Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Meldestelle für Geldwäscherei (MROS)

Jahresbericht 2020

Mai 2021

Meldestelle für Geldwäscherei (MROS)

Jahresbericht 2020

Mai 2021

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

Telefon: (+41) 058 463 40 40
E-Mail: mros.info@fedpol.admin.ch

Internet: http://www.fedpol.admin.ch

Inhaltsverzeichnis

1. Vorwort

Das Jahr 2020 war, wie die Jahre davor, sehr herausfordernd für die Meldestelle für Geldwäscherei (MROS). Dank der Einführung des elektronischen Meldesystems goAML, konnte die MROS zwar die ausserordentliche Lage bewältigen, die durch die COVID-Pandemie entstanden ist. Die Pandemie hat Kriminellen aber auch diverse Möglichkeiten geboten, um sich unrechtmässig zu bereichern. Dadurch verschärfte sich auch das Risiko der Geldwäscherei. Dieses Risiko kommt durch eine erneute Zunahme der Anzahl Verdachtsmeldungen an die MROS zum Ausdruck. Die im Jahr 2020 eingegangenen 5 334 Meldungen betreffen über 9 000 Geschäftsbeziehungen. Diese Zahl ist rund 25 Prozent höher als 2019. Die Zunahme der Anzahl Verdachtsmeldungen an die MROS in 2020 ist vergleichbar mit dem Anstieg in den Jahren 2018 und 2019. Im Verlaufe des letzten Jahres hat die MROS ausserdem mehr als 6 000 Geschäftsbeziehungen bearbeitet, welche zwischen 2016 und 2019 gemeldet wurden und deren Analyse Ende 2019 noch nicht abgeschlossen war.

Über 1 000 im Jahr 2020 erfolgte Meldungen betreffen einen Verdacht auf Betrug im Zusammenhang mit Krediten schweizerischer Finanzinstitute mit Bundesbürgschaft. Diese Fälle führten zu mehr als 800 Anzeigen an die Strafverfolgungsbehörden vonseiten der MROS. Es wurden daraufhin Hunderte von Strafuntersuchungen eröffnet. Diese Tatsache spiegelt sich auch in den Statistiken wider. Bei über der Hälfte (58 %) der Verdachtsmeldungen, die die MROS im Jahr 2020 erhalten hat, wird Betrug als Vortat angegeben. Dieser Anstieg um 25 Prozent gegenüber 2019 ist bemerkenswert. Des Weiteren haben die Finanzintermediäre im Berichtsjahr zum ersten Mal das Transaktionsmonitoring als häufigstes verdachtsbegründendes Element angegeben. Das System goAML hat sich bei den Finanzintermediären durchgesetzt. Im Dezember 2020 wurden der MROS beinahe 90 Prozent der Verdachtsmeldungen auf elektronischem Weg übermittelt. Dieses ermutigende Resultat ist das Ergebnis der intensiven Bemühungen, die die Finanzintermediäre unternommen haben, um sich an dieses neue System anzupassen. Die MROS hat ihrerseits viel Personal eingesetzt, um die Finanzintermediäre und ihre Partnerbehörden während der Übergangsphase zu unterstützen und zu begleiten. Allerdings muss die Meldestelle die übermittelten Daten manchmal noch korrigieren und systematisch bereinigen, um diese analysieren zu können. Es ist zwingend, dass sich das Personal, welches 2020 für diese Arbeiten eingesetzt wurde, zukünftig der Analysetätigkeit widmen kann. Aus diesem Grund sind Anpassungen und Verbesserungen des Systems notwendig, damit das Potenzial der elektronischen Übermittlung von Verdachtsmeldung voll ausgeschöpft werden kann.

Zum ersten Mal präsentiert die MROS in ihrem Jahresbericht thematische Fallbeispiele, um die Finanzintermediäre auf schwer erkennbare Risiken von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung aufmerksam zu machen. Wir haben spezifische Typologien ausgewählt, die Risiken von Terrorismusfinanzierung, Beteiligung an einer kriminellen Organisation, Menschenhandel und Geldwäscherei

mittels Kryptowährungen oder Online-Identifizierung hervorheben. Die Weiterentwicklung der strategischen Analyse und die Sensibilisierung der Finanzintermediäre sind zentrale Elemente der neuen Strategie der Meldestelle. Die elektronische Bearbeitung der Verdachtsmeldungen bietet hierfür neue Möglichkeiten, welche die MROS in den kommenden Jahren noch stärker nutzen wird.

Eine weitere Neuigkeit besteht darin, dass die MROS dieses Jahr Statistiken zum Informationsaustausch mit anderen nationalen Behörden präsentiert. Dieser Austausch hat eine neue Bedeutung erhalten, einerseits aufgrund des Inhalts und andererseits aufgrund des Aufwands, der bei der MROS deswegen entsteht. Der Austausch mit ausländischen Meldestellen hat im Berichtsjahr ebenfalls einmal mehr zugenommen. Im September 2020 hat das Parlament eine Änderung des Geldwäschereigesetzes vom 10. Oktober 1997 (GwG)[1] angenommen, welche der MROS zusätzliche Kompetenzen im Rahmen dieses internationalen Informationsaustauschs einräumt. In Zukunft kann die Meldestelle, unter den Bedingungen des neuen Art. 11a Abs. 2bis GwG, ausschliesslich aufgrund von Informationen einer anderen Meldestelle, bei den Finanzintermediären Auskunft über Geschäftsbeziehungen einfordern. Diese neue Kompetenz wird das Schweizer Dispositiv zur Bekämpfung der Geldwäscherei stärken.

Diese Resultate hätte die MROS ohne das Engagement der Mitarbeitenden nicht erreichen können. Ihnen gebührt unsere Anerkennung und unser Dank.

Bern, im Mai 2021

Eidgenössisches Justiz-
und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Meldestelle für Geldwäscherei MROS

[1] SR **955.0**

2. Neue Organisation und Strategie der MROS 2020–2021

Für die MROS stand das Jahr 2020 im Zeichen von Veränderungen und Neuerungen. Am 1. Januar 2020 wurde das Informationssystem der MROS, goAML, in Betrieb genommen. Gleichzeitig trat eine revidierte Fassung der Verordnung vom 25. August 2004 über die Meldestelle für Geldwäscherei (MGwV)[2] in Kraft. Am selben Tag verabschiedete die MROS eine neue Strategie; sie ergänzt die Strategie des Eidgenössischen Justiz- und Polizeidepartements (EJPD) zur Kriminalitätsbekämpfung 2020–2023.[3]
Diese Veränderungen schlugen sich in einer internen Reorganisation der MROS nieder, um den Einsatz von goAML und die Umsetzung der neuen Strategie zu gewährleisten (siehe Kapitel 2.3). Diese voneinander abhängigen Entwicklungen entsprangen dem Bestreben, aus der MROS eine moderne, proaktive Behörde zu machen, welche in der Lage ist, den Herausforderungen zu begegnen, die sich aus der ständigen Entwicklung in Sachen Geldwäschereitechniken und deren Vortaten, organisierte Kriminalität und Terrorismusfinanzierung ergeben.

2.1 Ein Jahrzehnt der Entwicklungen im Kampf gegen Geldwäscherei, organisierte Kriminalität und Terrorismusfinanzierung

In den Jahren von 2010 bis 2019 hat sich die Zahl der von Schweizer Finanzintermediären der MROS gemeldeten Geschäftsbeziehungen versiebenfacht. Der Informationsaustausch mit ausländischen Financial Intelligence Units (FIUs) nahm zu, und die MROS wurde von nationalen Behörden im Rahmen der Amtshilfe vermehrt angefragt. Diese Trends setzten sich im Berichtsjahr fort (siehe Kapitel 4), und nichts deutet auf eine Kehrtwende hin. Im Jahr 2013 erhielt die MROS zusätzliche Befugnisse, insbesondere was den Informationsaustausch mit ausländischen Meldestellen und mit Finanzintermediären anbelangt.[4] Diese Befugnisse werden ab dem 1. Juli dieses Jahres weiter ausgeweitet (siehe Kapitel 6.2).
Viele FIUs sehen sich in unterschiedlichem Tempo und in unterschiedlichem Ausmass mit ähnlichen Entwicklungen konfrontiert. Die Menge an Finanzinformationen, die sie erhalten, nimmt zu; die Geldwäschereitechniken haben sich weiterentwickelt– vor allem was die Nutzung neuer Technologien betrifft (siehe Kapitel 5.5); die Rolle der FIUs bei der Bekämpfung der Geldwäscherei wird immer wichtiger, und ihre Kompetenzen wachsen, insbesondere im Hinblick auf den nationalen und internationalen Informationsaustausch. Grund für diese Entwicklungen ist das allgemein verbesserte Dispositiv zur Bekämpfung von Geldwäscherei, deren Vortaten, organisierter Kriminalität und Terrorismusfinanzierung. Daraus ergeben sich mehr Hinweise, wobei jedoch nicht alle relevant sind für die Strafverfolgungsbehörden. Hier ist die Filterfunktion der FIUs entscheidend.

