte die MROS im 2023 43 % mehr Anzeigen an die Bundesanwaltschaft als im Vorjahr; die kantonalen Übermittlungen sind dagegen – mit Ausnahme der Staatsanwaltschaft Genf – rückläufig. Übrigens fielen im Jahr 2023 die Übermittlungen wegen COVID-Betrug gänzlich weg. Weiter werden in den Anzeigen an die Strafverfolgungsbehörden vermehrt verschiedene Verdachtsmeldungen gebündelt – die Fallzählung fällt demnach tiefer aus und ein Vergleich mit den Vorjahren ist nur bedingt aussagekräftig (vgl. Kap. 2.2).

Bern, im Mai 2024

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol
Meldestelle für Geldwäscherei MROS

[1] Money Laundering Reporting Office Switzerland.

[2] Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereigesetz, GwG), SR **955.0**.

2. Wichtige strategische Entwicklungen

2.1 Hohes Meldevolumen – Ursachen

Im letzten Jahrzehnt sind die Verdachtsmeldungen jährlich durchschnittlich um 20–30 % angestiegen. Die Gründe hierfür sind vielfältig. Die Basis bildet der seit 2013 kontinuierliche Ausbau der regulatorischen Anforderungen bei den Sorgfalts- und Meldepflichten. Damit verschärften sich die Finanzmarktaufsicht und das Enforcement massgeblich. Durch die zahlreichen Korruptions- und Geldwäscherei-Skandale, in welche ein Grossteil des Schweizer Bankenplatzes involviert war, ist das Bewusstsein für die Wichtigkeit der effektiven Geldwäschereibekämpfung bei den Finanzintermediären zusätzlich gestiegen. Viele Banken haben die Abteilungen, die sich um Compliance und Financial Crime kümmern, personell verstärkt. Zusätzlich konnten sie das Transaktionsmonitoring dank technologischen Fortschritts stetig verfeinern. Die Umstellung des Meldewesens von Papier auf die IT-Applikation goAML («government office Anti Money Laundering») und die XML[3]-Anbindung per 1. Januar 2020 vereinfachten der Finanzindustrie die Kommunikation von Verdachtsmeldungen. All diese Entwicklungen bewirken einen Anstieg von Verdachtsmeldungen bei der MROS.
Dieser Trend setzte sich 2023 fort – der Anstieg war jedoch erheblich steiler, als dies zu erwarten war. Per Ende des Jahres 2023 verzeichnete MROS gesamthaft 11 876 Meldungen. Im Vergleich zum Vorjahr entspricht dies einem Anstieg um mehr als 4200 Verdachtsmeldungen respektive einer Zunahme von 56 %. Innerhalb von zwei Jahren haben sich die Meldungen verdoppelt; rückblickend auf die letzten zehn Jahre gar verzehnfacht. Dieses eindrückliche Meldevolumen verlangt nach einer Einordnung und einer Prognose für die kommenden Jahre. Die Meldestelle und deren strategische Ausrichtung sind von diesem Anstieg massgeblich betroffen.

Der markante Anstieg des Meldevolumens lässt sich aus Sicht MROS auf nachfolgende Faktoren zurückführen:

– **Verankerung der Definition des begründeten Verdachts im Gesetz:** Per 1. Januar 2023 ist die «SIF-Vorlage»[4] in Kraft getreten. Damit ist der Begriff des «begründeten Verdachts», der bereits seit mehr als zehn Jahren durch die Praxis und die Rechtsprechung gefestigt ist, nun auch im Gesetz verankert (Art. 9 Abs. 1^{quater} GwG). Demnach muss ein Finanzintermediär immer dann eine Verdachtsmeldung absetzen, wenn er einen konkreten Hinweis oder mehrere Anhaltspunkte dazu hat, dass Vermögenswerte kriminellen Ursprungs sein könnten, und er diesen Verdacht trotz zusätzlicher eigener Abklärungen nicht ausräumen kann. Ein Teil der Meldungen dürfte auf diese nun unmiss-

[3] Das hier erwähnte XML-Schema definiert die Struktur der von den Finanzintermediären mittels eines XSD-Format-File an die MROS gelieferten Informationen. Mehr Informationen zu diesem Schema sind auf der Webseite der MROS zu finden. Vgl. *https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung.html*.

[4] *AS 2021 656*, siehe auch Botschaft vom 26. Juni 2019 zur Änderung des Geldwäschereigesetzes, *BBl* **2019** *5451, 5477 ff*.

verständliche Formulierung im Gesetz zurückzuführen sein.

- **Verschärfte Praxis in Bezug auf Artikel 37 GwG:** Die strafrechtliche Sanktionierung bei Verletzung der Meldepflicht wurde verschärft. Eine Auswertung der Urteile des Eidgenössischen Finanzdepartements (EFD) und des Bundesstrafgerichts zeigt, dass mittlerweile vermehrt auch Compliance Officer aus tiefen Hierarchiestufen zur Rechenschaft gezogen werden.[5] Die Verurteilungen wegen fahrlässiger Meldepflichtverletzung haben ebenfalls zugenommen.[6] Gespräche mit Exponentinnen und Exponenten der Finanzindustrie haben verdeutlicht, dass diese verschärfte Praxis in der Branche Wirkung zeigt und folglich auch das Verhalten beeinflusst. Es wird lieber einmal zu viel als zu wenig gemeldet.
- **Prüfgesellschaften und (interne) Revisionsstellen mit strengerem Massstab:** Rückmeldungen von Finanzintermediären weisen darauf hin, dass Prüfgesellschaften aber auch die internen Kontrollinstanzen die Einhaltung der aufsichtsrechtlichen Geldwäschereivorgaben tendenziell strenger beurteilen. Die allgemeine Verschärfung des Aufsichts- und Geldwäschereiabwehrdispositivs sowie der grössere mediale Fokus auf die Prüfthematik dürften hierfür ursächlich sein.
- **Kostendruck auf Finanzintermediäre mit asymmetrischen Geschäftsmodellen:** Der Kostendruck auf die Finanzindustrie ist spürbar. Sachverhalte werden teilweise nur noch sehr rudimentär abgeklärt und die besonderen Abklärungspflichten nach Artikel 6 GwG, welche für eine Verdachtsmeldung an die Meldestelle zwingend sind, werden nicht mehr oder nur noch ungenügend vorgenommen. Dies ist insbesondere bei Finanzinstituten im Nichtvermögensverwaltungsbereich mit aggressivem Onboarding für Auslandkunden zu beobachten. Ein Grossteil dieser ungenügend abgeklärten Verdachtsmeldungen ist für die Meldestelle wertlos. Die Finanzintermediäre kommen mit diesem Verhalten ihrer Aufgabe als «first line of the defense» im Geldwäschereiabwehrdispositiv nicht mehr oder nur noch ungenügend nach. Die MROS ist im Austausch mit der FINMA über die betroffenen Finanzintermediäre und die eingeleiteten Massnahmen.

Es ist davon auszugehen, dass der Trend der stark zunehmenden Meldungen im Jahr 2024 und darüber hinaus anhalten wird. Die Erfahrung zeigt, dass solche Entwicklungen in der Regel irreversibel sind. Hat sich das beschriebene Meldeverhalten einmal etabliert, wird es zum Standard. Die Finanzindustrie wird kaum aus eigenem Antrieb zurückbuchstabieren, zumal die Signale der Straf- und Aufsichtsbehörden, aber auch der Financial Action Task Force on Money Laundering (FATF) eher auf eine Verschärfung hindeuten. Folglich ist in Zukunft mit einem erhöhten Meldeaufkommen zu rechnen. Die Meldestelle ist für eine weitere Zunahme des Meldevolumens – ähnlich wie 2023 geschehen – nur bedingt gerüstet; sie stösst mit ihren personellen und technischen Ressourcen an ihre Grenzen. Durch die Anwendung des «risikobasierten Ansatzes» (vgl. Kap. 2.2) können steigende Zahlen zwar aufgefangen werden, indem die Aufgreifkriterien (sprich, die Kriterien für die Triage) verschärft werden. De facto wäre für den Entscheid der Abklärung einer Verdachtsmeldung nicht mehr das Risiko ausschlaggebend, sondern die Ressourcenlage.

2.2 Ausrichtung der MROS – Weiterentwicklung «Risikobasierter Ansatz»

Die Arbeitsweise der Meldestelle hat sich in den letzten Jahren stark verändert. Bedingt durch den drastischen Anstieg der Verdachtsmeldungen und des Reportingvolumens kann die Meldestelle nicht mehr alle Informationen im selben Detaillierungsgrad analysieren und weiterver-

[5] Zwischen 2014 – 2022 kam es seitens EFD/Bundesstrafgericht zu mindestens 21 rechtskräftigen Verurteilungen. Per Ende 2022 waren 47 Verfahren pendent (Quelle: «Strafrechtliche Verantwortlichkeit des Compliance Officers», Referat von Dr. Doris Hutzler vom 8. Juni 2023 anlässlich der 14. Tagung zum Wirtschaftsstrafrecht, EIZ, Zürich).

[6] Vgl. etwa: *Urteil des Bundesgerichts 6B_1176/2022 vom 5. Dezember 2023*.

arbeiten, wie dies vor fünf oder zehn Jahren möglich war. Die MROS sieht sich gezwungen, Prioritäten und Schwerpunkte zu setzen. Seit der Einführung des Informationssystems goAML per 1. Januar 2020 verfolgt die Meldestelle beim Empfang und bei der Bearbeitung von Verdachtsmeldungen einen «risikobasierten Ansatz»: Die eingehenden Verdachtsmeldungen werden mittels «Triage-Matrix» nach Risiko kategorisiert, priorisiert und dann basierend auf dieser Einteilung mit unterschiedlicher Ausprägung analysiert.
Die Meldestelle fokussiert auf die Bekämpfung von Schwerstkriminalität – die Schwerpunkte liegen auf der Organisierten Kriminalität (OK), der Terrorismusfinanzierung (TF) sowie bestimmten Formen der Wirtschaftskriminalität (WK). Dabei orientiert sich die Meldestelle auch an den Strategien der Strafverfolgungsbehörden, operiert erfolgsorientiert und berücksichtigt potenzielle Reputationsrisiken für den Finanzplatz Schweiz.
Die Strategie der MROS ist auch in den aktuellen Statistiken erkennbar. Während die Anzeigen an die Bundesanwaltschaft im Jahr 2023 zugenommen haben (+43 % gegenüber 2022)[7], sind die Anzeigen an die kantonalen Strafverfolgungsbehörden – mit Ausnahme des Kantons Genf – im Vergleich zu den Vorjahren rückläufig. Zurückzuführen ist dies darauf, dass die Meldestelle häufiger Anzeigen im Bereich der Schwerstkriminalität erstattete. Im Jahr 2023 übermittelte die MROS insgesamt 866 Anzeigen an die Strafverfolgungsbehörden. Zum Vergleich: 2022 waren es 1232 Anzeigen, 2021 1486[8]. Dies entspricht zahlentechnisch zwar einem Rückgang; die Informationen der Anzeigen verdeutlichen jedoch, dass die Anzeigen im Jahr 2023 mehr Verdachtsmeldungen und Antworten der Finanzintermediäre pro Übermittlung enthielten. Im Jahr 2021 waren im Schnitt 1,3 Verdachtsmeldungen Gegenstand einer Anzeige an die Strafverfolgungsbehörden; 2023 waren es 1,8. Zudem wurden im Jahr 2023 in 44 % der Fallkomplexe, die den Strafverfolgungsbehörden übermitteltet wurden, zusätzliche Informationen der Finanzintermediäre verarbeitet (im Jahr 2021: 18 % und 2022: 25 %). Diese Zahlen belegen, dass die heutigen Analysen der Meldestelle tendenziell mehr Informationen enthalten und komplexer sind. Die Meldestelle bewegt sich damit weg vom traditionellen Bearbeitungsansatz «1 Meldung gleich 1 Anzeige an die Strafverfolgungsbehörden» hin zu aktiver «Intelligence» und zur Vernetzung der vorhandenen Informationen. Nicht mehr die Verdachtsmeldung als solches, sondern deren Informationsgehalt steht im Mittelpunkt der Analyse.
Die Meldestelle wird ihre Intelligence-Strategie – Fokus, Triage, Priorisierung, Vernetzung – in den kommenden Jahren konsequent weiterentwickeln. Fakt ist jedoch, dass sich der Anteil der Verdachtsmeldungen, welche vertieft analysiert werden können, aufgrund des kontinuierlichen Anstiegs des Reportingvolumens[9] stetig verringert. Im Jahr 2023 wurde eine von fünf Meldungen tiefgreifend analysiert.[10] Die restlichen 80 % der Verdachtsmeldungen wurden weniger intensiv oder mit gesamtheitlichen Analyseverfahren (z. B. Clusteringmethoden) bearbeitet. Ein Teil der Meldungen wurde bereits beim Empfang aussortiert. Dies bedeutet, dass die Meldung und die darin enthaltene Information nicht mehr weiterverfolgt wird. Sie kann jedoch dank Aufbereitung und Ablage im Informationssystem goAML jederzeit reaktiviert und weiterbearbeitet werden. Im Jahr 2023 wurden über 300 aussortierte (alte) Verdachtsmeldungen reaktiviert. Dies aufgrund einer neuen Information, beispielsweise der Verdachtsmeldung eines Finanzintermediärs oder der Spontaninformation einer ausländischen FIU.
Mit dem Anstieg der Verdachtsmeldungen nimmt das Risiko, dass wesentliche Geldwäschereifälle unentdeckt bleiben, zu. Die Meldestelle ist bestrebt, ihre Bearbeitungskadenz und ihre Effizienz zu steigern. Limitierende Faktoren beim Empfang und der Triage der Verdachtsmeldungen sind, nebst den personellen Ressourcen, die technische Unterstützung (Automatisierung,

---

7 Übermittlungen an die Bundesanwaltschaft: 2022: 79; 2023: 113.

8 Vgl. hierzu Kap. 4.7: Die Statistiken für die Jahre 2021 und 2022 enthalten auch die sog. «COVID-Übermittlungen». Die Statistiken für diese Jahre sind somit erhöht.

9 Verdachtsmeldungen haben im Jahr 2023 um 56 % und das gesamte Reportingvolumen um 63 % zugenommen.

10 Vertiefte Analysen: 2021: 45 %; 2022: 32 %.

intelligente IT-Unterstützung) und die Datenqualität der eingehenden Meldungen und der Informationen der Finanzintermediäre. Letztere wirken sich massgeblich auf die Effizienz der Datenbearbeitung aus. Je schlechter die Datenqualität, desto aufwändiger gestaltet sich der Datenbearbeitungsprozess. Um diese Defizite auszugleichen, bräuchte es eine bessere IT-Unterstützung und/oder mehr personelle Ressourcen. Die Meldestelle hat 2023 im Bereich IT das Projekt «goAML Futuro»[11] weiter vorangetrieben. Angestrebt wird damit Interoperabilität: der automatisierte Abgleich der zugänglichen Justiz- und Polizeidatenbanken. Auch im Bereich der Datenbrüche hat die Meldestelle Verbesserungen erzielt. Die Datenqualität beim Eingang der Meldungen stellt die grösste Herausforderung für die Meldestelle dar – und damit auch das grösste Potenzial, um die Effizienz zu steigern. Die geplante Einführung von Artikel 23 Absatz 7 GwG im Rahmen der laufenden GwG-Revision[12] ist für die MROS von zentraler Bedeutung. fedpol würde dazu ermächtigt, in einer technischen Verordnung vorzugeben, in welcher Form und in welchem Format (Datenstandard) die Daten einzuliefern sind.

2.3 Nationale Risikoanalyse – Sektorieller Bericht zu Kryptowährungen und Virtual Assets

Die Risiken, die durch Geldwäscherei und Terrorismusfinanzierung entstehen, sollten stets Teil der Kriminalitätsbekämpfungsstrategie eines Landes sein. Die Schweiz hat bisher zwei nationale Risikoanalysen (NRA) publiziert (2015[13] und 2021[14]) und die auftretenden Risken umfassend bewertet. Auftraggeberin und verantwortlich für die Erstellung der NRAs und der zugrunde liegenden sektoriellen Risikoanalysen ist die Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT)[15]. Die Meldestelle ist Teil dieser Koordinationsgruppe; als Leiterin der Untergruppe Analyse ist sie für die Erstellung der Risikoberichte zuständig.

Unter der Leitung der Meldestelle wurde am 5. Dezember 2023 der sektorielle Risikobericht «National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets»[16] von der KGGT verabschiedet. Ein erster Bericht zum Thema Krypto-Assets erschien im Jahr 2018.[17] Dieser stufte die Gefährdungen und Verwundbarkeiten für die Schweiz als «erheblich» ein. Der Einfluss und die Bedeutung von Virtual Assets (VAs) haben sich seit 2018 grundlegend geändert. Die Sensibilisierung und das Bewusstsein im Markt sind deutlich gewachsen. Die Meldestelle erhält inzwischen täglich VA-relevante Verdachtsmeldungen – für die Strafverfolgungsbehörden gehören VAs mittlerweile zum Arbeitsalltag. Die MROS konnte vier zentrale Entwicklungen feststellen:

1. In der Schweiz ist die Anzahl Finanzintermediäre mit VASP-Tätigkeit von unter zehn im Jahr 2018 auf über 204 per Ende 2022 deutlich angestiegen. Trotzdem haben mindestens 180 dieser Finanzintermediäre keine Verdachtsmeldung an die MROS ausgelöst.
2. Die Verwendung von VAs hat sich in der Schweiz zwischen 2018 und 2023 vervielfacht. Immer mehr Privatpersonen und Unternehmen verwenden und akzeptieren VAs für Zahlungen im Handel, für Dienstleistungen und für Investitionen. Die Grenzen zwischen dem traditionellen Finanzsektor und dem VA-Bereich werden immer unschärfer; VAs werden

---

[11] Vgl. Ausführungen im *Jahresbericht 2022 der MROS*, S. 13 f.

[12] *Medienmitteilung des Bundesrates vom 30. August 2023*: «Bundesrat eröffnet Vernehmlassung zur Stärkung der Geldwäscherei-Bekämpfung».

[13] *Erste nationale Risikoanalyse (NRA) – Bericht über die nationale Beurteilung der Geldwäscherei und Terrorismusfinanzierungsrisiken in der Schweiz, Juni 2015*.

[14] *Zweite nationale Risikoanalyse (NRA) – Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz, Oktober 2021*.

[15] Die KGGT wird vom Staatssekretariat für Internationale Finanzfragen (SIF) geleitet. *Link* zum Mandat der KGGT.

[16] *National Risk Assessment (NRA), Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets.*

[17] *Sektorieller NRA-Bericht: Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding, Oktober 2018.*

zunehmend in herkömmliche Zahlungsplattformen integriert und die «beiden Welten» verschmelzen.