---

2 SR **955.23**

3 Vgl. *Strategie des EJPD zur Kriminalitätsbekämpfung 2020–2023*.

4 Siehe hierzu MROS-Jahresbericht 2013, S. 56 ff. (abrufbar auf der MROS-Internetseite).

Die internationalen Rahmenbedingungen, unter denen FIUs arbeiten, haben sich verändert. Vor mehr als zwanzig Jahren, als die internationalen Geldwäschereinormen entstanden, war Sinn und Zweck des rechtlichen Instrumentariums die Identifizierung und Beschlagnahme von Vermögenswerten, die aus Straftaten stammen. Zu diesem repressiven Ziel kommt nun eine präventive Aufgabe hinzu. Die Rolle der FIUs hat sich entsprechend weiterentwickelt: Ihre Aufgabe ist nicht nur, für die Strafverfolgungsbehörden nützliche Informationen zu identifizieren; vielmehr sollen FIUs auch die Gesamtheit der empfangenen Signale des Dispositivs zur Bekämpfung von Geldwäscherei, deren Vortaten, der organisierten Kriminalität und der Terrorismusfinanzierung verwenden und die Schwachstellen dieses Dispositivs identifizieren. Zu diesem Zweck erstellen die FIUs strategische Analysen, die darauf abzielen, Methoden und Trends in diesen Kriminalitätsbereichen zu identifizieren. Ihre Erkenntnisse teilen die FIUs mit Finanzintermediären, Händler*innen, Drittbehörden, politischen Entscheidungsträgerinnen und -trägern oder der interessierten Öffentlichkeit (*follow the money*).
In den letzten zehn Jahren sind die Ressourcen der MROS zwar gewachsen, aber nicht in einem Masse, als dass die MROS ihre Aufgaben weiterhin mit den bestehenden Methoden erfüllen könnte. Die Änderungen zu Beginn des Jahres 2020 sind das Ergebnis des Bestrebens, den Entwicklungen des letzten Jahrzehnts Rechnung zu tragen, um den Herausforderungen der Zukunft besser begegnen zu können.
Die Einführung von goAML, eines Informationssystems, das in der Lage ist, die der MROS gemeldeten Informationen digital zu verarbeiten, ist der Eckpfeiler der neuen Strategie der MROS. Dieses System ermöglicht eine schnelle und sichere Kommunikation mit Finanzintermediären und nationalen Behörden. Ausserdem ermöglicht es goAML den MROS-Analystinnen und -Analysten, die erhaltenen Informationen ohne grossen Erfassungsaufwand zu verarbeiten. Neben der Effizienzsteigerung stellt dieser Digitalisierungsschritt eine Etappe hin zum verstärkten Einsatz von Analysetechniken dar, dank denen unter Zuhilfenahme künstlicher Intelligenz grosse Datenmengen ausgewertet werden können (*intelligence-led policing*). GoAML ist mittlerweile seit einem Jahr in Betrieb. In einem späteren Kapitel wird eine erste Bilanz zur Nutzung dieses Informationssystems gezogen (siehe Kapitel 3).

2.2 Die MROS-Strategie 2020–2021

Mit Wirkung Anfang 2020 verabschiedete die MROS eine neue Strategie für die Jahre 2020–2021. Sie beruht auf sieben voneinander abhängigen Zielen:

1) Die Analysen der MROS sind effektiv.
2) Die Qualität der Verdachtsmeldungen ist erhöht.
3) Die MROS stärkt die Prävention von Schwerst- und transnationaler Kriminalität.
4) Die Strafverfolgungsbehörden werden durch die MROS optimal unterstützt.
5) Die internationale Zusammenarbeit ist verstärkt und effektiv.
6) Die technischen Kapazitäten der MROS sind ausgebaut.
7) Die Mitarbeitenden der MROS vertiefen ihr Wissen und aktualisieren es laufend.

Das erste Ziel dieser Strategie ist, die Informationen, die die MROS erhält, effektiver zu verarbeiten. Dazu gilt es, Informationen schnell zu triagieren und angemessen zu analysieren, damit die MROS ihre Ressourcen dort einsetzt, wo sie den grössten Nutzen erbringen. Über kurz oder lang soll diese Triage auch durch auf künstlicher Intelligenz basierenden IT-Tools unterstützt werden, die es beispielsweise erlauben, relevante Elemente einer Verdachtsmeldung oder Bezüge zu laufenden Fällen rasch zu identifizieren. Seit dem 1. Januar 2020 bemisst sich die Analysetiefe – etwa wie und welche Informationen die MROS-Mitarbeitenden überprüfen – nach dieser Triage. Die Analyse hängt vom Inhalt der Verdachtsmeldung ab (z. B. die Komplexität gemeldeter Vorgänge), aber auch von der Strategie des EJPD zur Kriminalitätsbekämpfung 2020–2023 und von den Bedürfnissen der Strafverfolgungsbehörden. Die Art der Analyse wird auf der Grundlage von internen Priorisierungskriterien festgelegt.
Seit dem 1. Januar 2020 sind erhebliche Anstrengungen unternommen worden, um sicher-

zustellen, dass die Analyse die Bedürfnisse der Strafverfolgungsbehörden bestmöglich erfüllt. Zu diesem Thema hat ein regelmässiger Austausch mit den MROS-Partnern stattgefunden. Das neue Informationssystem ermöglicht es, die aus Verdachtsmeldungen stammenden Informationen in digitaler Form zu übermitteln. Ausserdem können Fälle von geringerer Bedeutung schnell bearbeitet werden, und die internen Prozesse der MROS sind so umgestaltet worden, dass weniger Ressourcen mobilisiert werden müssen.
Das zweite Ziel dieser Strategie ist die Stärkung der Rolle, die die MROS bei der weiter oben erwähnten Prävention spielt. Es gilt, die strategische Analyse der Risiken, Methoden und Trends der Geldwäscherei und Terrorismusfinanzierung zu verstärken und die Erkenntnisse mit Finanzintermediären, Händler*innen wie auch mit den zuständigen Behörden zu teilen. Denkbar ist dies beispielsweise im Rahmen der nationalen Risikoanalyse, eines unter der Ägide der Interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT) geführten kontinuierlichen Prozesses. Diese Arbeiten werden im Jahr 2021 fortgesetzt.
Die Umsetzung dieser Strategie erfordert einen engeren Austausch zwischen der MROS und ihren Partnern, seien es nationale oder internationale Behörden, internationale Organisationen (allen voran die Financial Action Task Force (FATF) und die Egmont-Gruppe) oder der private Sektor. Die Qualität des Informationsaustauschs mit ausländischen Partnern muss gesteigert werden, wozu die neuen Kompetenzen der MROS beitragen werden. Die Zusammenarbeit mit den Finanzintermediären soll durch eine öffentlich-private Partnerschaft (*public private partnership*) institutionalisiert werden, um es den Finanzintermediären zu ermöglichen, Risiken und verdächtige Transaktionen besser zu identifizieren, qualitativ hochwertige Verdachtsmeldungen zu erstatten und präventiv zu handeln.

2.3 Die neue Organisation der MROS

Im Jahr 2019 bewilligte der Bundesrat der MROS zwölf zusätzliche Vollzeitstellen. Am 31. Dezember 2020 hatte die MROS 57 besetzte Stellen mit insgesamt 48,8 Vollzeitäquivalenten, davon 10,3 Vollzeitäquivalente mit befristeten Arbeitsverträgen. Die Umsetzung der MROS-Strategie 2020–2021 machte eine Reorganisation dieser fedpol-Abteilung notwendig. Seit dem 1. Januar 2020 ist die MROS daher in sechs Bereiche unterteilt, die jeweils spezifische Aufgaben vorsehen. Drei Bereiche sind für die operative Analyse zuständig, das heisst hauptsächlich für die Bearbeitung der an die MROS gerichteten Verdachtsmeldungen. Die Abteilung Primäranalyse ist für den Empfang der eingehenden Informationen zuständig und hat eine koordinierende Rolle bei der Triage und der Zuweisung von Verdachtsmeldungen. Ausserdem bearbeitet sie Fälle, die eine schnelle Analyse erfordern. Weitere zwei Bereiche sind für die vertiefte Analyse zuständig – einer für Fälle in kantonaler Zuständigkeit (Operative Analyse Kantone), der andere für Fälle in Bundeszuständigkeit (Operative Analyse Bund). Der Bereich Internationales beschäftigt sich mit dem internationalen Austausch von Informationen. Er ist auch für Arbeiten im Zusammenhang mit der Teilnahme der MROS an den Aktivitäten internationaler Organisationen (FATF, Egmont-Gruppe) verantwortlich. Der Bereich Strategische Analyse untersucht Methoden und Trends der Geldwäscherei und übernimmt die der MROS zugewiesenen Aufgaben im Zusammenhang mit der nationalen Risikoanalyse. Der Bereich Planung und Policy ist mit den Führungsaufgaben der Abteilung, dem Austausch mit nationalen Behörden und mit den für die MROS relevanten rechtlichen Angelegenheiten befasst.

2.4 Künftige Herausforderungen

Das Jahr 2020 war eine intensive Zeit für die MROS. In den ersten Monaten des Jahres lag der Schwerpunkt auf der Implementierung des neu-

en elektronischen Informationssystems goAML. Dies erwies sich als eine sinnvolle Entscheidung, denn goAML ermöglichte es der MROS, trotz der aussergewöhnlichen Umstände, die im März durch die COVID-Pandemie entstanden, ihre Aufgaben zu erfüllen. Die Einführung dieses Systems erforderte jedoch mehrere Anpassungen, und nicht alle daraus resultierenden Probleme konnten gelöst werden, vor allem, was die Qualität der von den Finanzintermediären, Händler*innen übermittelten Informationen anbelangt. Hier gibt es für MROS noch eine Reihe vordringlicher Arbeiten zu erledigen. Zunächst bedeutet dies einen wichtigen Aufwand. Letztendlich aber wird sich die Bearbeitungszeit von Verdachtsmeldungen verkürzen und die Qualität der Analyse verbessern. Im Laufe des Jahres 2020 bearbeitete die MROS auch die mehr als 6 000 im Zeitraum von 2016 bis 2019 gemeldeten Geschäftsbeziehungen, die Ende 2019 noch in der Bearbeitung waren (siehe Kapitel 4.13). Im Jahr 2021 wird sich die MROS prioritär auf die Umsetzung ihrer Strategie konzentrieren. Die Arbeit im Bereich der strategischen Analyse wird verstärkt und der Austausch mit den Finanzintermediären ausgeweitet.

.

3. Einführung des neuen Informationssystems goAML bei MROS

Auf den 1. Januar 2020 hat die MROS das Informationssystem goAML eingeführt. Der Wechsel auf ein neues Informationssystem war ein unerlässlicher Schritt in Zusammenhang mit der Digitalisierung. Das neue System ermöglicht einerseits den dem GwG unterstellten Finanzintermediären, Händler*innen, Behörden und Organisationen (Selbstregulierungsorganisationen [SRO] und Aufsichtsorganisationen [AO]), Verdachtsmeldungen digital über ein Online-Portal einzureichen. Andererseits erlaubt es der MROS, gestützt auf Art. 23 Abs. 4 GwG ihre Analyseberichte und Beilagen ebenfalls in digitaler Form an die zuständigen Schweizer Strafverfolgungsbehörden zu übermitteln sowie Informationen mit inländischen Behörden unter den Voraussetzungen von Art. 29 GwG auszutauschen.
GoAML hat sich seither als sicheres und effizientes Kommunikationstool zwischen den verschiedenen Parteien etabliert. Dank der elektronischen Übermittlung und Bearbeitung der Verdachtsmeldungen konnte nicht nur der Papierverbrauch drastisch reduziert werden, sondern ist es nun ebenfalls möglich, jederzeit ortsungebunden zu arbeiten, was sich angesichts der COVID-Pandemie als äusserst nützlich erwiesen hat.
Gleichzeitig hat dieses System die MROS vor gewisse Herausforderungen bezüglich der Datenübermittlung gestellt. Bestimmte Anpassungen in Zusammenhang mit der Quantität der elektronisch zu erfassenden Transaktionen wurden bereits am 21. Juli 2020 publiziert. Spätestens ab dem 1. April 2021 sind der MROS nur die verdächtigten Transaktionen gemäss Art. 3 Abs. 1 Bst. h MGwV elektronisch zu melden.[5]
Zudem entsprechen die eingereichten Daten nicht immer der notwendigen Qualität (vgl. unten Ziff. 3.5).

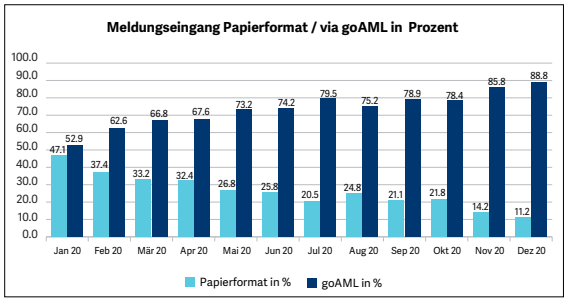
3.1 Anzahl registrierter Finanzintermediäre

Bis am 31. Dezember 2020 registrierten sich 728 Finanzintermediäre und damit verbunden 1494 Personen in goAML. Einige Finanzintermediäre haben zwar den Registrierungsprozess gestartet, den zweiten Schritt, nämlich die Registrierung in goAML selber, noch nicht vollendet.
Von den 728 registrierten Finanzintermediären haben bisher lediglich 252 eine Verdachtsmeldung via goAML an die MROS übermittelt.

3.2 Anteil elektronisch eingereichter Verdachtsmeldungen

Seit der Umstellung auf goAML wird die Möglichkeit, Meldungen elektronisch einzureichen von den Finanzintermediären rege benutzt. So erreichte der Anteil der über goAML eingereichten Verdachtsmeldungen schon im Januar über 50 % und erhöhte sich in den nachfolgenden Monaten stetig. Im Dezember 2020 schliesslich betrug die Quote der elektronisch übermittelten Verdachtsmeldungen knapp 90%. Nachfolgend eine Grafik zum Meldungseingang, unterteilt nach elektronisch und in Papierformat eingereichten Verdachtsmeldungen:

[5] Vgl. die *Publikation Anpassungen der Praxis für Meldungen via goAML*, auf der Internetseite der MROS. Diese Publikation wurde am 30. März 2021 durch die Version 2.0 ersetzt *(Anpassung der Praxis für Meldungen via goAML gültig ab 01.04.2021)*



goAML hat sich im Verlaufe des Jahres 2020 auch in Zusammenhang mit den Informationsanfragen der MROS basierend auf Art. 11a GwG etabliert. Die Finanzintermediäre können ihren mit diesem Gesetzesartikel verbundenen Pflichten mittels separatem Reporttyp über goAML nachkommen. In diesem Bereich ist die Quote der über einen entsprechenden Report in goAML eingereichten Unterlagen und Informationen erfreulich. Diese stieg von 46 % im Januar auf 68 % im Dezember 2020. Die MROS erhofft sich, diese Quote im Jahre 2021 weiter zu erhöhen.

3.3 Varianten für die Einreichung von Verdachtsmeldungen via goAML

Um den Bedürfnissen der Finanzintermediäre bestmöglich gerecht zu werden, wurden verschiedene technische Lösungen entwickelt, wie die elektronische Übermittlung von Verdachtsmeldungen an die MROS erfolgen kann. Es werden aktuell drei Arten der Einreichung von Verdachtsmeldungen via goAML angeboten (vgl. unten). Weitergehende Informationen und Dokumentationen zu den verschiedenen Lösungen sind online abrufbar.[6]

3.3.1 Automatisierte Datenaufbereitung (*Upload*)

Die automatisierte Meldungserstellung setzt voraus, dass der Finanzintermediär eine interne IT-Applikation programmiert hat. Diese Applikation sorgt dafür, dass die Daten aus dem System des meldenden Instituts Finanzintermediärs in einer XML-Datei aufbereitet wird. Diese XML-Datei hat eine klar vordefinierte Struktur. Die aufbereitete Datei wird anschliessend im Online-Portal von goAML hochgeladen und an die MROS übermittelt. Die Entwicklung der dafür notwendigen IT-Lösung liegt in der Verantwortung des jeweiligen meldenden Instituts.

3.3.2 Halbautomatisierte Erfassung

Bei der halbautomatisierten Meldungserstellung erfolgt eine manuelle Erfassung im goAML-Online-Portal, bei welcher jedoch die Informationen zu Konten und Transaktionen mittels einer XML-Datei hochgeladen werden. Fehlende Informationen können anschliessend manuell ergänzt werden. Diese Funktionalität führt zu Zeitersparnissen für jene Finanzintermediäre, welche die automatisierte Lösung nicht umsetzen möchten, jedoch eine grössere Anzahl von Transaktionen zu melden haben. Damit diese Option genutzt werden kann, müssen die Transaktionen aus dem Bankensystem in strukturierter und vordefinierter Form als XML-Datei lokal gespeichert und im goAML-web hochgeladen werden.

3.3.3 Manuelle Erfassung

Die manuelle Meldungserstellung erfolgt direkt im goAML-Online-Portal und stellt – neben dem Internetzugang und den persönlichen Login-Daten – keine technischen Anforderungen. Hierbei sind die relevanten Angaben zu erfassen und die einzelnen Felder auszufüllen. Je nach Art der Meldung kann die manuelle Erfassung zeitaufwändig sein. Dies ist insbesondere der Fall, wenn viele Transaktionen zu erfassen sind.

---

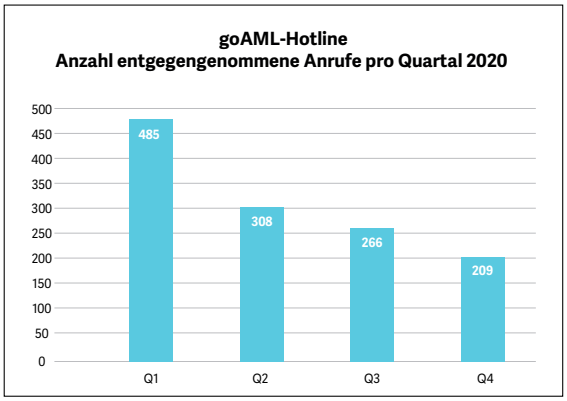
[6] Vgl. *Informationen zur Einführung des neuen Datenverarbeitungssystems goAML bei MROS,* auf der Internetseite der MROS.