3. Die kriminelle Verwendung von VAs hat sowohl in der Schweiz als auch global zugenommen. Sie ist zudem deutlich diverser geworden. Strafverfolgungsbehörden sind vermehrt mit Verfahren aus unterschiedlichen Wirtschaftsbereichen konfrontiert, die Bezüge zu VAs aufweisen. So werden immer mehr Strafanzeigen im Zusammenhang mit Diebstahl oder anderweitiger Entwendung (z. B. Betrug, ungetreue Geschäftsbesorgung) von VAs erstattet. Die Schadenssummen, die durch VAs anfallen, sind stark angestiegen und belaufen sich in der Schweiz für das Jahr 2022 mindestens auf einen zweistelligen Millionenbetrag (im Vergleich: 2007 sind es knapp 7 Mio. Franken). Die Verwendung von VAs ist bei gewissen Straftaten (z. B. Investmentbetrug, Ransomware) zum Standard geworden. VAs haben sich zu einem gängigen Werkzeug der Finanzkriminalität entwickelt.
4. Finanzintermediäre in der Schweiz haben in den vergangenen Jahren immer häufiger mutmasslich GW/TF-relevante Vorgänge mittels VAs auf den von ihnen geführten Konten festgestellt. Dies führt zu einem starken Anstieg VA-relevanter Verdachtsmeldungen an die MROS: Im Jahr 2022 wiesen bereits fast 14 % aller Verdachtsmeldungen einen Konnex zu VAs auf. In diesen konnten unter anderem Verbindungen zu politisch exponierten Personen (PEP), internationalen Korruptionsaffären, transnationalen Gruppen im Bereich der organisierten Kriminalität oder staatlichen Akteuren festgestellt werden.

Die Risikoanalyse kommt zum Schluss, dass die GW/TF-Risiken im VA-Bereich gegenüber 2018 angestiegen sind. Gefährdungen und Verwundbarkeiten, welche bereits 2018 identifiziert wurden, haben sich grösstenteils verschärft und erweitert. Aufgrund ihres höheren Stellenwerts und den mit ihnen verbundenen Risiken erfordern VAs die nötige Aufmerksamkeit sämtlicher involvierter Partner (Finanzintermediäre, FIU, Strafverfolgungsbehörden, Aufsichtsbehörden sowie Aufsichts- und Selbstregulierungsorganisationen).

Nebst den identifizierten Gefährdungen und Verwundbarkeiten der Schweiz gegenüber GW/TF im VA-Bereich tragen verschiedene Faktoren zur Minderung dieser Risiken bei:

- Die internationale Zusammenarbeit bei VA-Ermittlungen zeigt, dass verstärktes Tracing, Sperrungen und Einziehungen von VAs Geldwäscherei und Terrorismusfinanzierung effektiv bekämpfen können.
- Viele kleine VA-Anbieter sind mittlerweile verschwunden oder haben fusioniert. Dies hat dazu beigetragen, dass grosse Kryptobörsen ihre Compliance-Massnahmen verstärkt haben, was das Abwehrdispositiv weltweit stärkt.
- Blockchains sind naturgemäss transparenter als traditionelle Zahlungssysteme. Dies führt zu einer besseren Nachverfolgbarkeit von VAs; Blockchain-Analysetools können verdächtige Aktivitäten leichter identifizieren und verfolgen.
- Schliesslich trägt in der Schweiz die Ausweitung der Definition von Finanzintermediation im VA-Bereich dazu bei, eine breitere Palette von Akteuren in den Anwendungsbereich des Geldwäschereigesetzes zu bringen. Dies schliesst Lücken in den Massnahmen zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung.

Die KGGT schlägt basierend auf den Aussagen des Berichts vier Massnahmen vor, um das aktuelle GW/TF-Abwehrdispositiv im VA-Bereich zu stärken:

1. **Verbesserung des Daten- und Kenntnisstands zum VA-Sektor in der Schweiz**
   Informationen zum VA-Sektor und zur kriminellen Verwendung von VAs in der Schweiz sind unerlässlich, um GW/TF-Risiken angemessen zu identifizieren, zu verstehen und zu bewerten.
2. **Förderung eines proaktiven Meldeverhaltens von Finanzintermediären mit VASP-Tätigkeit**
   Finanzintermediäre mit VASP-Tätigkeit sollten künftig ihre GW/TF-Abklärungen verstärken, um besser in der Lage zu sein, verdächtige

Vorgänge zu entdecken und diese der MROS zu melden.

3. **Bereitstellung von ausreichenden Kapazitäten und Ressourcen für die GW/TF-Bekämpfung im VA-Bereich**
   Die Zusammenarbeit zwischen sämtlichen zuständigen Stakeholdern muss verstärkt werden, um den Herausforderungen der GW/TF-Bekämpfung im VA-Bereich gerecht zu werden.
4. **Stärkung der internationalen Zusammenarbeit**
   Die Schweiz soll sich auf internationaler Ebene weiterhin für eine wirksame Bekämpfung der Kriminalitätsrisiken im Finanzsektor einsetzen und die Umsetzung der Empfehlung der FATF vorantreiben.

Der Risikobericht betont abschliessend die Notwendigkeit, dass die Schweiz die Risiken von VAs ernst nimmt und angemessene Massnahmen ergreift, um Geldwäscherei und Terrorismusfinanzierung wirksam zu bekämpfen. Die Bedeutung von VAs im Finanzsektor nimmt stetig zu; die Schweiz muss sich den Herausforderungen stellen, um mit den rasanten Entwicklungen Schritt halten zu können.
Der sektorielle Bericht «National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets» wurde im ersten Quartal 2024 publiziert.[18] Derzeit sind weitere sektorielle Risikoanalysen unter der Federführung der Meldestelle in Planung: «Proliferationsfinanzierung» (Erscheinungsdatum voraussichtlich Q3/2024), «Juristische Personen» (Erscheinungsdatum voraussichtlich Q4/2024) und «Immobilienmarkt» (Erscheinungsdatum voraussichtlich im Verlaufe 2025).

2.4 Public-Private-Partnership (PPP)

Am 17. November 2021 beauftragte der Bundesrat fedpol / MROS in Zusammenarbeit mit weiteren Behörden, die Möglichkeiten der Einführung einer «Public-Private-Partnership» (PPP) für den Austausch von Finanzinformationen zu prüfen. Ziel ist, die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung in der Schweiz weiter zu stärken. Die Meldestelle hat sich im Jahr 2022 mit dem Staatssekretariat für internationale Finanzfragen (SIF), dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA), der Eidgenössischen Finanzmarktaufsicht (FINMA) sowie einer Expertenrunde bestehend aus Vertreterinnen und Vertretern der Finanzbranche über die Zweckmässigkeit und die Rahmenbedingungen einer PPP vertieft ausgetauscht. Die Behörden und Expertinnen und Experten kommen zum Schluss, dass eine PPP einen massgeblichen Beitrag zur Kriminalitätsbekämpfung – insbesondere zur Stärkung der Prävention – leisten kann. Die Meldestelle hat über die wichtigsten Ergebnisse des Behörden-Experten-Austauschs einen Bericht[19] erstellt und diesen dem Bundesrat im April 2023 zur Kenntnisnahme unterbreitet. Dafür wurde eine Arbeitsgruppe bestehend aus der Meldestelle, dem SIF sowie Vertreterinnen und Vertretern aus verschiedenen Bereichen der Finanzindustrie eingesetzt. Die Arbeiten für die Errichtung einer «Swiss PPP» laufen derzeit noch. Bis spätestens Ende 2024 sollen sämtliche noch offenen Fragen geklärt sein und ein tragfähiger Austausch zwischen dem öffentlichen und dem privaten Sektor, basierend auf zu konstituierenden Regeln, stattgefunden haben.
Die Meldestelle ist heute bereits in eine PPP eingebunden. Sie ist Mitglied des Europol Financial Intelligence Public Private Partnership (EFIPPP).[20] Das EFIPPP wurde 2017 vom European Financial and Economic Crime Center (EFECC), welches Teil von Europol ist, ins Leben gerufen. Ziel ist es, die grenzüberschreitende Zusammenarbeit und den Informationsaustausch zwischen Europol, den Strafverfolgungsbehörden, den FIUs, den Aufsichtsorganisationen sowie den regulierten Finanzdienstleistern zu fördern. Beim EFIPPP handelt es sich um die erste länderübergreifen-

[18] *National Risk Assessment (NRA), Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets*.

[19] *Bericht der Meldestelle: Public Private Partnership (PPP) zum Informationsaustausch für die Bekämpfung von Terrorismusfinanzierung und Geldwäscherei, März 2023.*

[20] *EFIPPP Homepage – EFIPPP.*

de Informationsaustauschplattform. Bei seiner Gründung 2017 bestand das EFIPPP aus 28 öffentlichen und privaten Institutionen aus acht EU- und Nicht-EU-Mitgliedstaaten. Per Anfang 2022 sind 79 Institutionen aus 18 EU- und Nicht-EU-Mitgliedstaaten Teil des EFIPPP.

Die Ziele des EFIPPP:
- der Aufbau eines gemeinsamen Informationsstandes und -verständnisses;
- das gemeinsame Erarbeiten von Risikoindikatoren und Bedrohungstypologien;
- die Erleichterung des Austausches von operativen und/oder taktischen Erkenntnissen im Zusammenhang mit laufenden Ermittlungen (in Übereinstimmung mit den geltenden nationalen und internationalen rechtlichen Bestimmungen);
- die Identifizierung von Gateways für den Informationsaustausch und von rechtlichen Hürden beim Informationsaustausch (im Einklang mit den geltenden nationalen und EU-Rechtsrahmen);
- die Förderung des Einsatzes neuer Instrumente zur Bekämpfung der Finanzkriminalität, der Nutzung neuer Technologien und des Austauschs gemeinsamer Erfahrungen und Methoden für Innovationen und Schulungen;
- die Unterstützung inländischer Kooperationsforen in den relevanten Rechtsordnungen mit dem Ziel, als effektive Drehscheibe zwischen den verschiedenen Plattformen zu fungieren und den öffentlich-privaten partnerschaftlichen Austausch von Informationen und Erkenntnissen zu erleichtern.

Die Struktur des EFIPPP basiert auf vier Säulen:
- **«The Strategic Oversight Body»:** Das strategische Aufsichtsgremium verantwortet die strategische Beratung und die Koordination in Angelegenheiten, die mit der Entwicklung und den Schwerpunktbereichen des EFIPPP zusammenhängen. Das Gremium trifft sich jährlich.
- **«The Steering Group»:** Die Steuerungsgruppe leitet die operativen Aktivitäten des EFIPPP und fungiert als Entscheidungsgremium. Die Gruppe legt Prioritäten für jedes Kalenderjahr fest, genehmigt die Aufnahme neuer Mitglieder und regelt die Aktivitäten der Arbeitsgruppen.
- **«The Working Groups»:** Verschiedene Arbeitsgruppen setzen die Ziele des EFIPPP um und entwickeln die einzelnen EFIPPP-Produkte und Papiere. Derzeit bestehen sieben Working Groups. Sie sind das operative Herz des EFIPPP.
- **«The Threat and Typologies Group»:** Diese Gruppe beschäftigt sich vorwiegend mit dem Aufbau von Wissen über bestimmte Bedrohungen.

Die Meldestelle profitiert massgeblich von den Informationen, welche innerhalb des EFIPPP ausgetauscht werden. Der «Alert» der Meldestelle an die Schweizer Finanzbranche betreffend Terrorismusfinanzierung vom 3. November 2023 sowie das «Addendum» vom 5. Dezember 2023 basieren zu einem grossen Teil auf Informationen und Analysen aus dem EFIPPP. Ein gut funktionierender internationaler Informationsaustausch ist heute der Schlüsselfaktor für eine effiziente und glaubwürdige Geldwäschereibekämpfung. Die Meldestelle engagiert sich aktiv im EFIPPP und ist seit Dezember 2023 Mitglied der Steering Group.

2.5 Gesetzesvorlage Transparenzregister und Revision des Geldwäschereigesetzes

2.5.1 Grundzüge der Vorlage

Der Bundesrat beauftragte das EFD an seiner Sitzung vom 12. Oktober 2022 mit der Erarbeitung einer Gesetzesvorlage zur erhöhten Transparenz und erleichterten Identifikation der wirtschaftlich Berechtigten von juristischen Personen. Der Gesetzesentwurf zielt darauf ab, die Integrität des Finanz- und Wirtschaftsplatzes Schweiz zu stärken. Er sieht die Einführung eines eidgenössischen Registers der wirtschaftlich Berechtigten (Transparenzregister) sowie weitere Massnahmen vor, die notwendig sind, um die Wirksamkeit des Dispositivs zur Bekämpfung der Geldwäscherei und der Wirtschaftskriminalität zu erhöhen. Die vorgeschlagenen Massnahmen ermöglichen es, auf die Entwicklung der internationalen Standards (FATF und Global Forum) zu reagie-

ren und die Konformität der Schweiz mit diesen Standards zu gewährleisten. Die Gesetzesvorlage beinhaltet folgende Punkte:

- Die Errichtung eines eidgenössischen **Transparenzregisters** über die wirtschaftlich berechtigten Personen von Rechtseinheiten. Es handelt sich dabei um ein nicht öffentlich einsehbares Register, welches vom Eidgenössischen Justiz- und Polizeidepartement (EJPD) geführt wird. Die Kontrollstelle, angesiedelt beim EFD, gewährleistet die qualitative Überprüfung des Registers und verfügt über entsprechende Sanktionsinstrumente.
- Die Einführung von **Sorgfaltspflichten** nach dem Geldwäschereigesetz für besonders **risikobehaftete Beratungstätigkeiten** (Unterstellung von Beraterinnen und Beratern sowie Anwältinnen und Anwälten).
- Zusätzliche **Massnahmen** für den Immobilien-, den Edelmetall- und Edelsteinhandel. Schliesslich findet eine Klärung der Pflichten der Finanzintermediäre bei der Überwachung der Umsetzung von Zwangsmassnahmen nach dem Embargogesetz[21] statt.

2.5.2 Auswirkungen auf die MROS

Der Gesetzesentwurf sieht vor, dass die Finanzintermediäre dem Register melden, wenn sie Diskrepanzen zwischen den ihnen vorliegenden und den im Register vorhandenen Informationen feststellen und diese Unterschiede zu Zweifeln an der Richtigkeit, Vollständigkeit oder Aktualität der Informationen über die wirtschaftlich berechtigte Person einer Rechtseinheit aufkommen lassen (Discrepancy Reporting; DR). Der Meldestelle obliegt wiederum eine Meldepflicht gegenüber dem Transparenzregister, sofern sie aufgrund ihrer Analysen Zweifel an den Registerinformationen zum wirtschaftlich Berechtigten hat.[22] Der Austausch der Informationen zwischen den Registerbehörden und der Meldestelle erfolgt über die angepassten Amtshilfebestimmungen im GwG.[23]

Durch die Unterstellung risikobehafteter Beratungstätigkeiten unter das GwG entsteht für die Meldestelle eine neue Meldepopulation; insbesondere – aber nicht nur – im Zusammenhang mit der Gründung und Strukturierung von juristischen Personen, was zu einem weiteren Anstieg des Meldevolumens führen wird. Die weiteren Anpassungen im GwG (u. a. im Immobilien-, Edelmetall- und Edelsteinhandel) schliessen wichtige Lücken und tragen zu einer weiteren Stärkung des Abwehrdispositives der Schweiz bei.

Die Meldestelle unterstützt und begrüsst die Gesetzesvorlage zum Transparenzregister und der Revision des GwG; nicht zuletzt, weil die erfolgreiche Umsetzung der Gesetzesvorlage auch entscheidend für die FATF-Länderprüfung sein wird. Ein gutes Prüfergebnis in den FATF-Evaluationsrunden ist für die Schweiz als internationaler Wirtschaftsstandort und Finanzplatz von grosser strategischer Bedeutung.

2.6 Internationale Entwicklungen

2.6.1 Sanktionen gegen Russland

Sanktionen im Kontext der militärischen Aggression Russlands gegen die Ukraine und des Entscheids des Bundesrates vom 28. Februar 2022, wonach die Schweiz die Sanktionen der Europäischen Union (EU) gegen Russland übernahm[24], beschäftigten die Meldestelle auch im Jahr 2023. Im letzten Jahresbericht stellte die MROS klar, dass zwischen den verschiedenen Meldesystemen und Zuständigkeiten (Sanktionen: Staatssekretariat für Wirtschaft [SECO]; Geldwäscherei: MROS) differenziert werden muss.

Die Überwachung des Vollzugs der Meldepflicht und der Einhaltung des Sanktionsregimes obliegen dem SECO. Eine Meldung an das SECO

---

[21] Bundesgesetz über die Durchsetzung von internationalen Sanktionen (Embargogesetz, EmbG), SR **946.231**.

[22] Entwurf Bundesgesetz über die Transparenz juristischer Personen und die Identifikation der wirtschaftlich berechtigten Personen [Gesetz über die Transparenz juristischer Personen; TJPG]).

[23] nArt. 29 Abs. 1 GwG.

[24] *Verordnung (EU) Nr. 833/2014* des Rates vom 31. Juli 2014 über restriktive Massnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren.

muss nicht zwingend auch eine Meldung an die Meldestelle nach sich ziehen. Sie entbindet einen Finanzintermediär jedoch nicht von den im GwG statuierten Sorgfalts- und Meldepflichten. Liegen bei Abklärungen im Zusammenhang mit der Verletzung oder der Umgehung von Sanktionen auch Anhaltspunkte für Geldwäscherei vor, so hat der Finanzintermediär zusätzliche Abklärungen vorzunehmen (Art. 6 GwG). Je nach Ausgang dieser Abklärungen resultiert daraus eine Meldung an die MROS.[25]
Voraussetzung für eine Meldung ist immer, dass die in eine Geschäftsbeziehung involvierten Vermögenswerte mutmasslich im Zusammenhang mit der Unterstützung einer kriminellen oder terroristischen Organisation oder mit Geldwäscherei stehen, aus einem Verbrechen oder aus einem qualifizierten Steuervergehen herrühren, der Verfügungsmacht einer kriminellen oder terroristischen Organisation unterliegen oder aber der Terrorismusfinanzierung dienen. Gemäss Artikel 10 Absatz 2 StGB gelten als Verbrechen all jene Taten, für die eine Freiheitsstrafe von mehr als drei Jahren angedroht ist. Eine Verletzung oder die Umgehung von Sanktionen qualifiziert nur in schweren Fällen als Verbrechen – eine einfache Sanktionsverletzung stellt demnach keine Vortat im Sinne der Geldwäschereigesetzgebung dar.[26]
Ähnlich wie im Jahr 2022 stellte die MROS bezüglich der erlassenen Sanktionen im Berichtsjahr kein signifikant verändertes Meldeverhalten fest. Es gab zwar Meldungen mit Bezug zu Sanktionsverletzungen und -umgehungen, bei diesen war aber grösstenteils auch ein Konnex zu mutmasslich Geldwäscherei, organisierter Kriminalität oder Terrorismusfinanzierung gegeben. Aus Sicht der MROS bestätigt sich weiterhin der Eindruck, dass die Finanzintermediäre zwischen den verschiedenen Meldesystemen und den unterschiedlichen Zuständigkeiten sehr gut unterscheiden können und ihre Verdachtsmeldungen differenziert absetzen.

Auch im internationalen Austausch mit Partnerbehörden hat die Meldestelle im Jahr 2023 im Zusammenhang mit den Sanktionsmassnahmen wieder regelmässig Informationsanfragen beantwortet und Spontaninformationen übermittelt. Soweit die gesetzlichen Voraussetzungen erfüllt waren, wurden eingehende Amtshilfeersuchen ausländischer FIUs beantwortet und/oder der zuständigen inländischen Behörde amtshilfeweise zur Kenntnis gebracht.
Anfang 2022 trat die MROS der Russia-Related Illicit Finance and Sanctions FIU Working Group (RRIFS) bei. Es handelt sich hierbei um eine FIU-Taskforce, in welcher neben der Schweiz auch weitere FIUs vertreten sind.[27] Der Informationsaustausch erfolgt basierend auf den Bestimmungen des GwG und den Egmont-Prinzipien. Der internationale Informationsaustausch ist Kernaufgabe der MROS und eine Notwendigkeit.