3.4 goAML-Support

Bereits bei der Einführung von goAML wurde ein Handbuch für die Erfassung von manuellen Meldungen im Online-Portal zur Verfügung gestellt. Im Verlaufe des Jahres 2020 hat die MROS die FAQs[7], also Antworten auf von Finanzintermediären häufig gestellte Fragen, erstellt und das goAML Web-Handbuch[8] überarbeitet. Weitere online zugängliche Dokumente helfen den Finanzintermediären bei der Erfassung von Verdachtsmeldungen und ein Newsletter bedient die meldenden Institute regelmässig mit Tipps und Tricks. Newsletter sind ein praktisches Hilfsmittel, um direkt an die Benutzer*innen von goAML zu gelangen. Es ist geplant, solche Newsletter regelmässig zu veröffentlichen.

3.4.1 goAML-Hotline

Um die Finanzintermediäre, Behörden und weiteren Nutzer bei der Umstellung auf goAML bestmöglich zu unterstützen, hat die MROS eine goAML-Hotline (Telefon oder E-Mail) eingerichtet. Die MROS hat für diesen fachlichen Support (z. B. bei der Registrierung, bei spezifischen Fragen zur Erfassung einer Meldung oder zur Umsetzung der automatisierten Meldungserstellung via XML-Datei) eigene Mitarbeitende bereitgestellt. Gerade während der Registrierungsphase und im ersten Halbjahr wurde die goAML-Hotline täglich von mehreren Dutzend Personen kontaktiert. Heute hat das Informationssystem goAML bei vielen meldenden Instituten eine hohe Akzeptanz. Positive Rückmeldungen von Finanzintermediären zeigen, dass sich der zusätzliche Aufwand, welcher neben dem Tagesgeschäft für die MROS anfiel, gelohnt hat.
In der nachfolgenden Grafik wird die Übersicht über die Auslastung der goAML-Hotline während des Jahres 2020 dargestellt. Insgesamt haben die Mitarbeitenden der MROS-Hotline im Jahre 2020 1 268 Anrufe entgegengenommen. Sie beantworteten zudem viele weitere Anrufe auf ihren direkten Telefonnummern (z. B. bei Folgefragen).



3.5 Qualität der eingehenden Informationen

Wie eingangs erwähnt war im ersten Jahr die Qualität der von den Finanzintermediären eingereichten Daten, namentlich die Transaktionsinformationen zum Teil ungenügend und dies bescherte der MROS einen beträchtlichen Korrekturaufwand. MROS musste zusätzliche Bereinigungsaufgaben vornehmen, dies mehrheitlich manuell, um korrekte und auswertbare Daten zur Verfügung zu haben, um gestützt darauf ihre Analysen durchführen zu können. Insbesondere war nicht immer klar, welche Person oder Geschäftsbeziehung gemeldet wurde. Zudem hat die MROS den Kontakt mit den Finanzintermediären gesucht, wenn systematische Fehler aufgrund der Programmierung ihrer Schnittstellen entstanden, um die Quote der vom System automatisch aufgrund von Datenqualitätsmängel verworfenen Meldungen zu senken.
Diese Ausführungen zeigen auf, inwieweit die Einreichung von qualitativ guten Daten für die MROS und die Strafverfolgungsbehörden von erheblicher Bedeutung ist. Es soll vermieden werden, dass die MROS systematisch unkorrekte Daten bereinigen muss und somit einer der Hauptvorteile des elektronischen Meldesystems zunichte gemacht wird.
Für die MROS und die zuständigen Strafverfolgungsbehörden ist es wichtig, korrekte und auswertbare Daten zu erhalten, damit diese effizient und zielführend analysiert werden können. Wenn

[7] Vgl. die Publikation goAML: *Frequently Asked Questions (FAQ)*, auf der Internetseite der MROS.

[8] Vgl. die Publikation *goAML-Web Handbuch*, auf der Internetseite der MROS.

es darum geht, Transaktionen zu melden, ist es unerlässlich, dass die notwendigen Grundinformationen (Angaben zu den Personen, Kontoangaben, etc.) den oben erwähnten Behörden erlauben, ihre Analysen durchführen zu können.

3.6 Ausblick

UNODC *(United Nations Office on Drugs and Crime),* eine Abteilung der Organisation der Vereinten Nationen (UNO) in Wien, ist die Anbieterin der Software goAML. Die Software wird bereits in über 60 Ländern eingesetzt. Die UNODC entwickelt die Software kontinuierlich weiter. Gerade in den Bereichen *Crypto Currencies, Entity-to-Entity-Relations* und politisch exponierte Personen (PEP) werden gegenwärtig weitere Funktionalitäten entwickelt. Diese Verbesserungen werden in enger Zusammenarbeit mit und aufgrund der Wünsche der beteiligten FIUs gemacht. Eine neue Version von goAML ist zurzeit in Arbeit.

4. Jahresstatistik der Meldestelle

Durch die Einführung des Systems goAML hat sich die Zählweise der von der MROS erhaltenen Verdachtsmeldungen geändert. Seit dem 1. Januar 2020 zählt die Meldestelle die Anzahl Meldungen und nicht wie bis anhin die Anzahl gemeldeter Geschäftsbeziehungen. Da mit einer einzigen Verdachtsmeldung mehrere Geschäftsbeziehungen gemeldet werden können, ist es deshalb schwierig, präzise Vergleiche mit den Zahlen der Vorjahre vorzunehmen.

Um dennoch einen Vergleich mit den Statistiken der Vorjahre zu ermöglichen, haben wir uns entschieden, wann immer möglich, Prozentzahlen zu veröffentlichen. Im Geschäftsjahr 2019 umfasste jede Verdachtsmeldung, die schweizerische Finanzintermediäre bei der MROS eingereicht haben, im Durschnitt 1,8 Geschäftsbeziehungen. Wir haben diesen Durchschnittswert verwendet, um die Entwicklung der Anzahl Verdachtsmeldungen zu analysieren, die die MROS im Jahr 2020 erhalten hat, und um, wo immer möglich, diese mit den Zahlen der Vorjahre zu vergleichen.

4.1 Gesamtübersicht Meldestelle-Statistik 2020

Zusammenfassung Geschäftsjahr 2020
(1. Januar–31. Dezember 2020)

Anzahl Meldungen	2020 Absolut	2020 Relativ
Total eingegangene Meldungen	**5 334**	**100,0 %**
Bearbeitete Meldungen	4 505	84,5 %
Meldungen in Bearbeitung per 31. Dezember 2020	829	15,5 %
Branche		
Banken	4 773	89,5 %
Zahlungsverkehrsdienstleister	185	3,5 %
Andere	121	2,3 %
Kreditkarten	83	1,6 %
Vermögensverwalter / Anlageberater	45	0,9 %
Treuhänder	30	0,6 %
Casinos	29	0,5 %
Versicherungen	20	0,4 %
Kredit-, Leasing-, Factoring- und Forfaitierungsgeschäfte	19	0,4 %
Rohwaren- und Edelmetallhandel	12	0,2 %
Rechtsanwälte und Notare	6	0,1 %
Trustees	4	0,1 %
Geldwechsel / Change	3	0,1 %
Effektenhändler	2	0,0 %
Selbstregulierungsorganisationen (SRO) / FINMA / ESBK	2	0,0 %

Die voranstehende Tabelle enthält die Übersicht der Verdachtsmeldungen, die die MROS im Berichtsjahr erhalten hat. Sie umfasst aber nicht die Gesamtzahl der Verdachtsmeldungen, die im Jahr 2020 bearbeitet worden sind. Ende 2019 befanden sich 6 095 Geschäftsbeziehungen, die zwischen

2016 und 2019 gemeldet worden waren, noch in Bearbeitung. Der Grossteil dieser Geschäftsbeziehungen konnte während dem Berichtsjahr bearbeitet werden (siehe Kapitel 4.13). Sie sind aber nicht auf dieser Tabelle aufgeführt.

Anzeigen	1 939	100,0 %
An die Bundesanwaltschaft	175	9,0 %
An die kantonalen Staatsanwaltschaften	1 764	91,0 %

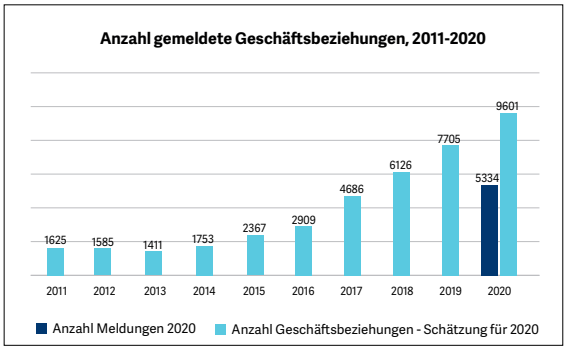
Die voranstehende Tabelle enthält die Übersicht der Anzeigen der MROS an die Strafverfolgungsbehörden im Jahr 2020. Bis 2019 bestanden diese Anzeigen darin, dass die MROS die von ihr erhaltenen Verdachtsmeldungen analysierte und den Strafverfolgungsbehörden weiterleitete. Neu erstellt die MROS, anhand der ihr zur Verfügung stehenden Informationen einen Bericht. Die Verdachtsmeldungen sind der zentrale aber nicht der einzige Bestandteil dieser Berichten. Folglich können die Informationen in einer Anzeige von verschiedenen Behörden und aus mehreren Verdachtsmeldungen stammen (siehe Kapitel 4.12). Eine geringe Anzahl der Anzeigen aus dem Jahr 2020 enthält Informationen, die der MROS bereits in den Vorjahren gemeldet worden waren. Deshalb können aber die Anzahl der Anzeigen und der Verdachtsmeldungen des Berichtsjahrs nicht miteinander verglichen werden.

4.2 Allgemeine Feststellungen

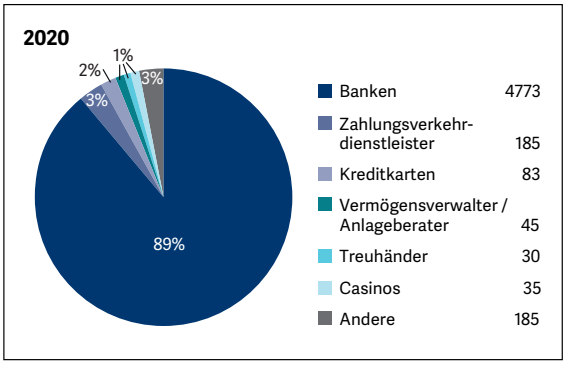
1. Im Jahr 2019 waren der MROS 7 705 Geschäftsbeziehungen gemeldet worden. 2020 hat die Meldestelle 5 334 Verdachtsmeldungen erhalten. Gestützt auf die Schätzung, wonach eine Verdachtsmeldung im Jahr 2019 im Durchschnitt 1,8 Geschäftsbeziehungen umfasste (d. h. die Schätzung gemeldeter Geschäftsbeziehungen im 2020 beläuft sich auf 9 601), entspricht die Anzahl Meldungen im Jahr 2020 einem Zuwachs von rund 25 Prozent gegenüber dem Vorjahr.
2. Dieser Anstieg ist zum Teil auf zahlreiche Meldungen zurückzuführen, die die MROS wegen Verdacht auf Veruntreuung oder Erschleichung von COVID-Krediten erhalten hat.
3. Unter den Finanzintermediären, ist der Bankensektor, wie schon 2019, nach wie vor die Branche, die bei weitem den grössten Teil von Verdachtsmeldungen erstattet hat.
4. Die Finanzintermediäre haben 2020 in 58 Prozent der Fälle Betrug als mutmassliche Vortat gemeldet. Obschon statistische Verzerrungen einen genauen Vergleich mit den Vorjahren verunmöglichen, beweist diese Zahl, dass Betrug zweifellos die häufigste durch die Finanzintermediäre gemeldete mutmassliche Vortat ist.
5. Zum ersten Mal ist das Transaktionsmonitoring die Erkenntnisquelle, die am häufigsten zu einem Verdacht der Finanzintermediäre geführt hat (siehe Kapitel 4.8).

4.3 Verdachtsmeldungen

Infolge der Einführung von goAML, wurde die Zählweise der Verdachtsmeldungen geändert. Um dennoch einen Vergleich mit den Statistiken der Vorjahre zu ermöglichen, stützen wir uns darauf, dass im Geschäftsjahr 2019 jede Verdachtsmeldung, die die schweizerischen Finanzintermediäre bei der MROS eingereicht haben, im Durschnitt 1,8 Geschäftsbeziehungen umfasste. Wir haben diesen Durchschnittswert verwendet, um die Entwicklung der Anzahl Verdachtsmeldungen zu analysieren, die die MROS im Jahr 2020 erhalten hat, und um, wo möglich, diese mit den Zahlen der Vorjahre zu vergleichen. Folglich entsprechen die 5 334 Verdachtsmeldungen, die die MROS im Jahr 2020 erhalten hat, schätzungsweise 9 061 Geschäftsbeziehungen. Aufgrund dieser Schätzung, ist die Anzahl Verdachtsmeldungen 2020, gegenüber dem Vorjahr, um beinahe 25 Prozent gestiegen. Die seit 2015 festgestellte Tendenz setzt sich somit fort.



4.4 Herkunft der meldenden Finanzintermediäre nach Branchen



- Fast 90 Prozent der Meldungen stammen von Banken.
- Im Vergleich zum Vorjahr sind die prozentualen Anteile der verschiedenen Finanzintermediäre sehr stabil. Wie 2019 stammt ein Prozent der Meldungen von Treuhändern, Vermögensverwaltern und Anlageberatern sowie Casinos, während der Anteil der Verdachtsmeldungen von Zahlungsverkehrsdienstleistern von vier auf drei Prozent gesunken ist.
- Zur Kategorie «Andere» zählen insbesondere Virtual Asset Service Providers (VASP)[9]. Die Zunahme der Anzahl Meldungen dieser Kategorie ist allerdings zum Teil davon beeinflusst, dass die Zählweise der Verdachtsmeldungen seit der Einführung von goAML geändert hat.

Zum Vergleich: 2011 bis 2020[10] (in %)

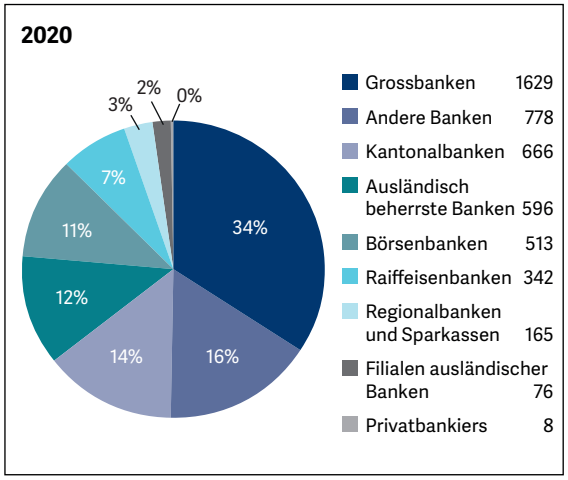
Branche	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2020 in absoluten Zahlen	Durchschnitt 2011–2020
Banken	66,5	66,2	79,6	85,3	91,3	86,0	91,0	88,8	89,9	89,5	4 773	**83,4**
Zahlungsverkehrsdienstleister	23,3	22,9	5,2	6,1	2,4	4,4	3,1	4,4	4,0	3,5	185	**7,9**
Andere	0,1	0,3	0,1	0,2	0,2	0,7	0,4	2,3	0,6	2,3	121	**0,7**
Kreditkarten	0,6	1,4	1,0	0,5	0,5	0,7	0,3	1,2	1,3	1,6	83	**0,9**
Vermögensverwalter / Anlageberater	1,7	3,1	5,2	2,3	1,9	2,2	1,9	1,0	0,9	0,8	45	**2,1**
Treuhänder	3,8	4,1	4,9	2,8	2,0	1,5	1,1	0,7	0,8	0,6	30	**2,2**
Casinos	0,4	0,4	0,6	0,5	0,1	0,5	0,6	0,5	0,7	0,5	29	**0,5**
Versicherungen	0,7	0,6	1,3	0,6	0,5	3,1	0,5	0,6	0,3	0,4	20	**0,9**
Kredit-, Leasing-, Factoring- und Forfaitierungsgeschäfte	0,3	0,1	0,3	0,2	0,3	0,3	0,3	0,3	0,3	0,4	19	**0,3**
Rohwaren- und Edelmetallhandel	0,1	0,2	0,7	0,2	0,3	0,1	0,2		0,3	0,2	12	**0,2**
Rechtsanwälte und Notare	1,9	0,8	0,6	0,6	0,3	0,2	0,1	0,1	0,1	0,1	6	**0,5**
Trustees										0,1	4	**0,0**
Geldwechsel / Change	0,2									0,1	3	**0,0**
Effektenhändler	0,0	0,1	0,1	0,6	0,1	0,1	0,3	0,1	0,3	0,0	2	**0,2**
SRO	0,1			0,1					0,1	0,0	2	**0,0**
Devisenhandel	0,4		0,4			0,1			0,3	0,0	0	**0,1**
Behörde				0,1							0	**0,0**
Vertriebsträger von Anlagefonds							0,1				0	**0,0**
Total	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**5 334**	**100,0**

[9] Unter VASPs versteht man Kryptobörsen, Wallet-Anbieter, Finanzdienstleister im Zusammenhang mit der Ausgabe, dem Angebot und dem Verkauf von virtuellen Vermögenswerten oder andere Finanzintermediationsdienste im Zusammenhang mit Kryptowährungen.

[10] Die absoluten Zahlen für die Jahre 2011–2019 sind in den Jahresberichten der MROS für die entsprechenden Jahre veröffentlicht. Der Vollständigkeit halber sei angemerkt, dass Händler*innen in dieser Statistik nicht enthalten sind, da die MROS 2017 und 2019 jeweils nur eine Meldung einer Händlerin oder eines Händlers erhalten hat, was weniger als 0,1 Prozent der Gesamtzahl der Verdachtsmeldungen in diesen Jahren entspricht.

4.5 Die Banken

Die nachfolgende Grafik zeigt die Verteilung der Verdachtsmeldungen der Banken aufgeschlüsselt nach Bankkategorien.