2.6.2 Terroristische Angriffe der Hamas auf Israel

Neben der militärischen Aggression Russlands gegen die Ukraine beschäftigte ein weiteres, internationales Thema die MROS: die Terrorangriffe der Hamas auf Israel. Die MROS ist in diesem Zusammenhang der Counter Terrorist Financing Taskforce Israel (CTFTI)[28] beigetreten. Die rechtliche Grundlage für die Teilnahme entspricht derjenigen der RRIFS Working Group. Anders als bei der militärischen Aggression Russlands gegenüber der Ukraine hat die Schweiz keine Sanktionen gegen die Hamas verhängt. Der Bundesrat hat am 11. Oktober 2023 beschlossen, die Hamas in der Schweiz zu verbieten. Er hat am 22. November 2023 dem EJPD und dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) den Auftrag erteilt, bis Ende Februar 2024 die Vernehmlassungsvorlage zu einem Spezialgesetz zu erarbeiten (sog. Hamas-Gesetz). Am 21. Februar 2024 beschloss der Bundesrat die Eröffnung des Vernehmlassungsverfahrens, wel-

[25] Melderecht (Art. 305ter Abs. 2 des Schweizerischen Strafgesetzbuchs [StGB], SR **311.0**) oder Meldepflicht (Art. 9 GwG).

[26] Art. 9 Abs. 1 und 2 EmbG.

[27] *RRIFS Task Force*.

[28] *CTFTI Task Force*.

ches bis zum 28. Mai 2024 dauert. Das Inkrafttreten wird jedoch noch einige Zeit in Anspruch nehmen.[29]
Ein Finanzintermediär unterliegt bereits heute einer Meldepflicht, wenn er den begründeten Verdacht hat, dass Finanzflüsse im Zusammenhang mit einer terroristischen Organisation stehen oder zu deren Finanzierung oder Unterstützung dienen.[30] Abklärungen hierzu sind in der Praxis allerdings mit grossen Schwierigkeiten verbunden. Solange die Hamas nicht klar als terroristische Organisation qualifiziert oder verboten wurde, begründet eine Zahlung an die Hamas zum Beispiel für sich alleine noch keine Verdachtsmeldung nach dem Geldwäschereigesetz im Zusammenhang mit der Unterstützung einer terroristischen Organisation nach Artikel 260ter StGB, da zusätzlich noch der Verdacht bestehen muss, dass die Gelder für Terrorismus verwendet werden oder im Zusammenhang mit einem Verbrechen oder einem qualifizierten Steuervergehen stehen. Mit der Qualifikation der Hamas als terroristische Organisation und einem entsprechenden Verbot im Hamas-Gesetz würde hier Klarheit geschaffen, so dass die blosse Transaktion ausreichen würde, um einen genügenden Verdacht auf eine geldwäschereirechtliche Vortat auszulösen.

2.7 Durchführung des «Top-30-Projekts» im Bereich Internationales

Die internationale Zusammenarbeit ist ein Eckpfeiler der Tätigkeit der Meldestelle. Geldwäscherei ist ein globales Phänomen, das sich nicht an nationale Grenzen hält. Etliche von der Meldestelle analysierte Informationen beinhalten Hinweise von internationalen Partnerstellen (ausländische FIUs). Umgekehrt ersuchen Letztere verstärkt um Informationen der MROS respektive via den FIU-Kanal um Finanzinformationen, welche die MROS bei den Finanzintermediären in der Schweiz erhältlich machen kann. Der Austausch hat sich in den vergangenen Jahren intensiviert. Die Amtshilfeersuchen und -anfragen an und von ausländischen Partnerbehörden nehmen nicht nur quantitativ zu, sondern sind auch inhaltlich umfangreicher. Einer der Hauptgründe für diese Entwicklung ist die im Jahr 2021 eingeführte erweiterte Kompetenz der MROS, aufgrund der Analyse von Informationen ausländischer FIUs, weitere Informationen bei den Finanzintermediären einzuholen (Art. 11*a* Abs. 2bis GwG). Ausländische FIUs haben erkannt, dass sie seit der Gesetzesanpassung in der Schweiz Informationen bei den Schweizer Finanzintermediären via MROS erhalten können. Der Austausch über die nationalen Grenzen hinweg untersteht strengen Anforderungen, wird aber rege genutzt.
Um die internationale Zusammenarbeit zu verbessern, Abläufe zu vereinfachen und die Effizienz des Informationsaustauschs zu steigern, ist es wichtig, die Bedürfnisse und Besonderheiten der Partnerstellen zu kennen. Aus diesem Grund hat die MROS im Jahr 2023 das «Top-30-Projekt» lanciert. Die Durchführung dieses Projektes entsprach einer Empfehlung der Eidgenössischen Finanzkontrolle (EFK) vom 20. Dezember 2021.[31] Ziel des Projekts war, die eingehenden Informationen und ausgehenden Antworten der MROS an die ausländischen FIUs zu analysieren und Muster, Auffälligkeiten und Schwachstellen in der Zusammenarbeit zu identifizieren. Ausgewertet wurden Daten im Zeitraum von 1. Juli 2021 (Inkrafttreten von Art. 11*a* Abs. 2bis GwG) bis 30. Juni 2022.
Wenig überraschend stellte sich heraus, dass acht der zehn FIUs, welche die meisten Anfragen an die MROS richteten, europäische FIUs waren. Zusätzlich fanden sich insbesondere jene FIUs unter den Top 30, welche selbst über grössere Finanzplätze verfügen oder sonstige enge (wirtschaftliche) Verbindungen zum Finanzplatz Schweiz aufweisen. Auch namhafte Jurisdiktionen, welche für die Errichtung von Domizilgesellschaften attraktiv sind, befanden sich unter den Top 30. Dasselbe galt für die eingegangenen

[29] Medienmitteilung des Bundesrates vom 24. Februar 2024: «*Der Bundesrat schickt den Gesetzesentwurf für ein Hamasverbot in die Vernehmlassung*».

[30] Art. 9 GwG i. V. m. Art. 260ter StGB.

[31] *Bericht der EFK zur Prüfung der Aufgabenerfüllung der Meldestelle für Geldwäscherei vom 20. Dezember 2021*.

Spontaninformationen aus dem Ausland und Anfragen der MROS an das Ausland.
Beurteilt wurde die Zusammenarbeit sowohl aus qualitativer als auch quantitativer Sicht. Zudem wurden die ausländischen FIUs zur Zufriedenheit mit dem Inhalt und der Dauer der Beantwortung durch die MROS befragt. Das Ergebnis war positiv – bei den von der MROS an ausländische FIUs gestellten Ersuchen wie auch bei den ausgehenden Antworten der Meldestelle.
Die Antworten der ausländischen FIUs wurden betreffend Frist und Informationsgehalt geprüft. Hierbei ist anzumerken, dass der Informationsaustausch immer von den gesetzlichen Rahmenbedingungen des jeweiligen Landes abhängt. So kann es sein, dass gewisse Informationen nur für kurze Zeit zur Verfügung stehen (kurze Aufbewahrungsdauer) oder dass der Austausch gewisser Informationen eines richterlichen Beschlusses bedarf. Der bilaterale und persönliche Austausch zwischen der MROS und den Partnerbehörden trägt wesentlich zur Qualität der Anfragen und Antworten (auf beiden Seiten) bei. Das gegenseitige Verständnis in Bezug auf die rechtlichen und tatsächlichen Möglichkeiten und Hindernisse werden damit weiter gestärkt.
Die Bearbeitungsdauer der Anfragen wurde vielfach diskutiert, da sie aufgrund unterschiedlicher Ursachen stark variieren kann. Die Informationen müssen – sofern sie nicht bereits wegen einer Verdachtsmeldung im Informationssystem vorhanden sind – bei den Finanzintermediären eingeholt und anschliessend aufbereitet werden. In der Regel dauert es einige Zeit, bis die Anfrage überhaupt anhand genommen werden kann. Eine schnelle Bearbeitung ist herausfordernd; einerseits wegen der stetig steigenden Zahlen, andererseits wegen der vielen notwendigen, manuellen Schritte. Einer Effizienzsteigerung dank moderner IT-Infrastruktur kommt auch für den internationalen Austausch ein hoher Stellenwert zu. Im internationalen Vergleich ist klar ersichtlich, dass FIUs oder Länder, die technisch auf hohem Niveau stehen (z. B. im Zusammenhang mit Datenbankabfragen, zugänglichen Registern), schneller antworten. Die Bearbeitungsdauer spielt im Bereich der Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung eine wesentliche Rolle und ist daher für die MROS zentral, um keine Abstriche bei der Qualität vornehmen zu müssen.
Die Einführung von Artikel 11*a* Absatz 2bis GwG führte zu einer klaren grösseren Zufriedenheit der FIUs mit den Antworten der MROS. Seit der Einführung des Artikels am 1. Juli 2021 kann die MROS auf Finanzintermediäre zugehen und die Herausgabe der ersuchten Informationen verlangen, selbst wenn keine Verdachtsmeldung hierzu im Informationssystem vorhanden ist, was bis dahin nicht zulässig war.

2.8 «MROS Crypto Symposium»

Die MROS erhält immer mehr Verdachtsmeldungen, die einen Konnex zu Kryptowährungen aufweisen. Die Anzahl der Finanzintermediäre, welche als VASP tätig sind, hat sich in den letzten Jahren vervielfacht.[32] Um die damit verbundenen Herausforderungen aufzuzeigen und zu besprechen, führte die Meldestelle am 30. Oktober 2023 erstmals eine Krypto-Konferenz mit rund 160 Teilnehmenden (überwiegend Vertreterinnen und Vertreter von VASPs sowie der Selbstregulierungsorganisationen [SROs]) in Zug durch. Die Referierenden (Vertreterinnen und Vertreter von nationalen und internationalen Behörden sowie des Privatsektors) beleuchteten regulatorische und aufsichtsrechtliche Themen sowie Risiken im Umgang mit Kryptowährungen. Sie referierten über die verschiedenen Herausforderungen bei der Nachverfolgung von inkriminierten Kryptowährungen, die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung sowie die Aufdeckung von Straftaten in Zusammenhang mit Kryptowährungen, über die verschiedenen Herausforderungen bei der Nachverfolgung von inkriminierten Kryptowährungen, die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung sowie die Aufdeckung von Straftaten in Zusammenhang mit Kryptowährungen.
Das Staatssekretariat für internationale Finanzfragen (SIF) richtete seinen Fokus auf die Rahmenbedingungen der Regulierung auf nationaler und internationaler Ebene sowie die

[32] Vgl. Kap. 2.3.

rechtliche Einordnung von Kryptowährungen in der Schweiz. Die FINMA verdeutlichte die rechtlichen Herausforderungen in der Aufsicht und den Enforcementverfahren. Die Meldestelle betonte die Wichtigkeit der Erkennung der Risiken und damit die Notwendigkeit der Nationalen Risikoanalysen (NRA). Die FIU von Luxemburg hob die Notwendigkeit der nationalen und internationalen Zusammenarbeit bei der Bekämpfung von Geldwäscherei anhand praktischer Beispiele bei der Terrorismusfinanzierung hervor. Die Staatsanwaltschaft Zürich legte ihren Fokus auf die Strafverfolgung von organisierter Kriminalität und Kryptowährungen. Dieses Bild vervollständigte die Guardia di Finanza aus Italien. Sie präsentierte neue Ermittlungsansätze und -methoden im Zusammenhang mit Kryptowährungen, inklusive Metaverse. Den Abschluss bildete der Vortrag einer Wirtschaftskanzlei, welche mittels Beispielen aus der Praxis den Bogen zwischen Privatsektor und Behörden schlug und auf die Komplexität der Materie aus Berateroptik hinwies.

Abbildung 1: Einladung Crypto Symposium MROS

3. Informationssystem goAML

Das per 1. Januar 2020 eingeführte Informationssystem goAML zur elektronischen Entgegennahme und Bearbeitung von Verdachtsmeldungen ist ein zentrales Element der MROS-Strategie zur Digitalisierung und Effizienzsteigerung. Das System hat sich, vier Jahre nach seiner Einführung, bei den Finanzintermediären vollends etabliert. Es läuft stabil und hat eine hohe Verfügbarkeit. Über 96 % aller Verdachtsmeldungen und Antworten auf Anfragen gemäss Artikel 11*a* GwG gelangen via goAML an die MROS. Diese Entwicklung ist erfreulich. Praktisch die gesamte Kommunikation mit den Finanzintermediären erfolgt über goAML. Die Daten werden jeweils strukturiert übermittelt. Derzeit werden einzig die Abbruchsmitteilungen[33] nach Artikel 9*b* GwG in erhöhter Anzahl unstrukturiert über das Message Board von goAML eingereicht. Es handelt sich aber um eine Übergangslösung – mit der Einführung der goAML-Version 5.2 wird die unstrukturierte Übermittlung nicht mehr möglich sein: Die Finanzintermediäre werden künftig alle Übermittlungen per XML-File oder per Web-Interface vornehmen müssen.

Bei der Qualität der Datensätze, welche die Finanzintermediäre einreichen, bestehen nach wie vor Defizite. Die Rückweisungsquote ist im Jahr 2023 zwar auf 10 % gesunken.[34] Jede zehnte Übermittlung wird aber immer noch mangels Einhaltung der Übermittlungsvorgaben an die Finanzintermediäre zurückgewiesen.

[33] Der Finanzintermediär ist nach 40 Arbeitstagen seit Eingang der Verdachtsmeldung zum Abbruch der Geschäftsbeziehung berechtigt, sofern die Meldestelle innerhalb dieser Zeit keine Anzeige an eine Strafverfolgungsbehörde erstattet. Die Meldestelle ist über den Abbruch wiederum zu informieren (vgl. Art. 9*b* Abs. 3 GwG).

[34] Vorjahre: 2022: 14 %; 2021: 24 %; 2020: 41 %.

Tabelle 1: Informationseingänge bei MROS 2023

Informationseingänge 2023 (Stichtag: 31.12.2023)	Gesamt (Anzahl)	Unstrukturiert: per Post oder via Secure E-Mail[35]	%-Anteil pro Kategorie	%-Anteil Gesamt
Sämtliche nationalen und internationalen Reportings *	21375	5857		
Sämtliche nationalen Reportings	19944	4426	–	22,2 %
Absender: Finanzintermediäre	16436	1502	9,1 %	7,5 %
• Verdachtsmeldungen[36]	11876	158	1,3 %	
• Antworten der FI gestützt auf eine Anfrage gemäss Art. 11*a* GwG[37]	1891	70	3,7 %	
• Abbruchsmitteilungen[38]	2669	1274	47,7 %	
Absender: Nationale Behörden	3508	2924	83,4 %	14,7 %
• Strafverfolgungsbehörden	2643	2643	100 %	
(davon per Post)		(1799)	68 %	
(davon per Secure E-Mail)		(844)	32 %	
• Andere Behörden	865	281	32,5 %	

** Die Zahlen umfassen auch die eingehenden internationalen Anfragen sowie Spontaninformationen der ausländischen FIUs.*

Während Finanzintermediäre in nur 9 % der Übermittlungen unstrukturierte Daten einreichen, liegt der Anteil bei den nationalen Behörden bei über 80 %. Diese werden entweder postalisch oder via Message Board der Meldestelle übersendet, wobei die postalische Zustellung der nationalen Behörden bei 68 % liegt. Die manuelle Erfassungsarbeit liegt in diesen Fällen bei der Meldestelle, was nach wie vor personelle Ressourcen beansprucht. Die MROS steht mit den Strafverfolgungsbehörden im Dialog und wird auch 2024 die nötigen Gespräche führen, um den Anteil unstrukturierter Daten mittelfristig zu senken.

Im Sommer 2023 führte die Meldestelle die goAML-Version 5.2 ein (von 4.9), vorerst nur intern zu Test- und Einführungszwecken. Für Finanzintermediäre wird diese Änderung im Jahr 2024 IT-Anpassungen zur Folge haben. Die betroffenen Finanzintermediäre wurden im Dezember 2023 über die Änderungen informiert. Um einen reibungslosen Übergang zu garantieren, kommunizierte die Meldestelle die technischen Vorgaben und richtete eine Testumgebung ein. Bis Ende 2024 sollen alle Finanzintermediäre die Umstellung vom alten XSD-Schema auf das neue vollzogen haben. Während dieser Übergangsphase akzeptiert die MROS weiterhin alte XML-Dateien. Die neue Version von goAML wird die Analysefähigkeit der Meldestelle stärken. Bei der Programmierung der Version 5.2 berücksichtigte UNODC[39] viele Anliegen und Ansprüche der Meldestelle. Die Datenbearbeitung wird dank dieser neuen Version sowohl für die Finanzintermediäre als auch für die Finanzanalysten der Meldestelle vereinfacht.

---

[35] Das goAML-System verfügt über eine Secure-E-Mail-Funktion (goAML Message Board), in welcher eine E2EE-Kommunikation (End-to-End Encryption) zwischen in goAML registrierten Parteien und der MROS sichergestellt ist.

[36] Verdachtsmeldungen gestützt auf Meldepflicht (Art. 9 GwG) und Melderecht (Art. 305ter Abs. 2 StGB).

[37] Darunter subsumieren sämtliche Anfragen gemäss Art. 11*a* GwG (Abs. 1, Abs. 2 und Abs. 2bis).

[38] Abbruchsmitteilungen gemäss Art. 9*b* GwG (Abbruch der Geschäftsbeziehung).

[39] Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (United Nations Office on Drugs and Crime, UNODC).

4. Jahresstatistik Meldestelle

Die MROS erstellt anonymisierte Statistiken, um Informationen über Geldwäscherei, deren Vortaten, organisierte Kriminalität und Terrorismusfinanzierung während des Geschäftsjahrs[40] auszuwerten. Diese umfassen insbesondere die eingegangen Verdachtsmeldungen der Finanzintermediäre, Auskunftsbegehren von entsprechenden ausländischen Behörden sowie die Verfahren, die auf die Meldungen folgen (vgl. Art. 23 Abs. 1 MGwV[41]).

4.1 Gesamtübersicht 2023

- *Das Volumen der eingereichten **Verdachtsmeldungen** hat 2023 weiter deutlich zugenommen: Im Jahr 2023 hat die MROS **11 876** Verdachtsmeldungen erhalten, was rund 47 Meldungen pro Werktag entspricht. Im Vergleich zu 2022 (7639) bedeutet dies eine Zunahme um 55,5 %. Seit der Einführung des Informationssystems goAML im Januar 2020 hat sich die Anzahl sogar mehr als verdoppelt (vgl. Abbildung 2).*
- ***90,5 %** der Verdachtsmeldungen stammt von Finanzintermediären aus dem **Bankensektor** (Durchschnitt 2014–2023: 89,4 %).*
- *Die Meldestelle übermittelte im Jahr 2023 **866 Anzeigen an die Strafverfolgungsbehörden**. Im Vergleich zum Vorjahr bedeutet dies einen Rückgang von 29,7 % (1232); die Anzeigen waren jedoch umfangreicher (vgl. Kap. 4.7). Zugenommen hat die durchschnittliche Anzahl der Verdachtsmeldungen, die pro Anzeige an die Strafverfolgungsbehörden übermittelt wurden (2023: 1,8; 2022: 1,4). Die MROS übermittelt den Strafverfolgungsbehörden jeweils einen Analysebericht mit den relevanten Informationen. Diese können aus mehreren Verdachtsmeldungen hervorgehen, die nicht zwingend im selben Jahr bei der MROS eingegangen sind und von verschiedenen in- und ausländischen Behörden stammen.*
- *Die Anzahl der **Informationsanfragen** nach **Artikel 11a GwG** hat weiter zugenommen (+7,1 % im Vergleich zum Vorjahr): Das Ziel der MROS ist es, die Strafverfolgungsbehörden optimal zu unterstützen, was eine vertiefte Analyse gewisser Meldungen voraussetzt. Der Artikel 11a Absatz 2bis GwG, der 2021 in Kraft trat[42], hat zur Folge, dass die MROS vermehrt Informationen bei nicht unmittelbar in die Meldung involvierten Finanzintermediären einholt (sogenannte Drittintermediäre).*
- *Der **Informationsaustausch** zwischen der MROS und den **Schweizer Behörden** nimmt stetig zu: 2023 erhielt die MROS 696 Informationsanfragen von anderen Schweizer Behörden (+4,3 %). Gleichzeitig übermittelte die MROS spontan 200 Informationen an inländische Aufsichtsbehörden oder Behörden, die Geldwäscherei und deren Vortaten, organisierte Kriminalität oder Terrorismusfinanzierung bekämpfen (+13,0 %).*

[40] Geschäftsjahr: 1. Januar bis 31. Dezember des jeweiligen Jahres.