- Die untenstehende Tabelle deutet auf erhebliche Veränderungen gegenüber 2019 hin: Der Anteil der Meldungen von Privatbankiers, Börsenbanken und ausländisch beherrschten Banken ist deutlich zurückgegangen (von 1 % auf 0 % bzw. von 25 % auf 11 % und von 27 % auf 12 %), während jener der Grossbanken, der Kantonalbanken, der Raiffeisenbanken und der anderen Banken zugenommen hat (von 28 % auf 34 % bzw. von 5 % auf 14 %, von 3 % auf 7 % und von 8 % auf 16 %).
- Diese Veränderungen sind teilweise darauf zurückzuführen, dass die Zählweise der Verdachtsmeldungen geändert hat (siehe Kapitel 4 und 4.3). Zahlenmässig haben Finanzintermediäre, welche tendenziell Verdachtsmeldungen mit mehreren Geschäftsbeziehungen erstatten, weniger Gewicht, da die Anzahl Verdachtsmeldungen – und nicht der gemeldeten Geschäftsbeziehungen – in der Statistik berücksichtigt wird.
- Die Zunahme der Meldungen von Kantonalbanken von 5,3 Prozent (2019) auf 14,0 Prozent im Berichtsjahr lässt sich zum Teil durch die hohe Zahl von Meldungen im Zusammenhang mit COVID-Krediten erklären.

Zum Vergleich: 2011 bis 2020[11] (in %)

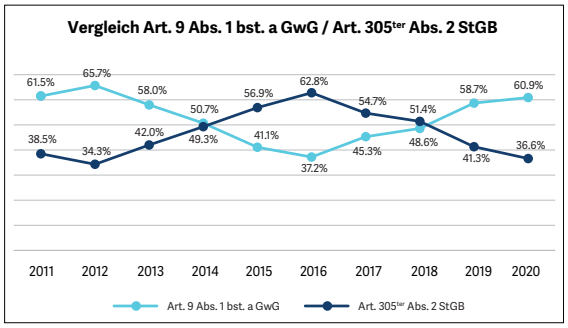
Bankenkategorie[12]	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2020 in absoluten Zahlen	Durchschnitt 2011–2020
Kantonalbanken	6,9	7,6	6,4	5,0	5,8	7,6	5,2	5,5	5,3	14,0	666	**6,9**
Grossbanken	28,7	29,3	28,9	31,7	35,3	31,1	26,3	26,7	28,2	34,1	1629	**30,0**
Regionalbanken und Sparkassen	1,4	1,8	0,5	0,9	0,5	1,2	0,6	1,1	1,3	3,5	165	**1,3**
Raiffeisenbanken	5,6	6,1	7,0	9,0	5,8	6,2	3,9	3,2	3,1	7,2	342	**5,7**
Börsenbanken	14,4	12,1	10,2	10,6	14,0	12,4	12,7	20,8	25,1	10,7	513	**14,3**
Andere Banken	2,5	4,0	20,5	14,3	9,9	12,9	9,6	9,5	8,6	16,3	778	**10,8**
Privatbankiers	2,4	5,7	4,6	2,6	1,8	2,3	1,7	1,9	1,3	0,2	8	**2,5**
Ausländisch beherrschte Banken	36,0	33,1	21,4	25,6	26,6	26,3	39,8	31,0	26,9	12,5	596	**27,9**
Filialen ausländischer Banken	1,9	0,2	0,4	0,2	0,3	0,1	0,1	0,3	0,2	1,6	76	**0,5**
Institute mit besonderem Geschäftskreis	0,1	0,0	0,1	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0	**0,0**
Total	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**4773**	**100,0**

[11] Die absoluten Zahlen für die Jahre 2011–2019 sind in den Jahresberichten der MROS für die entsprechenden Jahre veröffentlicht.

[12] Die Bankenkategorien und Reihenfolge entsprechen denjenigen der Schweizerischen Nationalbank. Vgl. die Publikation *Die Banken in der Schweiz, 2019, S. 9.*

4.6 Rechtsgrundlagen der Meldungen

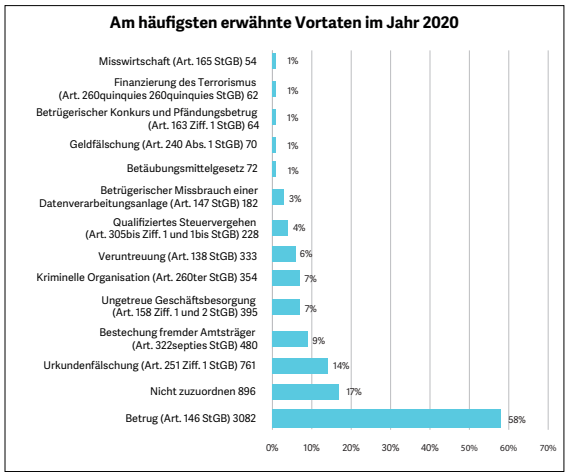
3 248 (60,9 %) der 5 334 Meldungen, die im Berichtsjahr eingegangen sind, wurden aufgrund der Meldepflicht gemäss Art. 9 Abs. 1 Bst. a GwG und 1 952 (36,6 %) aufgrund des Melderechts gemäss Art. 305ter Abs. 2 des Schweizerischen Strafgesetzbuchs vom 21. Dezember 1937 (StGB)[13] erstattet. 129 Meldungen basierten auf Art. 9 Abs. 1 Bst. b GwG (2,4 %) und zwei auf Art. 27 Abs. 4 GwG.



Die relative Zunahme der Anzahl Meldungen nach Art. 9 Abs. 1 Bst. a GwG, die seit 2016 zu beobachten ist, setzt sich also fort. Da die überwiegende Mehrheit der Meldungen an die MROS von Banken stammt, zeigt dieser Trend vor allem das Verhalten des Bankensektors auf. Die meldenden Schweizer Banken greifen allerdings je nach Bankenkategorie sehr unterschiedlich auf Art. 9 Abs. 1 Bst. a GwG oder aber Art. 305ter Abs. 2 StGB zurück, wie die nachfolgende Tabelle zeigt.

4.7 Vortaten

Die nachfolgende Grafik zeigt, wie häufig bei den eingegangenen Meldungen im Jahr 2020 eine bestimmte vermutete Vortat erwähnt wurde. Im Gegensatz zu den Vorjahren, kann der meldende Finanzintermediär seit 2020 bei jeder Meldung mehrere mutmassliche Vortaten angeben. Folglich ist es zwar möglich, den Anteil einer erwähnten Vortat unter allen Meldungen zu ermitteln. Die Summe dieser Anteile beträgt aber mehr als 100 Prozent, so dass ein Vergleich mit den Anteilen der Vorjahre verzerrt ausfallen würde und lediglich als Hinweis dienen kann.



– Die erheblichen Unterschiede zwischen 2020 und den Vorjahren lassen sich demnach zum

Bankenkategorie	Art. 9 Abs. 1 bst. a GwG	in %	Art. 305ter Abs. 2 StGB	in %	Andere	in %	Total	in %
Kantonalbanken	554	83,1	106	15,9	6	0,9	666	100,0
Grossbanken	790	48,5	829	50,8	10	0,6	1629	100,0
Regionalbanken und Sparkassen	97	58,7	60	36,3	8	4,8	165	100,0
Raiffeisenbanken	305	89,1	28	8,1	9	2,6	342	100,0
Börsenbanken	230	44,8	250	48,7	33	6,4	513	100,0
Andere Banken	663	85,2	101	12,9	14	1,8	778	100,0
Privatbankiers	3	37,5	5	62,5	0	0,0	8	100,0
Ausländisch beherrschte Banken	301	50,5	269	45,1	26	4,3	596	100,0
Filialen ausländischer Banken	12	15,7	64	84,2	0	0,0	76	100,0
Total	**2955**	**61,9**	**1712**	**35,8**	**106**	**2,2**	**4773**	**100,0**

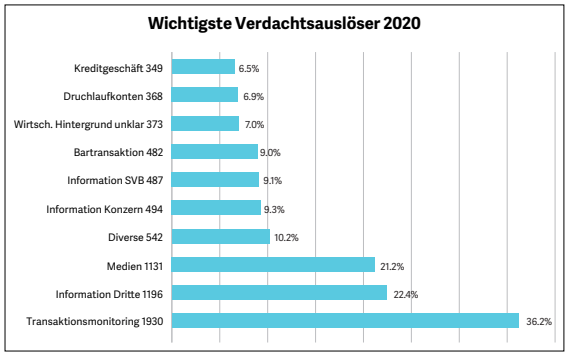
[13] SR **311.0**

Teil dadurch erklären, dass die Finanzintermediäre jetzt die Möglichkeit haben, mehrere vermutete Vortaten aus einer allgemeinen Liste anzugeben, welche ausserdem aktualisiert und erweitert worden ist.

– Es zeigt sich jedoch, dass die Zahl der Meldungen, bei denen Betrug als Vortat vermutet wurde, im Berichtsjahr geradezu explodiert ist: Während dieser Verdacht 2019 bei 25 Prozent und 2018 bei 20 Prozent der Meldungen erwähnt wurde, war dies 2020 bei 58 Prozent der Fall. Diese Entwicklung ergibt sich teilweise aus der hohen Anzahl Meldungen im Zusammenhang mit der Vergabe von COVID-Krediten (siehe Kapitel 5.1).
– 2020 gingen zudem die Meldungen mit der vermuteten Vortat der Bestechung drastisch zurück. Die Bestechung fremder Amtsträger wurde in 480 Meldungen, also 9 Prozent der Fälle genannt, die aktive Bestechung von inländischen Amtsträgern in 21 (0,39 %) und die passive Bestechung von inländischen Amtsträgern in 17 Fällen (0,32 %). Diese drei Kategorien, die in den früheren Berichten nicht unterschieden wurden, machten 2019 insgesamt 24 Prozent der eingegangenen Verdachtsmeldungen aus, 2018 waren es 27 Prozent.
  Es ist schwierig, solche Schwankungen von einem Jahr zum andern zu interpretieren. Der Rückgang der Meldungen wegen mutmasslicher Geldwäscherei im Zusammenhang mit Korruption lässt sich teilweise dadurch erklären, dass einige internationale Fallkomplexe, die in den letzten Jahren den schweizerischen Finanzplatz prägten und zu zahlreichen gemeldeten Geschäftsbeziehungen bei der MROS führten, mittlerweile kaum mehr Meldungen auslösen.

4.8 Verdachtsbegründende Elemente

Die nebenstehende Grafik zeigt den Anteil der verdachtsbegründenden Elemente unter den Meldungen, die 2020 eingegangen sind. Wie bei den Vortaten können die Finanzintermediäre im Gegensatz zu den Vorjahren im Informationssystem goAML neu mehrere Gründe angeben, die ihren Verdacht ausgelöst haben. Somit kann berechnet werden, bei welchem Anteil der Meldungen ein bestimmtes Element entscheidend war. Hingegen ist es nicht mehr möglich, einen präzisen Vergleich dieser Zahlen mit jenen der Vorjahre vorzunehmen.



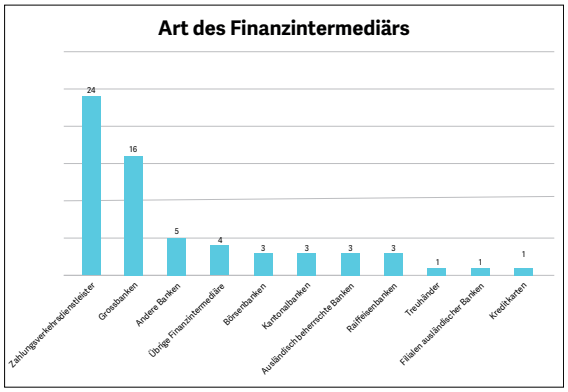
– Ein Vergleich mit den Vorjahren, in denen nur ein einziger Verdachtsauslöser genannt werden konnte, ist nicht aussagekräftig.
– Das Transaktionsmonitoring ist aber im Berichtsjahr erstmals der am häufigsten genannte Verdachtsauslöser (36,2 % im Jahr 2020 gegenüber 31 % im Vorjahr und 25 % im Jahr 2018). Dies bestätigt die erhöhte Sensibilität der Finanzintermediäre bei den Abklärungen und Analysen von Transaktionen gemäss Art. 6 Abs. 2 GwG.
– Medienberichte, die in den Vorjahren in den meisten Fällen den Verdacht der Finanzintermediäre begründet hatten, waren 2020 deutlich weniger dominant (21,2 % der Fälle gegenüber 35 % im Vorjahr und 38 % im Jahr 2018).

4.9 Terrorismusfinanzierung

Im Berichtsjahr erhielt die MROS 64 Meldungen wegen Verdacht auf Terrorismusfinanzierung und/oder Verstoss gegen das Bundesgesetz über das Verbot der Gruppierungen «Al-Qaïda» und «Islamischer Staat» sowie verwandter Organisationen[14], was einem Anteil von 1,2 Prozent aller Meldungen entspricht. Da es Schätzungen zufol-

[14] SR **122**

ge etwa 1,8 Geschäftsbeziehungen pro Meldung gibt, betreffen diese 64 Fälle rund 115 Geschäftsbeziehungen. Diese Zahl ist fast identisch mit jener aus 2019 (114). Diese 64 Meldungen werden auch mit anderen Vortaten in Verbindung gebracht, genauer gesagt mit Zugehörigkeit zu einer kriminellen Organisation (19 Fälle), Betrug (7 Fälle) und Bestechung von fremden Amtsträgern (3 Fälle). In zehn Fällen wurden ausserdem noch andere vermutete Vortaten erwähnt.
Der am häufigsten genannte Verdachtsauslöser der Finanzintermediäre – und vor allem der Zahlungsverkehrsdienstleister – ist das Transaktionsmonitoring (33 Fälle), gefolgt von Presseartikeln (20), Bartransaktionen (15), Informationen von Dritten (13) und Verbindungen mit kritischen Ländern (8). In zwölf Fällen wurden andere Gründe genannt.
Die meisten Meldungen (34) stammen von Banken, 24 von Zahlungsverkehrsdienstleistern. Nur gerade sechs wurden von anderen Arten von Finanzintermediären erstattet.



47 der 64 eingegangenen Meldungen waren nicht Gegenstand einer Anzeige seitens MROS. Zwei waren am Ende des Berichtsjahres noch in Bearbeitung. Die Informationen aus den restlichen 15 Meldungen führten zu 14 Anzeigen bei den zuständigen Strafverfolgungsbehörden. In drei Fällen wurde ein formelles Strafverfahren eröffnet, eines davon allerdings wegen Menschenhandel und nicht wegen Verstössen gegen das Bundesgesetz über das Verbot der Gruppierungen «Al-Qaïda» und «Islamischer Staat» sowie verwandter Organisationen.

4.10 Organisierte Kriminalität

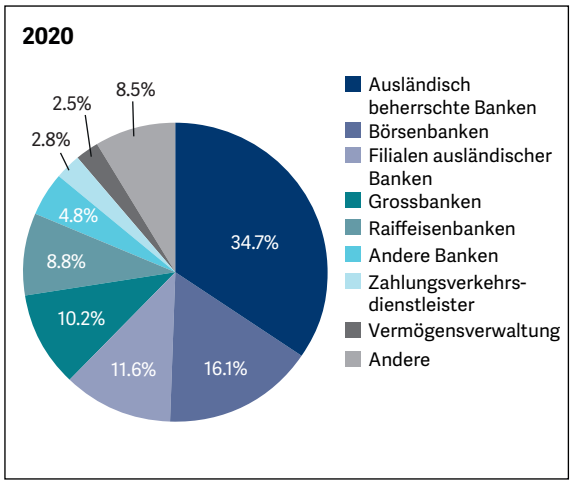
2020 erhielt die MROS 354 Verdachtsmeldungen wegen Verbindungen mit einer kriminellen Organisation, was 6,6 Prozent aller eingegangenen Meldungen entspricht. Unter Berücksichtigung der oben erwähnten Vorbehalte, was den Vergleich mit Vorjahreszahlen betrifft, deutet dieser Anteil auf eine Zunahme gegenüber 2019 hin, als gemeldete Geschäftsbeziehungen zu solchen Verdachtsfällen nur gerade 2,4 Prozent ausmachten.
Im Berichtsjahr wurden in den Verdachtsmeldungen, bei denen Verbindungen zu einer kriminellen Organisation vermutet wurden, auch folgende andere mögliche Vortaten erwähnt: Bestechung fremder Amtsträger (111 Fälle), Betrug (72 Fälle), Geldfälschung (67 Fälle), Urkundenfälschung (26 Fälle) und Terrorismusfinanzierung (23 Fälle).

Andere Vortaten, die am häufigsten in den Verdachtsmeldungen mit Verdacht auf Zugehörigkeit zu kriminellen Organisationen genannt werden	Anzahl Erwähnungen	in %
Bestechung fremder Amtsträger	111	31,4
Betrug (Art. 146 StGB)	72	20,3
Geldfälschung	67	18,9
Urkundenfälschung	26	7,3
Finanzierung des Terrorismus	23	6,5
Betäubungsmittelgesetz	20	5,6
Veruntreuung	12	3,4
Ungetreue Geschäftsbesorgung	9	2,5
Erpressung	5	1,4
Waffengesetz	4	1,1
Diebstahl	2	0,6
Ungetreue Amtsführung	2	0,6
Aktive Bestechung schweizerischer Amtsträger	1	0,3

Im Berichtsjahr wurden die Meldungen, bei denen – unter anderem – Zugehörigkeit zu einer kriminellen Organisation als mutmassliche Tat erwähnt wurde, aufgrund der folgenden Verdachtsauslöser an die MROS übermittelt.

Verdachtsauslöser	Anzahl Erwähnungen	In %
Medien	168	47,5
Transaktionsmonitoring	115	32,5
Bartransaktion	82	23,2
Diverse	76	21,5
Information Dritte	42	11,9
Information Konzern	28	7,9
Information SVB	20	5,6
Eröffnung Geschäftsbeziehung	18	5,1
Kritische Länder	16	4,5

Die überwältigende Mehrheit (88,7 %) der Verdachtsmeldungen wegen Verbindungen zu einer kriminellen Organisation wurden der MROS von Banken übermittelt, gefolgt von Zahlungsverkehrsdienstleistern (2,82 %), Vermögensverwaltern / Anlageberatern (2,54 %) und Versicherungen (2,26 %). Die meldenden Finanzintermediäre lassen sich den folgenden Arten zuteilen:



256 der eingegangenen 354 Meldungen (also 73,2 %) waren nicht Gegenstand einer Anzeige seitens MROS an eine Strafverfolgungsbehörde und 24 sind noch in Bearbeitung. Die MROS hat ausgehend von 74 Meldungen 46 Anzeigen bei den zuständigen Strafverfolgungsbehörden erstattet. In acht Fällen wurde eine Nichtanhandnahmeverfügung erlassen; die restlichen 38 Fälle werden von den zuständigen Strafverfolgungsbehörden noch bearbeitet.