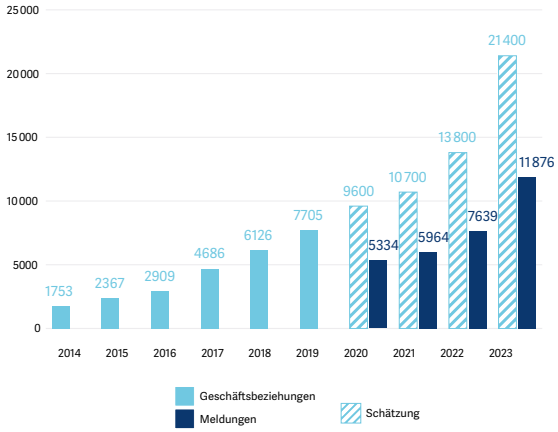
[41] Verordnung über die Meldestelle für Geldwäscherei (MGwV), SR **955.23**

[42] Art. 11*a* Abs. 2 und Abs. 2bis GwG bilden die gesetzliche Grundlage, damit die MROS auch von nicht Meldung erstattenden Drittintermediären die Herausgabe von Informationen einfordern kann (vgl. Kap. 4.12).

4.2 Verdachtsmeldungen

Die Anzahl der Verdachtsmeldungen nimmt von Jahr zu Jahr zu: 2023 hat die MROS insgesamt 11 876 Verdachtsmeldungen erhalten. Das bedeutet, dass 2023 pro Werktag im Schnitt 47 Meldungen eingegangen sind. Im Vergleich zum Vorjahr entspricht dies einem von Plus von 55,5 %. Seit der Einführung des Informationssystems goAML im Jahr 2020 hat sich das Volumen der übermittelten Verdachtsmeldungen sogar mehr als verdoppelt (vgl. Abbildung 2).
Die Entwicklung der gemeldeten Geschäftsbeziehungen seit 2014 ist beeindruckend: Im Jahr 2014 wurden 1753 verdächtige Geschäftsbeziehungen an die MROS gemeldet, 2023 waren es rund 21 400.[43] Die Anzahl der jährlich gemeldeten Geschäftsbeziehungen hat sich in dieser Zeit mehr als verzwölffacht.
Diese Zunahme hat mehrere Gründe: Zum einen sind die Sensibilität und das Bewusstsein der Finanzintermediäre für die Geldwäschereithematik gewachsen. Zum anderen spielen die rechtlichen Anpassungen – insbesondere in Zusammenhang mit der Definition des begründeten Verdachts – und die Fortschritte in der Digitalisierung (z. B. verbesserte Tools beim Transaktionsmonitoring und in der internen Analyse) eine zentrale Rolle (vgl. Kap. 2.1).

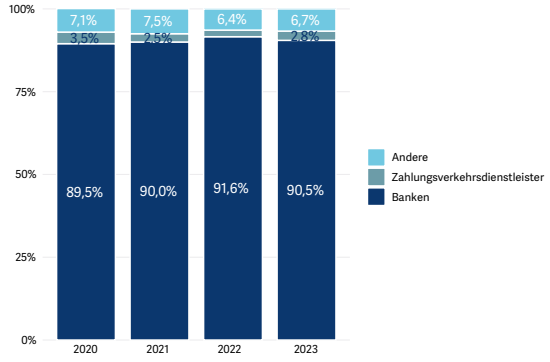
Abbildung 2: Anzahl gemeldete Geschäftsbeziehungen und Verdachtsmeldungen, 2014–2023



4.3 Verdachtsmeldungen nach Branche der Meldepflichtigen

Der überwiegende Teil der Verdachtsmeldungen an die MROS stammt von Finanzintermediären aus dem Bankensektor. Im aktuellen Berichtsjahr handelt es sich um 90,5 % der Meldungen (–1,1 Prozentpunkte gegenüber 2022; vgl. Abbildung 3). Das Meldeverhalten dieser Finanzintermediäre beeinflusst folglich massgeblich die Anzahl und Art der Meldungen, die bei der MROS eingehen. Die Verteilung der Verdachtsmeldungen auf die Meldepflichtigen hat sich seit Einführung des Informationssystems goAML kaum verändert.

Abbildung 3: Verdachtsmeldungen nach Branche, 2020–2023



Dasselbe Bild zeigt sich bei der Anzahl gemeldeter Geschäftsbeziehungen in den verschiedenen Branchen vor 2020 (vgl. Tabelle 2).

[43] Mit der Einführung von goAML wurde die Zählweise der Verdachtsfälle angepasst. Um dennoch einen Vergleich mit den Vorjahren zu ermöglichen, wird in Abbildung 2 die durchschnittliche Anzahl gemeldeter Geschäftsbeziehungen pro Verdachtsmeldung im Geschäftsjahr 2019 angewendet. Diese beläuft sich auf 1,8. Das bedeutet, dass die 11 876 Verdachtsmeldungen im Jahr 2023 geschätzt rund 21 400 Geschäftsbeziehungen entsprechen.

Tabelle 2: Verdachtsmeldungen nach Branche, 2014–2023[44]

Branche	2014[1]	2015[1]	2016[1]	2017[1]	2018[1]	2019[1]	2020[2]	2021[2]	2022[2]	2023[2]	2023 in absoluten Zahlen	Durchschnitt 2014–2023
Banken	85,3%	91,3%	86,0%	91,0%	88,8%	89,9%	89,5%	90,0%	91,6%	90,5%	10744	89,8%
Zahlungsverkehrs-dienstleister	6,1%	2,4%	4,4%	3,1%	4,4%	4,0%	3,5%	2,5%	2,0%	2,8%	328	2,9%
Treuhänder	2,8%	2,0%	1,5%	1,1%	0,7%	0,8%	0,6%	0,5%	0,1%	0,2%	25	0,8%
Vermögensverwaltung	2,3%	1,9%	2,2%	1,9%	1,0%	0,9%	0,8%	1,0%	0,6%	0,8%	90	0,8%
Versicherungen	0,6%	0,5%	3,1%	0,5%	0,6%	0,3%	0,4%	0,3%	0,3%	0,4%	47	0,3%
Übrige Finanzintermediäre	0,2%	0,2%	0,7%	0,4%	2,3%	0,6%	2,3%	2,1%	2,1%	2,0%	240	2,1%
Kreditkartenanbieter	0,5%	0,5%	0,7%	0,3%	1,2%	1,3%	1,6%	1,7%	1,6%	1,3%	154	1,5%
Casinos	0,5%	0,1%	0,5%	0,6%	0,5%	0,7%	0,5%	0,5%	0,7%	0,5%	65	0,6%
Rechtsanwälte und Notare	0,6%	0,3%	0,2%	0,1%	0,1%	0,1%	0,1%	0,1%	0,0%	0,1%	14	0,1%
Kredit-, Leasing-, Factoring- + Forfaitierungsgeschäfte	0,2%	0,3%	0,3%	0,3%	0,3%	0,3%	0,4%	0,3%	0,3%	0,2%	26	0,3%
Wertpapierhäuser	0,6%	0,1%	0,1%	0,3%	0,1%	0,3%	0,0%	0,2%	0,1%	0,2%	22	0,1%
Rohwaren- und Edelmetallhandel	0,2%	0,3%	0,1%	0,2%		0,3%	0,2%	0,5%	0,3%	0,3%	38	0,3%
Devisenhandel			0,1%			0,3%	0,0%					0,0%
SRO	0,1%					0,1%	0,0%			0,1%	6	0,0%
Geldwechsel/Change							0,1%	0,1%	0,3%	0,6%	75	0,4%
Behörden (FINMA/ESBK/GESPA)	0,1%							0,1%		0,0%	2	0,0%
Vertriebsträger von Anlagefonds				0,1%								0,0%
Trustees							0,1%	0,1%				0,0%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**11876**	**100,0%**

[1] *Nach alter Zählweise (Geschäftsbeziehung)*

[2] *Nach neuer Zählweise (Meldungen)*

4.4 Rechtsgrundlage der Meldungen

Die Rechtsgrundlage für eine Verdachtsmeldung ist abhängig vom Verdachtsgrad. Liegt ein begründeter Verdacht vor, haben Finanzintermediäre nach Artikel 9 Absatz 1 Buchstabe a GwG[45] die Pflicht, dies der MROS zu melden. Bei einfachem Verdacht können sie sich auf das Melderecht nach Artikel 305ter Absatz 2 StGB[46] stützen. Seit 2018 gewinnt die Meldepflicht – gegenüber dem Melderecht – an Bedeutung. Diese Entwicklung hat sich 2023 weiter akzentuiert. 2023 meldeten die GwG-Unterstellten in 70,4% der Fälle aufgrund der Meldepflicht gemäss Artikel 9 Absatz 1 Buchstabe a GwG. Das Melderecht nach Artikel 305ter Absatz 2 StGB wendeten sie bei 21,6% der eingereichten Verdachtsmeldungen an. Der Gebrauch des Melderechts hat im Vergleich zum Vorjahr nochmals deutlich abgenommen (-9,1 Prozentpunkte). Es ist anzunehmen, dass dieser markante Bedeutungsgewinn der Meldepflicht über den Jahresverlauf 2023 unter anderem eine

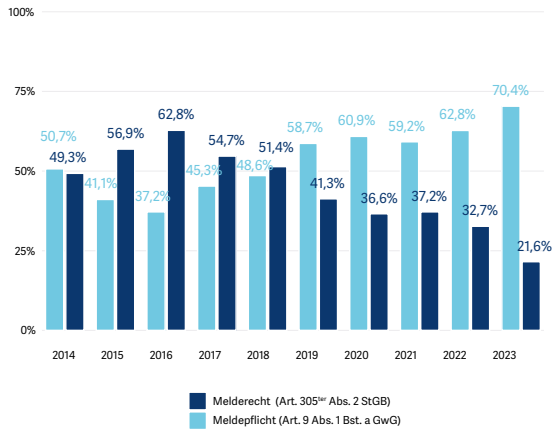
[44] Die absoluten Zahlen für die Jahre 2014–2022 sind in den *Jahresberichten der MROS* der entsprechenden Jahre veröffentlicht.

[45] Art. 9 Abs. 1 Bst. a GwG: Ein Finanzintermediär muss der Meldestelle für Geldwäscherei nach Artikel 23 (Meldestelle) unverzüglich Meldung erstatten, wenn er weiss oder den begründeten Verdacht hat, dass die in die Geschäftsbeziehung involvierten Vermögenswerte (1.) im Zusammenhang mit einer strafbaren Handlung nach Artikel 260ter oder 305bis StGB stehen, (2.) aus einem Verbrechen oder aus einem qualifizierten Steuervergehen nach Artikel 305bis Ziffer 1bis StGB herrühren, (3.) der Verfügungsmacht einer kriminellen oder terroristischen Organisation unterliegen, oder (4.) der Terrorismusfinanzierung (Art. 260^{quinquies} Abs. 1 StGB) dienen.

[46] Art. 305ter Abs. 2 StGB: Die von Absatz 1 erfassten Personen sind berechtigt, der Meldestelle für Geldwäscherei im Bundesamt für Polizei Wahrnehmungen zu melden, die darauf schliessen lassen, dass Vermögenswerte aus einem Verbrechen oder aus einem qualifizierten Steuervergehen nach Artikel 305bis Ziffer 1bis herrühren.

Folge des Inkrafttretens der GwG-Revision am 1. Januar 2023 ist: Neu definiert Artikel 9 Absatz 1quarter GwG den begründeten Verdacht.[47]

Abbildung 4: Meldungen bei bestehender Geschäftsbeziehung nach Rechtsgrundlage, 2014–2023

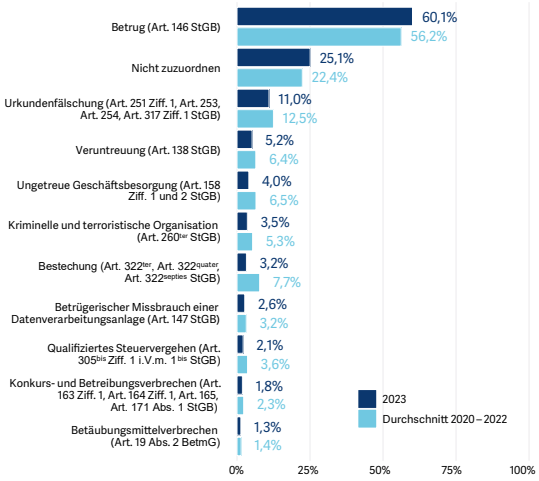


In 941 Fällen (7,9 %) meldeten die Finanzintermediäre zudem, dass sie Verhandlungen zur Aufnahme einer Geschäftsbeziehung wegen eines begründeten Verdachts nach Artikel 9 Absatz 1 Buchstabe a GwG abgebrochen hätten.[48]

4.5 Vortaten

Finanzintermediäre geben bei einer Meldung jeweils an, welche Vortaten sie vermuten. Seit 2020 hat sich an der Häufigkeitsverteilung der vermuteten Vortaten wenig verändert (vgl. Abbildung 5). 2023 rangieren unter den ersten zehn dieselben wie bereits 2020. Betrug wird von den Finanzintermediären am häufigsten genannt (2023: 60,1 %; 2020–2022: 56,2 %).

Abbildung 5: Häufigkeit der vermuteten Vortaten, 2020–2023, Mehrfachnennungen möglich



Es zeigt sich eine leichte Tendenz, dass Finanzintermediäre vermehrt Betrug als vermutete Vortat nennen, während Vortaten wie Bestechung oder ungetreue Geschäftsbesorgung an Bedeutung verlieren. Ob diese Entwicklung auf einem veränderten Meldeverhalten der Finanzintermediäre oder auf einer Verschiebung der zugrunde liegenden tatsächlichen Vortaten basiert, lässt sich aufgrund der vorhandenen Zahlen nicht beurteilen.
Allgemein lässt sich aus den Angaben der Finanzintermediäre zu den vermuteten Vortaten nicht auf die effektiv begangenen Geldwäschereivortaten schliessen. Diese Zahlen zeigen lediglich auf, welche Straftaten die Finanzintermediäre bei der Erstattung der Verdachtsmeldung vermuteten. Die Analyse der MROS kann auch den Verdacht auf eine andere Straftat ergeben. Eine detailliertere Analyse zu den verschiedenen Geldwäschereivortaten wurde 2022 unter der Federführung der KGGT vorgenommen.[49]

---

47 Art. 9 Abs. 1quarter GwG definiert, dass ein begründeter Verdacht nach Art. 9 Abs. 1 Bst. a GwG vorliegt, wenn der Finanzintermediär einen konkreten Hinweis oder mehrere Anhaltspunkte hat, dass für die in die Geschäftsbeziehung involvierten Vermögenswerte Art. 9 Abs. 1 Bst. a GwG erfüllt sein könnte, und dieser Verdacht aufgrund zusätzlicher Abklärungen gemäss Art. 6 GwG nicht ausgeräumt werden kann.

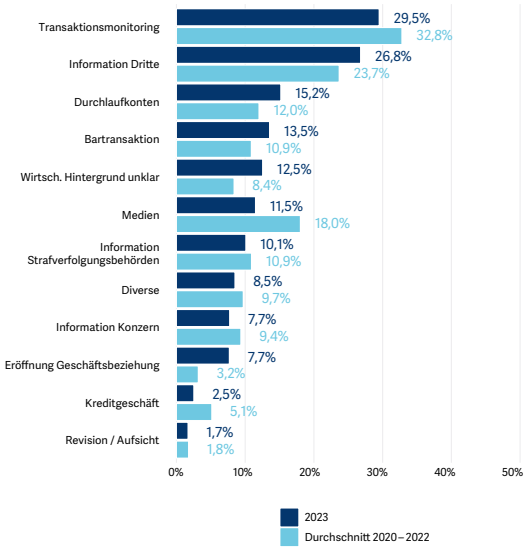
48 Art. 9 Abs. 1 Bst. b GwG: Ein Finanzintermediär muss der Meldestelle für Geldwäscherei nach Artikel 23 (Meldestelle) unverzüglich Meldung erstatten, wenn er Verhandlungen zur Aufnahme einer Geschäftsbeziehung wegen eines begründeten Verdachts nach Art. 9 Abs. 1 Bst. a GwG abbricht.

49 Vgl. Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung (KGGT): *Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung*, Oktober 2021, S. 25–29.

4.6 Verdachtsauslösende Elemente

Wie in den Jahren zuvor zeigt sich auch 2023, dass Finanzintermediäre am häufigsten wegen eines Transaktionsmonitorings eine Verdachtsmeldung an die MROS absetzen (2023: 29,5 %; 2020 – 2022: 32,8 %; vgl. Abbildung 6). Bei 15,2 % der 2023 eingegangenen Meldungen waren Durchlaufkonten der Auslöser für einen Verdacht. Eine wesentliche Rolle für die Beurteilung der Finanzintermediäre spielen allerdings auch externe Informationsquellen: 2023 erfolgten 26,8 % der Verdachtsmeldungen aufgrund Informationen Dritter (2020 – 2022: 23,7 %; vgl. Abbildung 6).

Abbildung 6: Wichtige Verdachtsauslöser 2020 – 2023[50]
Mehrfachnennungen möglich



4.7 Anzeigen an die Strafverfolgungsbehörden

2023 hat die MROS, gestützt auf Artikel 23 Absatz 4 GwG, 866 Anzeigen an die Strafverfolgungsbehörden übermittelt. Dies entspricht einem Rückgang von 29,7 % gegenüber dem Vorjahr (2022: 1232). Die 2023 übermittelten Anzeigen sind im Vergleich zum Vorjahr umfangreicher: Während 2022 eine Anzeige im Schnitt auf rund 1,4 Meldungen der Finanzintermediäre an die MROS basierte, stützen sich 2023 die Übermittlungen im Schnitt auf 1,8 Verdachtsmeldungen ab.

Die 866 übermittelten Anzeigen enthalten Informationen aus:
- 1201 im Jahr 2023 eingegangenen Meldungen
- 276 im Jahr 2022 eingegangenen Melduen
- 28 im Jahr 2021 eingegangenen Meldungen
- 12 im Jahr 2020 eingegangenen Meldungen
- Fünf im Jahr 2019 gemeldeten Geschäftsbeziehungen
- Drei im Jahr 2018 gemeldeten Geschäftsbeziehungen
- Zwei im Jahr 2017 gemeldeten Geschäftsbeziehungen

Auch in diesem Jahr zeigt sich, dass die Grösse des Finanzsektors eines Kantons einen bedeutenden Einfluss auf die Anzahl der Anzeigen an die jeweilige Staatsanwaltschaft hat (vgl. Tabelle 3). 2023 erfolgen die meisten Anzeigen der Meldestelle an die Staatsanwaltschaften der Kantone Genf (17,6 %) und Zürich (16,3 %) – wie bereits in den Vorjahren. An dritter Stelle steht die Bundesanwaltschaft (BA) mit 13,0 % – was einer Zunahme von 6,6 Prozentpunkten im Vergleich zum Vorjahr entspricht.

[50] Gegenüber den Jahren vor 2020 können die Finanzintermediäre im Informationssystem goAML mehrere verdachtsauslösende Elemente für ihre Meldungen angeben. Hingegen ist es nicht mehr möglich, einen aussagekräftigen Vergleich mit den Zahlen der Jahre vor 2020 vorzunehmen.

Tabelle 3: Übermittelte Anzeigen nach Strafverfolgungsbehörden 2020–2023

Behörde	2020	2021	2022	2023	2023 in absoluten Zahlen	Durchschnitt 2020–2023
Genf	11,5 %	11,3 %	11,6 %	17,6 %	152	13,0 %
Zürich	18,9 %	21,1 %	20,4 %	16,3 %	141	19,2 %
Bundesanwaltschaft	9,0 %	9,1 %	6,4 %	13,0 %	113	9,4 %
Waadt	11,1 %	11,6 %	10,6 %	8,3 %	72	10,4 %
Bern	7,5 %	6,7 %	6,9 %	6,5 %	56	6,9 %
St. Gallen	3,5 %	4,0 %	6,3 %	5,3 %	46	4,8 %
Tessin	5,0 %	4,8 %	3,6 %	4,6 %	40	4,5 %
Aargau	5,3 %	5,2 %	6,7 %	4,2 %	36	5,3 %
Thurgau	3,0 %	2,1 %	2,6 %	3,2 %	28	2,7 %
Luzern	3,5 %	2,9 %	2,6 %	2,5 %	22	2,9 %
Wallis	2,7 %	2,4 %	3,0 %	2,2 %	19	2,6 %
Zug	2,5 %	2,6 %	2,2 %	2,2 %	19	2,4 %
Schwyz	1,0 %	1,1 %	1,9 %	2,1 %	18	1,5 %
Basel-Stadt	2,6 %	2,3 %	2,3 %	1,8 %	16	2,3 %
Basel-Landschaft	2,1 %	1,7 %	2,3 %	1,8 %	16	2,0 %
Solothurn	1,9 %	2,0 %	2,1 %	1,4 %	12	1,8 %
Freiburg	2,7 %	3,1 %	2,1 %	1,3 %	11	2,3 %
Neuenburg	2,3 %	1,9 %	1,7 %	1,3 %	11	1,8 %
Appenzell Ausserrhoden	0,6 %	0,8 %	1,3 %	0,9 %	8	0,9 %
Schaffhausen	0,5 %	0,5 %	0,6 %	0,7 %	6	0,6 %
Jura	0,3 %	1,0 %	0,2 %	0,7 %	6	0,6 %
Graubünden	1,5 %	1,0 %	1,1 %	0,6 %	5	1,0 %
Nidwalden	0,3 %	0,4 %	0,6 %	0,6 %	5	0,5 %
Glarus	0,2 %	0,1 %	0,4 %	0,6 %	5	0,3 %
Appenzell Innerrhoden	0,0 %	0,1 %	0,2 %	0,2 %	2	0,1 %
Uri	0,3 %	0,1 %	0,2 %	0,1 %	1	0,2 %
Obwalden	0,2 %	0,1 %	0,2 %	0,0 %	0	0,1 %
Total	**100,0 %**	**100,0 %**	**100,0 %**	**100,0 %**	**866**	**100,0 %**

Insgesamt übermittelte die MROS 13,0 % der Strafanzeigen (113 Anzeigen) an die Bundesanwaltschaft und 87,0 % an die kantonalen Staatsanwaltschaften (753 Anzeigen).

4.8 Rückmeldungen der Strafbehörden

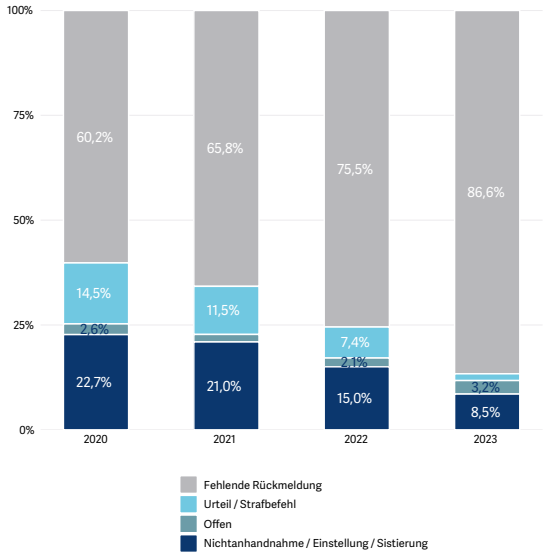
Gemäss Artikel 29*a* GwG melden die Strafbehörden der MROS sämtliche hängigen Verfahren insbesondere zu Geldwäscherei, kriminellen und terroristischen Organisationen sowie Finanzierung des Terrorismus. Sie stellen ihr rasch die diesbezüglichen Urteile und Einstellungsverfügungen zu.[51] Zudem melden sie ihr unverzüglich Verfügungen, die sie aufgrund einer Anzeige der Meldestelle erlassen haben.[52] Diese Rückmeldungen sind für den Auftrag der MROS, die

[51] Art. 29a Abs. 1 GwG: Die Strafbehörden melden der Meldestelle umgehend sämtliche hängigen Verfahren im Zusammenhang mit den Artikeln 260ter, 260^{quinquies} Absatz 1, 305bis und 305ter Absatz 1 StGB. Sie stellen ihr rasch Urteile und Einstellungsverfügungen inklusive Begründung zu.

[52] Art. 29a Abs. 2 GwG.

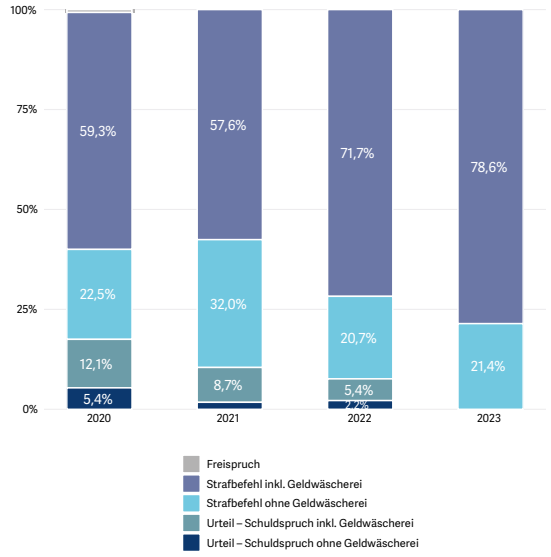
Strafverfolgungsbehörden bestmöglich zu unterstützen, entscheidend.
Die Rückmeldung der Strafbehörden stehen bei einer Mehrheit der Anzeigen noch aus (vgl. Abbildung 7 sowie Ausführung in Kap. 6.2). Es lassen sich deshalb keine Erkenntnisse über das Verhältnis von Urteil und Einstellungsverfügung aus den aktuell verfügbaren Zahlen ziehen.

Abbildung 7: Rückmeldungen der im jeweiligen Jahr übermittelten Anzeigen, 2020–2023



Von den zwischen 2020 und 2022[53] übermittelten Anzeigen fehlen der MROS in zwei Drittel der Fälle die Angabe über den Verfahrensstand. Je nach Kanton variieren die Rückmeldungsquoten dabei deutlich.
Bei den Rückmeldungen, die die MROS bis Ende 2023 erhalten hat und zu einem Strafbefehl oder einem Urteil führten, war Geldwäscherei der überwiegende Tatbestand (78,6 %; vgl. Abbildung 8). 2022 hatten 77,1 % der Urteile oder Strafbefehle einen Bezug zu Geldwäscherei, 2021 waren es 66,3 %, 2020 71,4 %.

Abbildung 8: Aufteilung der kommunizierten Urteile / Strafbefehle, 2020–2023



4.9 Terrorismusfinanzierung

2023 erhielt die MROS 93 Meldungen wegen Verdacht auf Terrorismusfinanzierung und/oder wegen Verstoss gegen das Bundesgesetz über das Verbot der Gruppierungen «Al-Qaïda» und «Islamischer Staat» sowie verwandter Organisationen.[54] Dies entspricht 2023 0,8 % aller eingegangenen Meldungen. Die meisten davon werden zusätzlich mit anderen Vortaten in Verbindung gebracht. Weitere Verdachtsgründe waren in 30 Fällen die Zugehörigkeit zu kriminellen und terroristischen Organisationen[55], in sieben Fällen Betrug[56] und in je zwei Fällen qualifiziertes Steu-

[53] Um zu berücksichtigen, dass eine Rückmeldung der Strafbehörden an die MROS eine gewisse Zeit beansprucht, werden jeweils die Zahlen des aktuellen Berichtsjahrs in der Statistik nicht hinzugezogen.

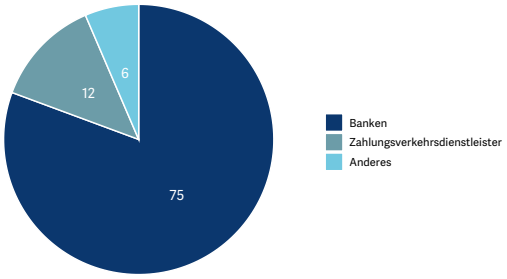
[54] Bundesgesetz über das Verbot der Gruppierungen «Al-Qaïda» und «Islamischer Staat» sowie verwandter Organisationen, SR **122**, vollständige Aufhebung per 1. Dezember 2022.

[55] Art. 260ter StGB.

[56] Art. 146 StGB.

ervergehen[57], Bestechung[58], Urkundenfälschung[59] und/oder Veruntreuung[60].
Die meisten Meldungen mit Verdacht auf Terrorismusfinanzierung stammen von Banken (75 von 93; vgl. Abbildung 9); 12 davon von Zahlungsverkehrsdienstleistern.

Abbildung 9: Anzahl Meldungen wegen Verdacht auf Terrorismusfinanzierung nach Branche, 2023



Die von den Finanzintermediären am häufigsten genannten Verdachtsauslöser waren im Jahr 2023 Presseberichte (37 Fälle), Transaktionsmonitoring (19 Fälle) sowie Informationen von Dritten (16 Fälle), von Konzernen (13 Fälle) oder von Strafverfolgungsbehörden (10 Fälle) sowie Bartransaktionen (13 Fälle).
Die 93 im Verlauf des Jahres 2023 eingegangenen Meldungen führten zu fünf Anzeigen zuhanden der zuständigen Strafverfolgungsbehörden. Drei der im Vorjahr 2022 eingegangen Meldungen mit Verdacht auf diesen Straftatbestand wurden ebenfalls 2023 an die zuständigen Strafverfolgungsbehörden zur Anzeige übermittelt.

4.10 Organisierte Kriminalität

2023 erhielt die MROS 421 Meldungen wegen eines Verdachts auf Verbindungen zu kriminellen und terroristischen Organisationen, was 3,5 % der insgesamt erhaltenen Verdachtsmeldungen entspricht.

Die überwiegende Mehrheit (90 %) dieser Verdachtsmeldungen wurden der MROS von Banken zugestellt (vgl. Abbildung 10). Auslöser für eine Verdachtsmeldung waren Informationen aus Medien (37 %) und/oder ein Transaktionsmonitoring (25 %; vgl. Tabelle 5). Neben der vermuteten Verbindung zu einer kriminellen Organisation nannten die Finanzintermediäre weiter Betrug (44 %) und Bestechung (8 %, vgl. Tabelle 4) als mögliche Vortat. Die 421 Meldungen im Berichtsjahr führten zu 33 Anzeigen an die zuständigen Strafverfolgungsbehörden.

Abbildung 10: Meldungen wegen Verdachts auf Verbindungen zu kriminellen oder terroristischen Organisationen nach Branche, 2023

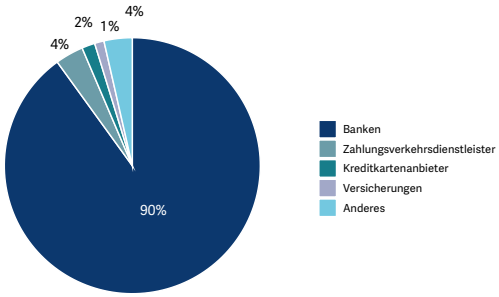


Tabelle 4: Weitere Vortaten in Verdachtsmeldungen wegen mutmasslichen Verbindungen zu kriminellen und terroristischen Organisationen

Weitere Vortaten (Mehrfachnennungen möglich)	**Anzahl Nennungen**	**In %**
Betrug (Art. 146 StGB)	185	44 %
Bestechung (Art. 322ter, Art. 322quater, Art. 322septies StGB)	33	8 %
Finanzierung des Terrorismus (Art. 260quinquies StGB)	27	6 %
Betäubungsmittelverbrechen (Art. 19 Abs. 2 BetmG)	26	6 %
Veruntreuung (Art. 138 StGB)	23	5 %

[57] Art. 305bis Ziff. 1 und 1bis StGB.
[58] Art. 322ter, Art. 322quater oder Art. 322septies StGB.
[59] Art. 251 Ziff. 1, Art. 253, Art. 254, Art. 317 Ziff. 1 StGB.
[60] Art. 138 StGB.

Weitere Vortaten (Mehrfachnennungen möglich)	Anzahl Nennungen	In %
Urkundenfälschung (Art. 251 Ziff. 1, Art. 253, Art. 254, Art. 317 Ziff. 1 StGB)	18	4%
Qualifiziertes Steuervergehen (Art. 305bis Ziff. 1 und 1bis StGB)	15	4%
Ungetreue Geschäftsbesorgung (Art. 158 Ziff. 1 und 2 StGB)	15	4%
Erpressung (Art. 156 StGB)	8	2%

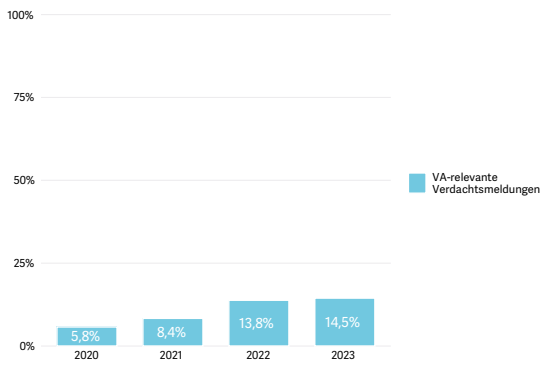
Tabelle 5: Häufigkeit verdachtsauslösender Merkmale in Meldungen wegen mutmasslichen Verbindungen zu kriminellen und terroristischen Organisationen

Verdachtsauslöser (Mehrfachnennungen möglich, Häufigkeitsauswahl)	Anzahl Nennungen	In %
Medien	155	37%
Transaktionsmonitoring	105	25%
Information Dritte	80	19%
Durchlaufkonten	49	12%
Diverse	46	11%
Bartransaktionen	44	10%
Eröffnung einer Geschäftsbeziehung	43	10%
Information Strafverfolgungsbehörde	38	9%
Wirtschaftlicher Hintergrund unklar	31	7%
Information Konzern	25	6%
Kreditgeschäft	12	3%

4.11 Verdachtsmeldungen mit Bezug zu Kryptowährungen

Verdachtsmeldungen, die einen Bezug zu Kryptowährungen (Virtual Assets, VAs) haben, gewinnen zunehmend an Bedeutung.[61] 2023 spielten Kryptowährungen bei 14,5% aller Meldungen eine Rolle; dies entspricht zweieinhalbmal so vielen wie noch 2020 (5,8%; vgl. Abbildung 11).[62] Diese Entwicklung stellt die MROS vor zunehmende Herausforderungen: Kryptowährungen erschweren die Nachverfolgung von Geldströmen und damit die Herkunft des Vermögens und die eindeutige Identifikation des wirtschaftlich Berechtigten. Die MROS analysierte im sektoriellen Bericht «National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets» die Risiken, welche mit Kryptowährungen einhergehen. Der entsprechende Bericht wurde im ersten Quartal 2024 publiziert (vgl. Kap. 2.3).[63]

Abbildung 11: Anteil der VA-relevanten Meldungen am Total der Verdachtsmeldungen, 2020–2023



4.12 Herausgabe von Informationen nach Artikel 11*a* GwG

Seit 2021 nimmt die Zahl der Informationsanfragen an die Finanzintermediäre auf Basis von Artikel 11*a* GwG stetig zu. Im Berichtsjahr zeigt sich erneut eine Zunahme der Informationsanfra-

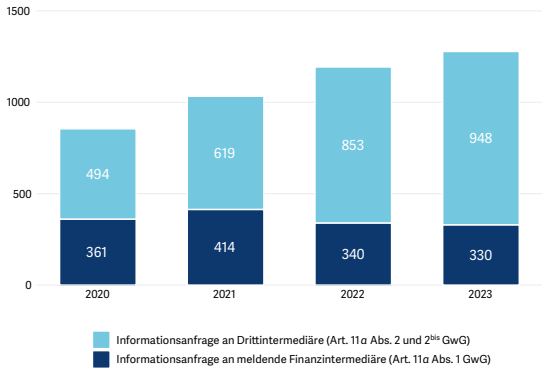
[61] Mit der Verankerung von Art. 4 Abs. 2 Bst. a in der Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereiverordnung, GwV), SR **955.01**, am 1. Januar 2016 wurde in der Schweiz der Begriff der «virtuellen Währung» erstmals in einem rechtlichen Erlass erfasst.

[62] Inwiefern in einer Meldung Transaktionen mit Kryptowährungen Gegenstand des Verdachts sind, lässt sich bis anhin nicht direkt erfassen, da solche Transaktionen nicht eindeutig identifizierbar sind. Verdachtsmeldungen mit einem relevanten VA-Bezug wurden deshalb einerseits mittels Transaktionen zwischen den in der Meldung angezeigten Konten und Konten von schweizerischen oder ausländischen Finanzintermediären mit VASP-Tätigkeit und andererseits mit einer Schlagwortliste relevanter Begriffe identifiziert. Es ist deshalb anzunehmen, dass die Bedeutung von Kryptowährungen in Verdachtsmeldungen eher unterschätzt wird.

[63] *National Risk Assessment (NRA), Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets*.

gen im Vergleich zum Vorjahr (+7,1 %; vgl. Abbildung 12). Dieser Anstieg betrifft hauptsächlich mehr Anfragen an sogenannte Drittintermediäre, die neben dem meldenden Finanzintermediär an einer Transaktion oder einer Geschäftsbeziehung beteiligt sind oder waren (+11,1 %; Art. 11*a* Abs. 2[64] und 2[bis] GwG[65]). Vergleichsweise konstant ist dagegen die Anzahl der Anfragen nach Artikel 11*a* Absatz 1 GwG[66] (–2,9 % im Vergleich zum Vorjahr), die sich an die Finanzintermediäre der ursprünglichen Verdachtsmeldungen richten.

Abbildung 12: Aufforderung zur Herausgabe von Informationen nach Artikel 11a GwG, 2020–2023

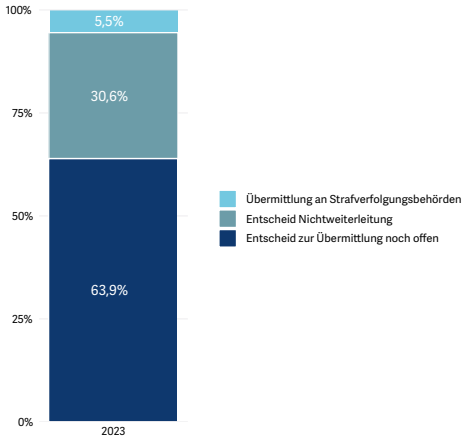


4.13 Abbruchsmeldungen nach Artikel 9*b* GwG

Seit dem 1. Januar 2023 können Finanzintermediäre, gestützt auf Artikel 9*b* GwG[67], eine Geschäftsbeziehung 40 Arbeitstage, nachdem sie sie der MROS gemeldet haben, abbrechen – insofern sie nicht über eine Übermittlung an die Strafverfolgungsbehörden informiert wurden. Den Abbruch der Geschäftsbeziehung hat der Finanzintermediär unmittelbar der MROS zu melden.[68]

2023 hat die MROS 2669 Abbruchsmeldungen erhalten. 5,5 % davon beziehen sich auf Verdachtsmeldungen, die nach Ablauf der 40 Arbeitstage dennoch an Strafverfolgungsbehörden weitergeleitet wurden, 63,9 % auf solche, bei denen der Entscheid zur Übermittlung noch aussteht, und 30,6 % auf solche, die nicht weitergeleitet wurden (vgl. Abbildung 13).

Abbildung 13: Stand der Verdachtsmeldungen mit Abbruchsmeldungen, 2023



[64] Art. 11*a* Abs. 2 GwG: Wird aufgrund dieser Analyse erkennbar, dass neben dem meldenden Finanzintermediär weitere Finanzintermediäre an einer Transaktion oder Geschäftsbeziehung beteiligt sind oder waren, so müssen die beteiligten Finanzintermediäre der Meldestelle auf Aufforderung hin alle damit zusammenhängenden Informationen herausgeben, soweit sie bei ihnen vorhanden sind.

[65] Art. 11*a* Abs. 2[bis] GwG: Wird aufgrund der Analyse von Informationen, die von einer ausländischen Meldestelle stammen, erkennbar, dass diesem Gesetz unterstellte Finanzintermediäre an einer Transaktion oder Geschäftsbeziehung im Zusammenhang mit diesen Informationen beteiligt sind oder waren, so müssen die beteiligten Finanzintermediäre der Meldestelle auf Aufforderung hin alle damit zusammenhängenden Informationen herausgeben, soweit sie bei ihnen vorhanden sind.

[66] Art. 11*a* Abs. 1 GwG: Benötigt die Meldestelle zusätzliche Informationen für die Analyse einer bei ihr nach Artikel 9 GwG oder nach Artikel 305[ter] Absatz 2 StGB eingegangenen Meldung, so muss ihr der meldende Finanzintermediär diese auf Aufforderung hin herausgeben, soweit sie bei ihm vorhanden sind.

[67] Nach Art. 9*b* GwG können Finanzintermediäre eine nach Art. 9 Abs. 1 Bst. a GwG oder nach Art. 305[ter] Abs. 2 StGB gemeldete Geschäftsbeziehung abbrechen, sofern die Meldestelle nicht dem Finanzintermediär innert 40 Arbeitstagen mitteilt, dass sie die gemeldeten Informationen einer Strafverfolgungsbehörde übermittelt hat

[68] Art. 9*b* Abs. 3 GwG.

4.14 Informationsaustausch mit ausländischen Meldestellen (FIUs)

Im Kampf gegen die Geldwäscherei und deren Vortaten, die Terrorismusfinanzierung und die organisierte Kriminalität funktioniert der Informationsaustausch zwischen der MROS und ihren ausländischen Partnerbehörden (den FIUs) über die Amtshilfe. Gehen bei der MROS Verdachtsmeldungen zu ausländischen (natürlichen oder juristischen) Personen ein, kann die MROS bei den FIUs der entsprechenden Länder Informationen über diese Personen einholen. Diese Informationen sind für die Analysen der MROS von grosser Bedeutung, da eine Vielzahl der Verdachtsmeldungen einen Auslandsbezug haben.[69] Die Zahl der Anfragen der MROS an ausländische FIUs hat während der letzten Jahre kontinuierlich zugenommen. 2023 richtete die MROS 280 Auskunftsersuchen an 67 verschiedene FIUs im Ausland – im Vergleich zum Vorjahr bedeutet dies eine Zunahme um 6,9 %.
Im Juli 2021 erhielt die MROS im Bereich des Informationsaustausches mit ausländischen Partnerstellen mehr Kompetenzen (Art. 11*a* Abs. 2bis GwG). Dies hatte zur Folge, dass 2022 die Anzahl der Anfragen ausländischer Meldestellen an die MROS deutlich anstieg (2022: 851 Anfragen aus 89 Ländern). Die MROS darf seither ihre Antworten an die Partnerbehörden mit weiteren relevanten Finanzinformationen anreichern. Dies führt in gewissen Fällen zu komplexeren Anfragen und einer aufwändigeren Bearbeitung als vor 2021. 2023 ist die Anzahl der Anfragen (705; –17,2 %) aus 92 Ländern wieder gesunken. Die MROS bearbeitete 350 davon und 306 Anfragen aus dem Vorjahr.
Ausländische FIUs und die MROS können auch Spontaninformationen austauschen. Es handelt sich um einen Informationsaustausch ohne vorherige Anfrage, sei es aus dem Ausland mit einem Bezug zur Schweiz oder von der MROS an eine ausländische FIU. Im Berichtsjahr gingen 726 solcher Spontaninformationen aus 53 Ländern bei der MROS ein (2022: 709 aus 50 Ländern). Die MROS versendete 160 Spontaninformationen an 47 ausländische FIUs (2022: 178 an 56 ausländische FIUs).

4.15 Informationsaustausch mit Schweizer Behörden

Gestützt auf Artikel 29 GwG teilt die MROS auch mit Schweizer Behörden relevante Informationen – auf Anfrage oder spontan. Es handelt sich um Aufsichtsbehörden oder andere Behörden, die im Kampf gegen die Geldwäscherei und deren Vortaten, organisierte Kriminalität oder Terrorismusfinanzierung aktiv sind.
Die Statistiken der Vorjahre belegen, dass der Austausch mit inländischen Behörden seit 2020 an Bedeutung gewonnen hat.[70] Im aktuellen Berichtsjahr erhielt die MROS 696 Informationsanfragen von 29 Schweizer Behörden zu bestimmten Bankkonten, Personen oder Unternehmen (im Vergleich zum Vorjahr bedeutet dies ein Plus von 4,3 %). Wie bereits in den Vorjahren stammt der Grossteil der Anfragen von polizeilichen Behörden: 82,0 % der Anfragen kamen von einer Kantonspolizei oder von der Bundeskriminalpolizei.
2023 gingen zudem 119 Spontaninformationen von inländischen Behörden bei der MROS ein (2022: 109). Die MROS übermittelte ihrerseits in 200 Fällen unaufgefordert Informationen an Schweizer Aufsichts- und andere Behörden (+13,0 %; 2022: 177). Die MROS kann im Rahmen ihrer Analysen auch bei anderen Bundes-, Kantons- und Gemeindebehörden Informationen anfragen; diese Anfragen sind in den vorgängig aufgeführten Zahlen nicht erfasst.

---

[69] Vgl. Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung (KGGT): *Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung*, Oktober 2021.

[70] Vgl. Bundesamt für Polizei (fedpol), Publikationen der Meldestelle für Geldwäscherei (MROS), *Jahresberichte der MROS*.

5. Typologien[71]

Das Dispositiv zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung ist komplex. In ihrer Funktion als Drehscheibe kann die Meldestelle in Situationen, in welchen Informationen lediglich fragmentarisch verfügbar sind, einen substanziellen Beitrag an die Vermittlung eines ganzheitlichen Bildes leisten. Die effiziente Nutzung der gesetzlich zur Verfügung stehenden Instrumente und die Verknüpfung der ihr vorliegenden Informationen führen zu einem Gesamtüberblick und schaffen einen konkreten Mehrwert für Strafverfolgungs- und andere Behörden. Diese Aufgaben versteht die MROS unter «Schaffung von Intelligence», worin sie auch ihre zentrale Rolle sieht. Ziel dieses Kapitels ist es, anhand konkreter Beispiele das Verständnis von «Intelligence» bei der MROS zu veranschaulichen.

5.1 Typologie 1 – Nationale und internationale Kooperation

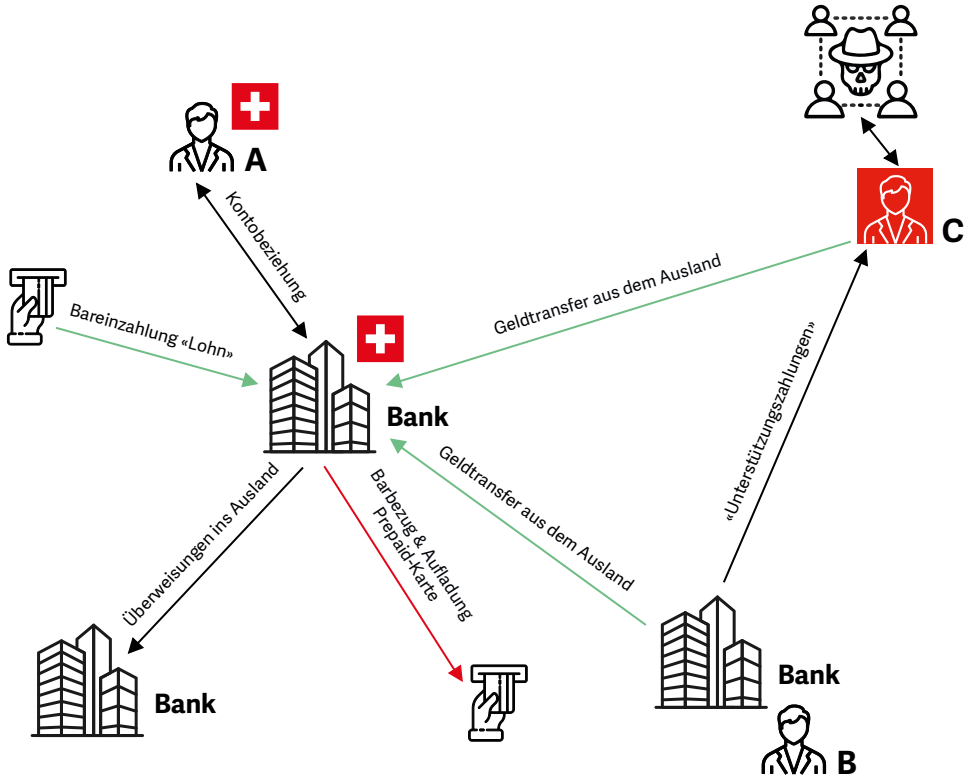
Der nachfolgende Fall legt dar, wie wichtig die nationale und internationale Kooperation bei der Bekämpfung der Geldwäscherei, deren Vortaten, der organisierten Kriminalität oder der Terrorismusfinanzierung ist. Nur durch den nationalen und internationalen Austausch können einzeln vorhandene Informationen in den Systemen zu einem gesamtheitlichen Bild zusammengefügt und die entsprechenden Schlüsse gezogen werden.

Fallbeispiel: Verdacht auf Staatssturz
Anfangs 2022 begannen in der Schweiz und im Ausland Ermittlungen gegen verschiedene Personen wegen des Verdachts auf Planung eines Staatssturzes. Mitte desselben Jahres erhielt die MROS erstmals ein Amtshilfeersuchen im Zusammenhang mit einem Ermittlungsverfahren im Ausland. Konkret ging es um eine in der Schweiz wohnhafte Person (A), welche über einen Mittelsmann (B) Unterstützungszahlungen an eine ausländische Zielperson (C) getätigt haben soll. Die Zielperson (C) sei ein hochrangiges Mitglied einer Organisation, welche einen Staatssturz plane. Kurz darauf erhielt die MROS eine weitere Anfrage einer ausländischen FIU im selben Zusammenhang, dieses Mal mit Fokus auf die sich im Ausland befindliche Zielperson (C) und deren Beziehungen zu einer weiteren Person mit Wohnsitz in der Schweiz. Die von der FIU übermittelten Informationen enthielten einen Hinweis auf eine Geschäftsbeziehung bei einem Schweizer Finanzintermediär. Die MROS edierte beim besagten Finanzintermediär Informationen zur relevanten Geschäftsbeziehung. Die MROS leitete eine eigene Analyse ein und ersuchte gleichzeitig die ausländische FIU um Auskunft. Für die Analyse war wichtig zu wissen, ob in Bezug auf die ausländischen Geldabsender und -empfänger Informationen im Zusammenhang mit Geldwäscherei und deren Vortaten bekannt sind oder ob ein Strafverfahren hängig ist.
Die MROS führte für ihre holistische Analyse die nationalen und internationalen Informationen sowie die Verdachtsmeldungen zusammen und zeichnete folgendes Gesamtbild: A tätigte in den zweieinhalb Jahren vor Eingang der ersten Verdachtsmeldung ungewöhnlich viele und hohe

[71] Für alle beteiligten Personen gilt die Unschuldsvermutung.

Bareinzahlungen. Er erklärte dies damit, dass er seine Lohnzahlungen jeweils in bar erhalten würde. Die Beträge wurden jeweils entweder kurz nach der Einzahlung in bar bezogen oder direkt ins Ausland weitergeleitet. Diese Vorgehensweisen wertete die MROS als Durchlauftransaktionen. A konnte nicht schlüssig darlegen, weshalb eine fremde Person Zugriff auf sein persönliches Konto hatte und regelmässig Prepaid-Travel-Cash-Karten mit hohen Beträgen lud. Zudem nahm A von ausländischen Personen Gelder entgegen, welche dank der Informationen aus der internationalen Zusammenarbeit als Drahtzieher des geplanten Staatssturzes identifiziert werden konnten. Weiter entdeckte die MROS Verbindungen zur rechtsextremen Szene im In- und Ausland. Im Januar 2023 sandte die MROS eine Spontaninformation an eine ausländische FIU, die die Informationen konsolidiert aufarbeitete. Zusätzlich übermittelte die MROS den Analysebericht an die zuständige Schweizer Strafverfolgungsbehörde (Art. 23 Abs. 4 GwG), die im März 2023 ein Strafverfahren gegen die Beschuldigten mit Wohnsitz in der Schweiz eröffnete, wegen Beteiligung an kriminellen und terroristischen Organisationen (Art. 260ter StGB). Dieses Beispiel veranschaulicht, dass eine Verdachtsmeldung an und für sich oder eine Anfrage aus dem Ausland oftmals nicht genügend Substanz bieten, um eine mögliche Straftat zu erkennen. In diesem Fall brachte zudem nicht ein Finanzintermediär, sondern eine ausländische FIU den Sachverhalt der Meldestelle zur Kenntnis. Die Zusammenarbeit zwischen der MROS, den nationalen und internationalen Partnerbehörden und die daraus resultierende Schaffung von «Intelligence» waren ausschlaggebend für die Übermittlung an die zuständige Schweizer Strafverfolgungsbehörde. Ausserdem zeigt dieser Fall besonders gut auf, dass Informationen bei deren Übermittlung an die MROS nicht immer unmittelbar aufschlussreich sind, aber zu einem späteren Zeitpunkt und in Kombination mit weiteren Informationen gesamtheitlich betrachtet strafrechtlich relevant sein können.

Abbildung 14: Typologie 1 – Verdacht auf Staatssturz



5.2 Typologie 2 – Nutzung des gesetzlichen Instrumentariums

Das folgende Fallbeispiel illustriert, dass die MROS bei der Analyse der Verdachtsmeldungen einen Fokus auf die Bekämpfung von Schwerstkriminalität richtet. Die MROS entscheidet anhand der Triagematrix, wie tief eine Verdachtsmeldung zu analysieren ist. Danach setzt sie alle notwendigen und gesetzlich vorgesehenen Instrumente ein, um für die Strafverfolgungsbehörde einen möglichst vollständigen Überblick der Sachlage zu erstellen.

Fallbeispiel: Menschenhandel und Zwangsprostitution

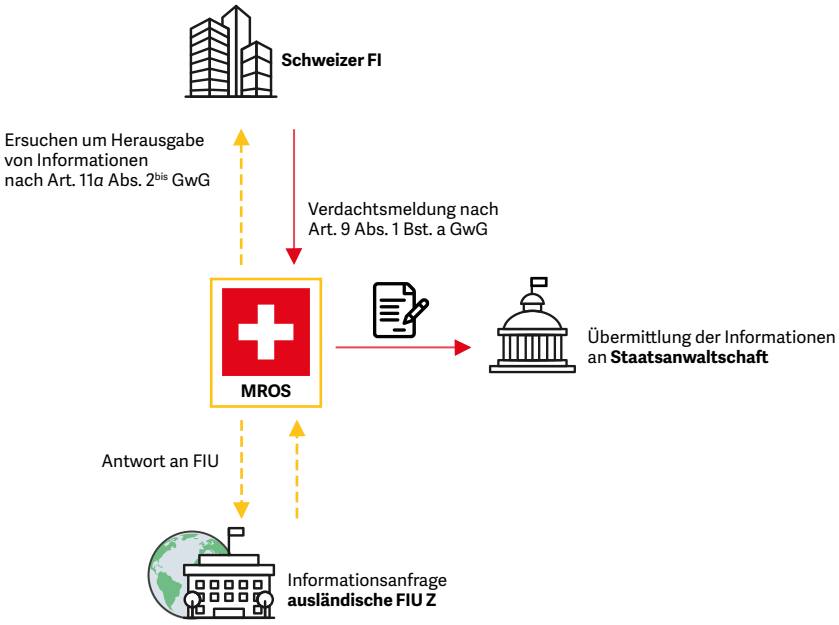
Die MROS erhielt im Jahr 2022 eine Anfrage einer ausländischen FIU zu einer Gesellschaft X mit Sitz in der Schweiz sowie zur transaktionellen Aktivität auf deren Schweizer Konten. Es bestand der Verdacht, dass inkriminierte Gelder verschiedener Verbrechen (u. a. Menschenhandel und Zwangsprostitution) über deren Schweizer Konten geflossen seien. Die ausländische FIU erhielt mehrere Verdachtsmeldungen mit demselben Modus Operandi: Ein Netzwerk von natürlichen und juristischen Personen, mit Sitz in einer Grenzregion zur Schweiz, erhielt Gelder von hauptsächlich natürlichen Personen aus dem Land Z. Diese Vermögenswerte wurden anschliessend auf die Schweizer Konten von X transferiert. Gemäss den Informationen der ausländischen FIU waren involvierte Gegenparteien unter anderem in Fälle von Menschenhandel und Zwangsprostitution verwickelt, wobei diese Verbrechen jeweils im Ausland begangen worden seien.

Ausgehend von den Informationsanfragen der ausländischen FIUs forderte die MROS gestützt auf Artikel 11*a* Absatz 2bis GwG die Informationen zu den betroffenen Schweizer Konten bei den entsprechenden Schweizer Finanzintermediären ein.

Menschhandel und Zwangsprostitution sind ohne weitere Indizien und nur basierend auf dem zugrunde liegenden Transaktionsverhalten oftmals schwer zu erkennen, da es sich bei den Cashflows und Überweisungen meist um niedrige Beträge handelt. Dank der Informationen der Schweizer Finanzintermediäre konnte die MROS eine ausführliche Transaktionsanalyse erstellen. Die Analyse ergab, dass eine gleiche Gruppe von natürlichen Personen mehrmals am Tag die gleiche Summe auf die besagten Schweizer Konten überwies. Später wurden weitere Einzahlungen von juristischen Personen – mit höheren Beträgen und in zeitlich grösseren Abständen – getätigt und lösten diejenigen der natürlichen Personen ab. Beim anschliessenden Weitertransfer der Vermögenswerte konnte unter anderem festgestellt werden, dass Zahlungen an Migrationsbehörden und an eine Reiseagentur getätigt wurden, welche in einer für Menschenhandel und Zwangsprostitution sensiblen Jurisdiktion ansässig ist. Diese Informationen wurden der ausländischen FIU mitgeteilt.

Der Finanzintermediär erstattete im Anschluss an die Anfrage der MROS gemäss Artikel 11*a* Absatz 2bis GwG und aufgrund eigener Abklärungen eine Verdachtsmeldung nach Artikel 9 Absatz 1 Buchstabe a GwG an die MROS. Alle Informationen wurden mit Verdacht auf Menschenhandel anschliessend an die zuständige kantonale Staatsanwaltschaft übermittelt.

Abbildung 15: Typologie 2 – Menschenhandel und Zwangsprostitution

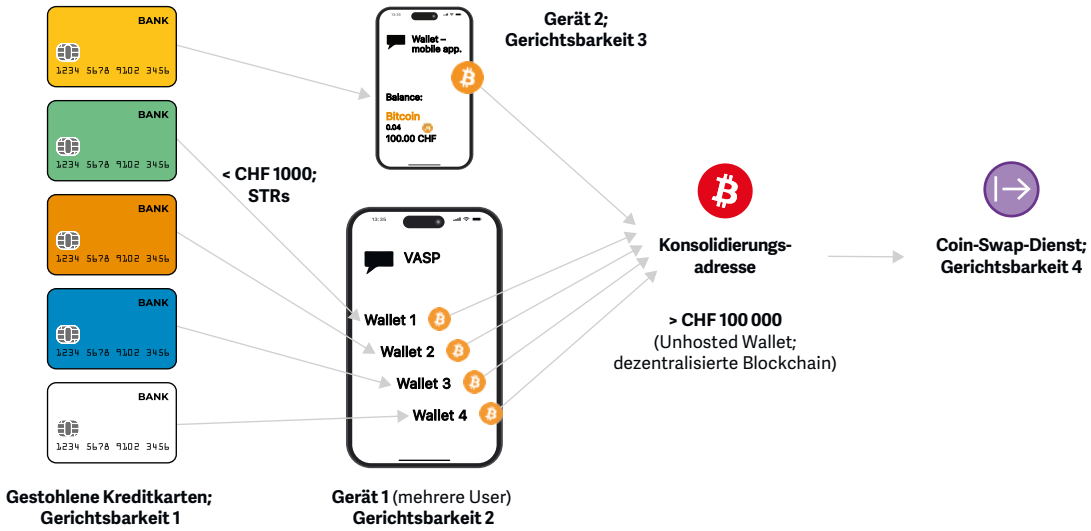


5.3 Typologie 3 – Ganzheitliche Analyseverfahren

Meldungen zu virtuellen Vermögenswerten und Kryptowährungen können angesichts der Komplexität sowie des dezentralen und grenzüberschreitenden Charakters der geldwäschereirelevanten Sachverhalte oft nur erfolgreich analysiert werden, wenn mehrere Fälle konsolidiert betrachtet werden. Das Gesamtkonstrukt lässt sich nur dank eines ganzheitlichen Analyseverfahrens (Cluster; vgl. Kap. 2.2) erkennen. Der vorliegende Fall zeigt eine Konstellation, in welcher analysierte Einzelfälle zu einem umfangreichen Gesamtfall aufbereitet wurden.
Auf diesen Fall stiess die MROS im Rahmen einer auf Blockchain-Intelligence-Techniken gestützten Analyse, deren Ziel die Identifikation von Serienkriminalität war. Bei den (konsolidiert) analysierten Fällen handelte es sich hauptsächlich um der MROS gemeldete Informationen, die bis anhin noch nicht Gegenstand einer Informationsübermittlung an eine Strafverfolgungsbehörde waren.

Im Rahmen der Analyse stellte sich heraus, dass mehrere Verdachtsmeldungen bezüglich Geldwäscherei (STRs) dieselbe Gruppe mutmasslicher Täter involvierte (Cluster). Die betreffenden STRs stammten von Schweizer Finanzintermediären mit VASP-Tätigkeit, welche auf den Kauf und Verkauf von Virtual Assets spezialisiert sind, die Vermögenswerte ihrer Kundinnen und Kunden aber nicht verwalten (non-custodial).
Die Verdachtsmeldungen betrafen Diebstähle von in einem westeuropäischen Land ausgestellten Kreditkarten, welche der MROS vom Finanzintermediär gemeldet wurden, der seinerseits Informationen von Dritten erhalten hatte. Demzufolge hätten mehrere Geschädigte jeweils bei der lokalen Polizei ihres Landes Anzeige erstattet, nachdem sie festgestellt hatten, dass über ihre Kreditkarte missbräuchlich Bitcoin-Käufe abgewickelt wurden. Die STRs bezogen sich alle auf unterschiedliche polizeiliche Ermittlungen im Ausland. Das Gesamttotal aller der MROS gemeldeten verdächtigen Transaktionen lag unter 1000 Schweizer Franken (für dieses Cluster).

Abbildung 16: Typologie 3 – Ganzheitliches Analyseverfahren (Cluster)



Für jede gestohlene Kreditkarte war beim Finanzintermediär ein neues Benutzerkonto eröffnet worden. Da die Transaktionen alle unter einem bestimmten Schwellenwert lagen, war keine Identifikation mittels KYC-Formular (Know Your Costumer) erforderlich. Der Finanzintermediär zeichnete jedoch andere Datenspuren (logs) auf (Art. 51*a* GwV-FINMA[72]).

Bei einem Bitcoin-Kauf via Kreditkarte tauscht der Finanzintermediär zum Beispiel Euro (Fiat-geld) gegen Bitcoin. Dabei überträgt er das Eigentum an den Bitcoins an eine Adresse, die seine Kundin oder sein Kunde auf der Blockchain (Distributed-Ledger-Technologie) kontrolliert, etwa eine Wallet in einer App auf dem Smartphone. Einzig die Kundin oder der Kunde ist im Besitz des geheimen Codes, der nötig ist, um über die Vermögenswerte zu verfügen – der Finanzintermediär hat keinerlei Möglichkeit, diese Vermögenswerte beispielsweise zu sperren.

Jede STR betraf demnach eine gestohlene Kreditkarte und eine Geschäftsbeziehung. Die MROS hat pro Transaktion Kenntnis von einer Kreditkarte und einer vom Vertragspartner kontrollierten Bitcoin-Adresse. Letztendlich konnte sie so eruieren, dass mindestens ein halbes Dutzend Geschäftsbeziehungen vermutlich von ein- und demselben Smartphone aus eröffnet worden waren (gleiches Handymodell, Geolokalisierung der IP-Adresse in derselben osteuropäischen Stadt). Eine weitere mit dem Ziel-Cluster assoziierte Geschäftsbeziehung wies andere Merkmale auf. Jedoch wurden bei all diesen Meldungen sämtliche Vermögenswerte, die mit den in den STRs gemeldeten Bitcoin-Adressen verknüpft waren, anschliessend unverzüglich und systematisch zur gleichen direkten Gegenpartei beziehungsweise Bitcoin-Adresse transferiert (1 hop). Bei der Analyse, die unter anderem mithilfe verschiedener Blockchain-Analysetools durchgeführt wurde, zeigte sich rasch, dass die betreffende Empfängeradresse offenbar eine Unhosted Wallet war, welche zur Konsolidierung von Geldern kriminellen Ursprungs genutzt wurde. Diese Schlussfolgerung stützt sich auf die Tatsache, dass die Vermögenswerte aus mehreren Hundert unterschiedlichen Quellen stammten und systematisch nach einer gewis-

[72] Verordnung der Eidgenössischen Finanzmarktaufsicht über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor (Geldwäschereiverordnung- FINMA, GwV-FINMA), SR **955.033.0**.

sen Zeit gebündelt zu einem mutmasslichen in einer Offshore-Jurisdiktion registrierten VASP überwiesen wurden. Letzterer schien von seinen Kundinnen und Kunden keine KYC-Identifikation zu verlangen. Wie die MROS zum Zeitpunkt der Nachforschungen feststellen konnte, diente die Adresse zur Konsolidierung von insgesamt über 100 000 Schweizer Franken.
Zu diesem Zeitpunkt wiesen die verwendeten Blockchain-Analysetools in ihren Datenbanken jedoch keine kryptografischen Adressen (Cluster) in Verbindung mit dem Schweizer Finanzintermediär auf, welcher die STRs absetzte. Es war daher nicht möglich, auf diesem Weg in Erfahrung zu bringen, ob weitere verdächtige Transaktionen von derselben Quelle ausgingen. Erst eine vertiefte Blockchain-Analyse[73], gestützt auf eine Informationsanfrage (Art. 11*a* GwG) an den Finanzintermediär, ermöglichte die Identifikation anderer potenzieller Nutzerinnen und Nutzer, die Vermögenswerte an die sogenannte Konsolidierungsadresse überwiesen hatten. Damit erschien plausibel, dass noch weitere Kunden des Finanzintermediärs in die mutmasslichen kriminellen Machenschaften involviert sein oder dass einer oder mehrere mutmassliche Täter weitere Konten ohne Angabe ihrer Identität beim Finanzintermediär erstellt haben könnten. Auf der Grundlage der angeforderten Stichprobe liess sich ferner erkennen, dass die Geschädigten offenbar in unterschiedlichen Ländern zu finden waren.
Im vorliegenden Fall – einer ziemlich typischen Konstellation – stellt die MROS fest, dass die Geschädigten im Ausland wohnen, die Täterschaft in Gruppen zu agieren scheint, und zwar von anderen, ebenfalls ausländischen Jurisdiktionen aus, und die verwendeten Modelle den Betrug dank Internet vereinfachen oder im grösseren Massstab ermöglichen (Cyber-enabled Fraud). Die gestohlenen Vermögenswerte werden anschliessend direkt bei Schweizer Finanzintermediären in Kryptowährungen umgewandelt, im vorliegenden Fall unterhalb des Schwellenwerts, ab dem eine KYC-Identifikation erforderlich wäre. Die Kryptowährungen kriminellen Ursprungs stehen der Täterschaft sodann in Non-Custodial Wallets unmittelbar zur Verfügung. So können die mutmasslichen Täter oder auch professionelle Geldwäscher die Bitcoins direkt zu risikobehafteten Diensten in anderen Jurisdiktionen transferieren, um den kriminell erlangten Profit umzuwandeln. Im vorliegenden Fall hat die MROS die ihr bekannten Informationen über den FIU-Kanal weitergeleitet.

[73] Identifikation von Transaktionsmustern.

6. Aus der Praxis der Meldestelle

6.1 Auslegung von Artikel 11*a* GwG – Herausgabe von Informationen durch die Finanzintermediäre

Artikel 11*a* GwG erlaubt der MROS bei Finanzintermediären Informationen einzuholen, wenn sich aufgrund der Analyse von Meldungen nach Artikel 9 GwG (Meldepflicht) bzw. Artikel 305ter Absatz 2 StGB (Melderecht) oder von Informationen ausländischer Meldestellen ergibt, dass die entsprechenden Finanzintermediäre mit Transaktionen oder Geschäftsbeziehungen am Sachverhalt beteiligt waren.
Die Möglichkeit zur Informationsbeschaffung bei Finanzintermediären nach Artikel 11*a* GwG ist ein wichtiges Instrument zur wirksamen Bekämpfung der Geldwäscherei, welche regelmässig unter Verwendung komplexer Schemen und über nationale Jurisdiktionen hinaus betrieben wird. Sie ermöglicht einerseits, Verdachtsmeldungen von Finanzintermediären in einen grösseren Zusammenhang zu stellen, und andererseits, ausländische Meldestellen mit den zur Bekämpfung der Geldwäscherei notwendigen Informationen zu beliefern.
Erhält die MROS Auskunftsbegehren von ausländischen FIUs zu Geschäftsbeziehungen in der Schweiz, prüft sie vorab, ob ein Bezug zur Schweiz besteht, und stellt damit sicher, dass keiner «Fishing Expedition» ausländischer Behörden stattgegeben wird (vgl. Art. 31 GwG). Werden der Kunde sowie der kontoführende Schweizer Finanzintermediär von der ausländischen FIU namentlich genannt, geht die MROS praxisgemäss von einem ausreichenden Bezug zur Schweiz aus, auch wenn keine genaueren Informationen zur Geschäftsbeziehung (z. B. Kontonummern) vorliegen. Vermutet die ausländische FIU hingegen lediglich das Vorhandensein einer Geschäftsbeziehung in der Schweiz, ohne einen konkreten Finanzintermediär anzugeben, geht die MROS auf die Anfrage nicht ein.
Holt die MROS Informationen zu bestimmten Kontobeziehungen ein, erkundigt sie sich regelmässig nach weiteren Konten innerhalb derselben Geschäftsbeziehung: Vertragspartner, wirtschaftlich Berechtigte oder verbundene Personen oder Gesellschaften können eine zentrale Rolle spielen. In manchen Fällen ist der MROS sodann lediglich bekannt, dass eine Kundenbeziehung zwischen einer Person oder einer Gesellschaft und einer Bank besteht, ohne dass sie über Angaben zu Kontonummern oder Transaktionen verfügt. In diesen Fällen verlangt die MROS von den Finanzintermediären Informationen zur besagten Geschäftsbeziehung unter Angabe der entsprechenden Person oder Gesellschaft. Eine rasche und vollständige Informationsherausgabe seitens der Finanzintermediäre ist dabei unabdingbar für eine wirkungsvolle Bekämpfung der nationalen und internationalen Geldwäscherei.
Die Finanzintermediäre sind verpflichtet, der MROS alle relevanten Informationen, über welche sie verfügen, zur Verfügung zu stellen. Das Gesetz räumt den Finanzintermediären keinen Beurteilungsspielraum betreffend die Verhältnismässigkeit der Anfrage oder eine Möglichkeit

zur Anfechtung oder Siegelung ein. Die verlangten Informationen müssen sie innerhalb der von der MROS gesetzten Frist[74] einreichen.
Kommt ein Finanzintermediär den Aufforderungen der MROS nicht nach, kann dieses Verhalten eine Aufsichtsrechtverletzung darstellen. Gemäss Artikel 10 Absatz 2 MGwV kann die MROS die zuständigen Aufsichtsbehörden, Aufsichts- oder Selbstregulierungsorganisation nach Artikel 29 Absatz 1 oder Artikel 29*b* GwG über allfällige aufsichtsrechtliche Verstösse von Finanzintermediären informieren – was sie auch regelmässig macht. Es liegt in ihrer Verantwortung, solchen potenziellen Aufsichtsrechtsverstössen nachzugehen und allenfalls entsprechende Massnahmen zu ergreifen.

6.2 Interpretation von Artikel 29*a* GwG – Zustellung von Urteilen und Verfügungen durch die Strafbehörden

Artikel 29*a* Absatz 1 GwG verpflichtet sämtliche Strafbehörden[75], der Meldestelle Urteile und Einstellungsverfügungen inklusive deren Begründung zu Verfahren im Zusammenhang mit Artikel 260ter, Artikel 260^{quinquies} Absatz 1, Artikel 305bis und Artikel 305ter Absatz 1 StGB zuzustellen. Die Urteile und Einstellungsverfügungen gestatten es der Meldestelle, sich einen Überblick über die Entwicklungen im Zusammenhang mit Geldwäscherei, deren Vortaten, der organisierten Kriminalität und der Terrorismusfinanzierung zu verschaffen, und unterstützen sie darin, die Finanzintermediäre für diese Problematik zu sensibilisieren. Zusätzlich haben die Strafbehörden der Meldestelle basierend auf Artikel 29*a* Absatz 2 GwG sämtliche Verfügungen, die sie aufgrund einer Anzeige der Meldestelle erlassen haben, zuzustellen. Die Liste der zu meldenden Urteile und Verfügungen umfasst insbesondere:

- Eröffnung einer Strafuntersuchung (Art. 309 Abs. 3 StPO);
- Nichtanhandnahmeverfügungen (Art. 310 Abs. 1 StPO);
- Verfügungen betreffend die Ausdehnung einer Strafuntersuchung (Art. 311 Abs. 2 StPO);
- Sistierungen (Art. 314 StPO);
- Wiederanhandnahme (Art. 315 StPO);
- Strafbefehle (Art. 353 StPO);
- Einstellungsverfügungen (Art. 320 StPO);
- Wiederaufnahme (Art. 323 StPO);
- gerichtliche Urteile (z. B. gemäss Art. 351 StPO oder gemäss Art. 408 StPO).

Diese Mitteilungen informieren die Meldestelle nicht nur über den Fortschritt der Verfahren, sondern ermöglichen es, Informationen aus allfälligen weiteren Meldungen zum gleichen Sachverhalt rasch an die zuständige Behörde zu übermitteln und die relevanten Statistiken zu führen. Darüber hinaus erhält die Meldestelle Rückschlüsse auf ihre Arbeit, insbesondere mit Blick auf ihre Übermittlungspraxis an die Strafverfolgungsbehörden.
Die in Artikel 29*a* GwG erwähnte Pflicht umfasst auch die unaufgeforderte Übermittlung von Informationen im Sinne von Artikel 67*a* des Rechtshilfegesetzes[76]. Diese Informationen haben zum Zweck, ein gezieltes Rechtshilfeersuchen an die Schweiz auszulösen.
Die Eidgenössische Finanzkontrolle (EFK) hat in ihrem Bericht «Prüfung der Aufgabenerfüllung der Meldestelle für Geldwäscherei» vom 20. Dezember 2021[77] bemängelt, dass die MROS über unvollständige Daten zu den Entscheiden der Strafbehörden im Bereich der Geldwäscherei verfüge, insbesondere wenn diese mit einer Verdachtsmeldung verbunden waren (nimmt Bezug auf Art. 29*a* Abs. 1 und 2 GwG). Die EFK weist in ihrem Bericht darauf hin, dass der Rücklauf der kantonalen Strafverfolgungsbehörden lücken-

[74] Art. 11*a* Abs. 3 GwG.

[75] Der Begriff «Strafbehörden» umfasst sowohl die kantonalen Strafverfolgungsbehörden als auch die Bundesanwaltschaft sowie sämtliche urteilenden Gerichte aller Instanzen (Botschaft zur Umsetzung der revidierten Empfehlungen der Groupe d'action financière [GAFI], BBl **2007** 6269, 6302).

[76] Bundesgesetz über internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, IRSG), SR **351.1**.

[77] *Bericht der EFK zur Prüfung der Aufgabenerfüllung der Meldestelle für Geldwäscherei vom 20. Dezember 2021, S. 33 (publiziert am 28. März 2022)*.

haft respektive unbefriedigend ist: «*MROS fehlt der Überblick über die gesamte Prozesskette und den Lebenszyklus ihrer Verdachtsmeldungen. Dies wäre zur Beurteilung der Wirksamkeit und der Verbesserung der eigenen Arbeit aber entscheidend. MROS moniert seit 20 Jahren, dass die BA, die kantonalen Staatsanwaltschaften und die urteilenden Gerichte ihrer gesetzlichen Pflicht nach Art. 29a GwG nicht nachkommen. Analog zum seit dem Jahr 2020 mit der BA praktizierten, systematischen Meldungsabgleich, sollten sich auch die kantonalen Staatsanwaltschaften und die urteilenden Gerichte an die gesetzliche Vorgabe halten.*»
Die Meldestelle hat die Kritik der EFK zum Anlass genommen, die Strafbehörden im Berichtsjahr an ihre diesbezügliche Pflicht zu erinnern. Die im Kapitel 4.8 ausgewiesene Statistik zeigt, dass nach wie vor Verbesserungspotenzial besteht. Damit die Meldestelle die Informationen basierend auf Artikel 29*a* GwG effektiv auswerten und die von ihr geforderten Mehrwerte in der Kriminalitätsbekämpfung und Prävention schaffen kann, bedarf es eines möglichst vollständigen Rücklaufs.

7. Internationale Zusammenarbeit in der Bekämpfung der Geldwäscherei

7.1 Egmont-Gruppe

Die MROS ist seit 1998 Mitglied der Egmont-Gruppe. Das internationale Netzwerk besteht aus 173 operativ unabhängig tätigen FIUs, welche darauf spezialisiert sind, Geldwäscherei, deren Vortaten sowie Terrorismusfinanzierung aufzudecken und zu bekämpfen. Die Egmont-Gruppe orientiert sich an den Standards der FATF, des führenden internationalen Gremiums zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung (vgl. Kap. 7.2). Die Egmont-Gruppe ermöglicht auf operativer Ebene den von den FATF-Grundsätzen konzipierten Informationsaustausch zwischen den FIUs der verschiedenen Mitgliedsländer. Eine Mitgliedschaft in der Egmont-Gruppe ist seit der Überarbeitung der FATF-Empfehlungen von 2012 Voraussetzung für ein adäquates Geldwäscherei- und Terrorismusbekämpfungssystem.

Die Ziele der Egmont-Gruppe sind insbesondere:
- jene Voraussetzungen zu schaffen, die für einen internationalen, systematischen Informationsaustausch erforderlich sind;
- FIUs dabei zu unterstützen, ihre Effizienz zu steigern, indem Ausbildungsstrategien ausgebaut und Mitarbeiter-Austauschprogramme gefördert werden;
- den internationalen Informationsaustausch zwischen FIUs unter sicheren Bedingungen zu ermöglichen;
- die operationelle Unabhängigkeit von FIUs sicherzustellen;
- die Errichtung zentralisierter Meldestellen zu unterstützen.

Die Leiterinnen und Leiter der FIUs (Head of FIUs) konstituieren das Führungsgremium der Egmont-Gruppe. Einmal jährlich und an wechselnden Austragungsorten findet eine Plenarversammlung (Plenary) statt: Wichtige Entscheide werden gemeinsam besprochen und getroffen. Unterstützt werden die Leiterinnen und Leiter der FIUs durch das Egmont-Committee, ein Konsultations- und Koordinationsgremium, sowie das Egmont-Sekretariat mit Sitz in Kanada.

Die Egmont-Gruppe verfügt über vier Arbeitsgruppen:
- **«Information Exchange Working Group» (IEWG):** Diese Arbeitsgruppe hat die Aufgabe, operative und strategische Synergien der einzelnen FIUs zu erkennen und sicherzustellen, dass diese entsprechend genutzt werden. Des Weiteren sorgt sie dafür, die Zusammenarbeit und den Informationsaustausch stetig zu verbessern.
- **«Membership, Support and Compliance Working Group» (MSCWG):** Die Arbeitsgruppe stellt sicher, dass die Egmont-Prinzipien von den FIUs eingehalten werden – bei neuen und bestehenden Mitgliedern der Egmont-Gruppe.
- **«Policy and Procedures Working Group» (PPWG):** Die Arbeitsgruppe beschäftigt sich mit strategischen Fragen, einschliesslich des effektiven Informationsaustausches zwischen den FIUs und der Einhaltung internationaler Standards (FATF).
- **«Technical Assistance and Training Working Group» (TATWG):** Die Arbeitsgruppe verantwortet die Identifizierung, Entwicklung und Bereitstellung technischer Hilfestellungen

und Schulungsmöglichkeiten für alle FIUs – bestehende Mitglieder und FIUs, die sich im Aufnahmeprozess befinden – und sämtliche Beobachterorganisationen und andere internationale Partner der Egmont-Gruppe.

Die vier Arbeitsgruppen werden jeweils von einer oder einem Vorsitzenden und einer oder einem oder auch mehreren stellvertretenden Vorsitzenden aus verschiedenen FIUs geleitet. Es finden regelmässig Sitzungen (Plenary, Arbeitsgruppen und Regionalmeetings) statt, an denen die MROS teilnimmt. Bei den Regionalmeetings werden die FIUs nach geografischen Aspekten einer Gruppe zugeordnet. Die europäischen FIUs sind in zwei Gruppen aufgeteilt: «Europe I» umfasst die FIUs der EU-Mitgliedsländer, alle anderen FIUs, inklusive der MROS, sind der «Europe-II-Regionalgruppe[78]» zugeteilt. Regionale Gruppen ermöglichen eine Auseinandersetzung mit regionalspezifischen Herausforderungen und Fragestellungen.

Treffen mit Egmont-Mitgliedern
Vom 30. Januar bis 3. Februar 2023 fand ein Arbeits- und Regionalgruppen-Meeting in Dakar, Senegal, statt. 287 Delegierte und 12 Observer und internationale Partner nahmen teil. Insgesamt wurden 15 Sitzungen abgehalten, um die Fähigkeiten der Mitglieder der Egmont-Gruppe zu stärken, den Informationsaustausch zwischen ihnen zu verbessern und auf die Erfüllung der Entwicklungsmission, die Zusammenarbeit und den Austausch von Fachwissen hinzuarbeiten. Zwischen dem 3. und 7. Juli 2023 fand die Egmont-Plenarversammlung (Plenary) in Abu Dhabi, Vereinigte Arabische Emirate, statt. Teilgenommen haben 533 Delegierte, 12 Observer und ein internationaler Partner. Als grosser Meilenstein wurde die Umstellung auf eine neue IT-Infrastruktur, das Egmont Secure Web, beschlossen. Die IT-Infrastruktur war ein wichtiger Fokus der Plenarversammlung: Die stark steigenden Verdachtsmeldungen und Anfragen aus dem Ausland können nicht mehr nur mit Manpower bewältigt werden. Die FIUs benötigen neue IT-Lösungen, um ihre Effizienz zu steigern.

7.2 GAFI / FATF

Die Financial Action Task Force (FATF), auch bekannt unter ihrem französischen Namen Groupe d'action financière (GAFI), ist eine zwischenstaatliche Organisation; sie wurde 1989 anlässlich eines Ministertreffens in Paris von der G7 gegründet. Die FATF ist das international führende Gremium zur Bekämpfung der Geldwäscherei, der Terrorismus- und der Proliferationsfinanzierung. Mitglieder sind die jeweiligen Länder, nicht einzelne Ämter. Die FATF untersucht, wie Gelder gewaschen werden und Terrorismus finanziert wird. Sie fördert globale Standards[79] zur Minderung der Risiken und bewertet, ob die Länder wirksame Massnahmen ergreifen.
Im Jahr 2023 fanden drei Plenarversammlungen unter dem Vorsitz von Singapur im Headquarter der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) in Paris statt.[80]
Die FATF veröffentlichte im Jahr 2023 einige Publikationen, darunter Bekanntmachungen zu «Missbrauch von Staatsbürgerschaft und Wohnsitz durch Investitionsprogramme»[81], «Bewährte Praktiken zur Bekämpfung des Missbrauchs von gemeinnützigen Organisationen»[82], «Illegale Finanzströme durch Cyber-Betrug»[83] und «Crowdfunding zur Terrorismusfinanzierung»[84]. Insbesondere Letztere gewann durch die terroristischen Angriffe der Hamas auf Israel am 7. Oktober 2023 an Aktualität. Die MROS versandte in

[78] Weitere Mitglieder der Egmont-II-Regionalgruppe sind beispielsweise das Financial Crimes Investigation Board (MASAK), Türkei, der State Financial Monitoring Service of Ukraine (SFMS), Ukraine, sowie die UK Financial Intelligence Unit (UKFIU), Vereinigtes Königreich.

[79] *The FATF-Recommendations 2012 – Updated November 2023*.

[80] Bemerkenswert ist dabei der Entscheid über die Aussetzung der Mitgliedschaft Russlands anlässlich des ersten Treffens im Februar 2023: *FATF Statement on the Russian Federation (fatf-gafi.org)*

[81] *Misuse of Citizenship and Residency by Investment Programmes (fatf-gafi.org)*.

[82] *Best Practices on Combating the Abuse of Non-Profit Organisations (fatf-gafi.org)*.

[83] *Illicit Financial Flows from Cyber-enabled Fraud (fatf-gafi.org)*.

[84] *Crowdfunding for Terrorism Financing (fatf-gafi.org)*.

diesem Zusammenhang am 3. November 2023 ein Sensibilisierungsschreiben (Alert) und Typologien an die Schweizer Finanzintermediäre; am 5. Dezember 2023 ergänzte sie den Alert mit einem Addendum.[85]

Länderevaluation

Die von der FATF festgelegten Standards der Massnahmen zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung richten sich an die Mitgliedstaaten, welche verpflichtet sind, diese umzusetzen. Die FATF bewertet periodisch den aktuellen Stand der Umsetzung in den einzelnen Mitgliedstaaten und publiziert die Ergebnisse ihrer Evaluationen in einem Bericht. Die FATF-Empfehlungen sind rechtlich nicht bindend, für die Schweiz jedoch von grosser Bedeutung. Mitgliedstaaten, die erhebliche Defizite zu den FATF-Empfehlungen aufweisen, werden öffentlich benannt und auf eine Länderrisikoliste (graue und schwarze Liste) gesetzt, was für die betroffenen Länder in der Regel erhebliche Konsequenzen hat. Transaktionen von oder in das verzeichnete Land werden behördlich geprüft und sind somit schwerfälliger und teurer. Ausländische Investoren halten sich zudem entsprechend zurück, da das Risiko zu gross scheint. Diesfalls leidet die Reputation des ganzen Finanzplatzes eines Landes.

Die Schweiz wurde letztmals 2016 während der vierten Evaluationsrunde einer Länderprüfung unterzogen. Das Resultat fiel positiv aus. Die FATF stellte aber gewisse Mängel im Abwehrdispositiv fest, weshalb die Schweiz in den sogenannten «Enhanced Follow-up-Process» aufgenommen wurde. Um den FATF-Empfehlungen gerecht zu werden, setzte die Schweiz konsequenterweise verschiedene Massnahmen zur Verbesserung der technischen Konformität um, insbesondere mit der Revision des Geldwäschereigesetzes vom Juli 2021.[86] Die FATF hat diese Fortschritte inzwischen anerkannt und die Schweiz im Oktober 2023 aus dem «Enhanced Follow-up-Prozess» entlassen.

Die nächste Länderprüfung steht voraussichtlich 2027/2028 an. Die FATF wird das Dispositiv der Schweiz neu und umfassend beurteilen, mittels einer neuen Evaluationsmethodik (im Vergleich zur Evaluation 2016). Neben der technischen Einhaltung der FATF-Standards wird neu ein weiterer Fokus auf die Wirksamkeit des Abwehrdispositivs gelegt. In die Prüfung miteinbezogen werden dabei nicht nur die Behörden, sondern der gesamte Finanzplatz Schweiz, inklusive des Privatsektors. Die FATF prüft, ob ein Land seine Risiken kennt und Massnahmen zu deren Begrenzung und Unterbindung eingeleitet hat.

Die neue Methodik umfasst dabei zwei miteinander verknüpfte Komponenten:

- Die **technische Bewertung** der Einhaltung der Vorschriften befasst sich mit den spezifischen Anforderungen der einzelnen FATF-Empfehlungen. Es geht dabei vor allem um den rechtlichen und den institutionellen Rahmen des Landes sowie um die Befugnisse und Verfahren der zuständigen Behörden. Dies sind die grundlegenden Bausteine eines effektiven Systems zur Bekämpfung der Geldwäscherei sowie der Terrorismus- und der Proliferationsfinanzierung.[87]
- Die **Wirksamkeit** beurteilt, inwieweit ein Land für ein robustes System zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung sorgt. Ausserdem wird analysiert, inwieweit der rechtliche und institutionelle Rahmen eines Landes die erwarteten Ergebnisse beeinflusst.[88]

Die Länderprüfung dauert rund 18 Monate und lässt sich für die Schweiz in drei Phasen einteilen: die Vorbereitung des Vor-Ort-Besuchs (ab 2024), der Vor-Ort-Besuch (ca. Juli 2027) sowie die Vorbereitung auf die FATF-Plenarversammlung, in welcher der Bericht zur Schweiz verabschiedet wird.

---

[85] Der MROS-Alert setzte sich aus den Publikationen der FATF sowie Informationen ausländischer FIUs und MROS-eigenen Erkenntnissen zusammen.

[86] Insbesondere Einführung neuer Abklärungskompetenz für die MROS nach Art. 11*a* Abs. 2bis GwG.

[87] Der Grad der Einhaltung der einzelnen Empfehlungen wird mit einer der folgenden Bewertungen angegeben: eingehalten, weitgehend eingehalten, teilweise eingehalten oder nicht eingehalten.

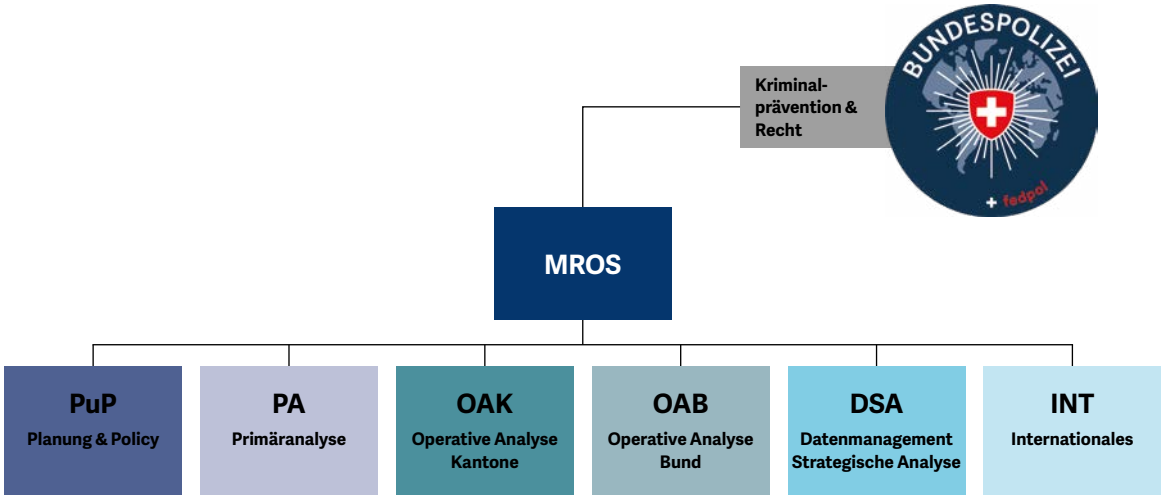
[88] Die Effektivität wird wie folgt ausgewiesen: hohe Effektivität, erhebliche Effektivität, mässige Effektivität und geringe Effektivität.

8. Organisation der MROS

Die MROS ist organisatorisch dem Direktionsbereich Kriminalprävention & Recht von fedpol angegliedert. In ihrer operativen Kerntätigkeit agiert die MROS vollständig unabhängig und setzt damit die internationalen Anforderungen um.

Im Jahr 2020 wurde die MROS neu organisiert. Seitdem ist sie neu in sechs Bereiche aufgeteilt (vgl. Organigramm; Abbildung 17). Im Jahr 2023 beschäftigte die MROS durchschnittlich 59 Mitarbeitende (50,3 Vollzeitstellen).

Abbildung 17: Organisation MROS



Planung und Policy (PuP)
Der Bereich PuP fungiert als klassische Querschnittsdisziplin. Im Fokus stehen dabei die juristischen Fragestellungen im Bereich Geldwäscherei und Terrorismusfinanzierung, die Bearbeitung und Begleitung der politischen Projekte und Publikationen (z. B. Jahresberichte, Gesetzesrevisionen, Rechtsgutachten zu MROS-spezifischen Fachthemen) sowie die Unterstützung der operativen Bereiche der MROS. PuP pflegt den regelmässigen Austausch mit internen und externen Stakeholdern und kümmert sich um die administrativen Belange der MROS.

Primäranalyse (PA)
Der Bereich PA ist für die Erfassung und Aufbereitung aller eingehenden Meldungen in formeller, technischer und inhaltlicher Hinsicht verantwortlich. Dies beinhaltet ebenfalls manuelle Korrekturen bei mangelhafter Datenqualität. Dar-

über hinaus übernimmt sie die Triage und übergibt die Fälle anhand einer Gesamtbewertung an einen der nachgelagerten Bereiche. Ebenfalls in ihre Zuständigkeit fällt die nationale Amtshilfe nach Artikel 29 GwG.

Operative Analyse Kantone (OAK)
Der Bereich OAK analysiert eingehende Verdachtsmeldungen, welche grossmehrheitlich in die Zuständigkeit der kantonalen Strafverfolgungsbehörden fallen und vom Bereich PA zugewiesen wurden. Bei begründetem Verdacht werden die aggregierten Informationen an die jeweils zuständige Strafverfolgungsbehörde übermittelt (in der Regel kantonale Strafverfolgungsbehörden). OAK teilt die Informationen bei Bedarf auch mit anderen nationalen Behörden sowie FIUs anderer Länder.

Operative Analyse Bund (OAB)
Der Bereich OAB analysiert eingehende Verdachtsmeldungen, welche a priori in die Zuständigkeit der BA fallen und vom Bereich PA zugewiesen wurden. Bei begründetem Verdacht werden die aggregierten Informationen an die jeweils zuständige Strafverfolgungsbehörde übermittelt (in der Regel BA bzw. gegebenenfalls auch kantonale Strafverfolgungsbehörden). OAB teilt die Informationen bei Bedarf auch mit anderen nationalen Behörden sowie FIUs im Ausland.

Datenmanagement und strategische Analyse (DSA)
Der Bereich DSA verantwortet die Betriebssicherheit und die Entwicklung des Informationssystems der MROS (goAML). Dabei bietet DSA den Finanzintermediären unter anderem technischen Support, insbesondere bei der Programmierung ihrer Schnittstellen. DSA ist zudem für die Entwicklung der technischen Möglichkeiten der Datenverarbeitung der Verdachtsmeldungen zuständig. Der Bereich führt die strategischen Analysen der MROS aus und wertet unterschiedlichste Daten im Zusammenhang mit der Bekämpfung von Geldwäscherei, deren Vortaten und Terrorismusfinanzierung aus, um Risiken, Tendenzen und Methoden der Geldwäscherei zu identifizieren.

Internationales (INT)
Der Bereich INT kümmert sich um den gesamten (Informations-)Austausch mit ausländischen FIUs sowie um die Mitgliedschaft und die Teilnahme in internationalen Gremien (u. a. Egmont-Gruppe, GAFI/FATF, United Nations Convention against Corruption und Europol Financial Intelligence Public Private Partnership).