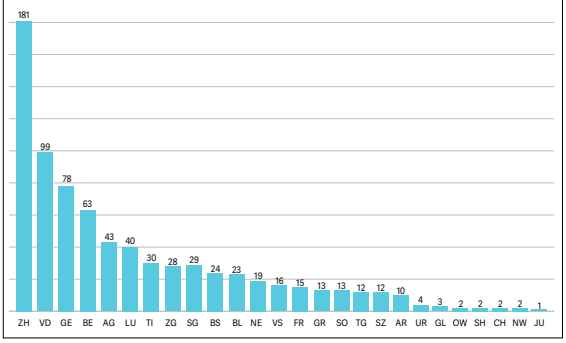
4.11 COVID-Pandemie

Die COVID-Pandemie prägte das Jahr 2020 und bot Kriminellen diverse Möglichkeiten sich unrechtmässig zu bereichern. Dadurch verschärfte sich auch das Risiko der Geldwäscherei. Unter den Verdachtsmeldungen bezüglich einer der verschiedenartigen Formen der Geldwäscherei, die im Berichtsjahr bei der Meldestelle eingegangen sind (siehe Kapitel 5.1), finden sich in den Statistiken der MROS auch Veruntreuung und betrügerischer Missbrauch von Krediten schweizerischer Finanzinstitute mit Bundesbürgschaft. Zwischen dem 25. März 2020, als der Bundesrat die Verordnung zur Kreditgewährung verabschiedet hat[15], und dem Jahresende 2020 registrierte die MROS 1046 Verdachtsmeldungen dieser Art. Sie betrafen 1054 COVID-Kredite von 43 Banken über eine Gesamtsumme von CHF 146 853 347.[16] Im Jahr 2020 erstattete die MROS 764 Anzeigen im Zusammenhang mit 914 Meldungen an eine Strafverfolgungsbehörde. 27 Meldungen betreffend COVID-Krediten waren am Ende des Berichtsjahrs noch in Bearbeitung.
Die nachfolgende Grafik zeigt, an welche Strafverfolgungsbehörden diesbezüglich wie viele Anzeigen von der MROS erstattet wurden. Darauf basierend eröffneten die Strafverfolgungsbehörden mehrere hundert Strafuntersuchungen, was die zentrale Rolle der MROS bei der Bewältigung dieser unerwarteten Entwicklung aufzeigt (siehe Kapitel 5.1).

[15] SR **951.261.** Die Verordnung wurde am 19. Dezember 2020 durch das Bundesgesetz über Kredite mit Solidarbürgschaft infolge des Coronavirus (Covid-19-Solidarbürgschaftsgesetz, Covid-19-SBüG; SR **951.26**) ersetzt.

[16] Vgl. Statistiken auf der Website der MROS: *Covid-19-Überbrückungskredite*.

Anzeigen im Zusammenhang mit COVID-Krediten an die zuständigen Strafverfolgungsbehörden 2020



Legende

AG	Aargau	**NW**	Nidwalden
AI	Appenzel Inner Rhodes	**OW**	Obwalden
AR	Appenzel Outer Rhodes	**SG**	St. Gallen
BE	Bern	**SH**	Schaffhausen
BL	Basel-Landschaft	**SO**	Solothurn
BS	Basel-Stadt	**SZ**	Schwyz
CH	Schweizerische Bundesanwaltschaft	**TG**	Thurgau
FR	Fribourg	**TI**	Ticino
GE	Geneva	**UR**	Uri
GL	Glarus	**VD**	Vaud
GR	Graubunden	**VS**	Valais
JU	Jura	**ZG**	Zug
LU	Lucerne	**ZH**	Zurich
NE	Neuchatel		

4.12 Anzeigen an die Strafverfolgungsbehörden

Im Jahr 2020 hat die MROS den Strafverfolgungsbehörden 1939 Anzeigen erstattet. Mit der am 1. Januar 2020 erfolgten Anpassung der MGwV werden keine Meldungen mehr an die Strafverfolgungsbehörden übermittelt. Um den Quellenschutz zu gewährleisten, werden auch keine Angaben zur Herkunft oder zum Verfasser der Verdachtsmeldung geliefert (Vgl. Art 8 Abs. 1 MGwV).[17] Die relevanten Informationen und die Einschätzung der MROS zu diesen Informationen werden vielmehr in Berichtsform elektronisch an die Staatsanwaltschaften übermittelt. Die Anzeigen an die Strafverfolgungsbehörden können Informationen aus verschiedenen Quellen und aus mehreren Verdachtsmeldungen enthalten (Vgl. Art. 1 Abs. 2 Bst. a–e MGwV). In der Praxis gibt es zwar weiterhin Fälle, bei denen eine Anzeige hauptsächlich auf den Informationen aus einer einzigen Verdachtsmeldung basiert, diese klassische Konstellation ist jedoch nicht mehr die Regel. Die Gesamtheit der Informationen, die der Meldestelle zur Verfügung stehen, entscheidet, ob Anzeige erstattet wird. Wie bereits im Jahresbericht 2019[18] angekündigt, hat die Weiterleitungsquote der Verdachtsmeldungen in ihrer alten Form damit ausgedient. Die erstatteten Anzeigen können Informationen aus diversen Quellen und mehreren Meldungen aus zuweilen unterschiedlichen Jahren enthalten. Daher können sie nicht mit der Anzahl Meldungen eines bestimmten Jahres in Beziehung gesetzt werden.

Die Anzeigen von 2020 enthalten Informationen aus

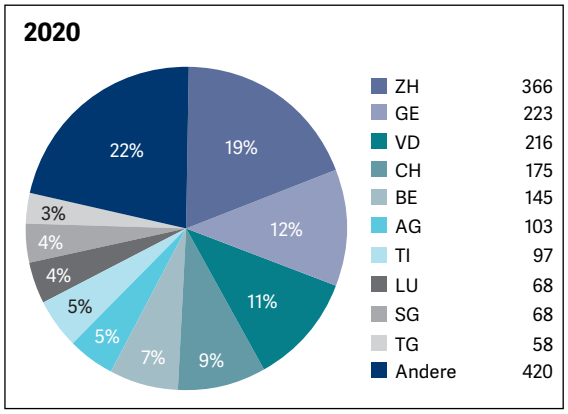
- 2156 Meldungen, die im Jahr 2020 eingegangen sind
- 179 im Jahr 2019 gemeldeten Geschäftsbeziehungen
- 52 im Jahr 2018 gemeldeten Geschäftsbeziehungen
- 12 im Jahr 2017 gemeldeten Geschäftsbeziehungen
- 3 im Jahr 2016 gemeldeten Geschäftsbeziehungen
- 1 im Jahr 2014 gemeldeten Geschäftsbeziehung
- 4 im Jahr 2011 gemeldeten Geschäftsbeziehungen

[17] Vgl. ebenfalls die *Erläuterungen zur Teilrevision der MGwV* vom 24. November 2019, S. 9f. sowie S. 16.

[18] Vgl. *MROS-Jahresbericht 2019*, S. 9.

Die Zahlen, die auf Verdachtsmeldungen mit Eingang nach dem 22. November 2019[19] zurückgehen – total 2 235 Fälle –, betreffen Meldungen, die sich auf mehrere Geschäftsbeziehungen beziehen können. Die Zahlen mit Bezug auf vorangehende Zeitspannen entsprechen jeweils einer Geschäftsbeziehung.

Betroffene Strafverfolgungsbehörden
Die folgende Grafik illustriert, an welche Strafverfolgungsbehörden die Anzeigen der MROS im Jahr 2020 ergangen sind.



Vergleiche mit den Vorjahren sind aus statistischen Gründen und aufgrund der unterschiedlichen Zählweise der Verdachtsmeldungen nicht aussagekräftig. Seit der Einführung des Informationssystems goAML, kann eine Anzeige auf mehreren Meldungen mit jeweils mehreren Geschäftsbeziehungen basieren, wobei die übermittelten Informationen auch ganz oder teilweise aus anderen Quellen als einer Verdachtsmeldung stammen können.
Zum ersten Mal war die Bundesanwaltschaft (BA) nicht die Strafverfolgungsbehörde, an welche die meisten Anzeigen der MROS gingen. 2020 gingen nur 9 Prozent der Anzeigen an die BA, während es 2019 noch 40 Prozent und 2018 49 Prozent waren. Dieser Rückgang muss indessen differenziert betrachtet werden: Der BA werden in der Mehrheit Fälle zur Anzeige gebracht, die Geldwäschereimeldungen im Zusammenhang mit Vortaten im Ausland betreffen. Dabei handelt es sich um Fälle von grösserer Komplexität, und die Informationen dazu stammen oft aus verschiedenen Meldungen betreffend mehrere Geschäftsbeziehungen. Die Übermittlungen an die kantonalen Strafverfolgungsbehörden gehen hingegen mehrheitlich auf eine einzige Verdachtsmeldung zurück.
An die Strafverfolgungsbehörden des Kantons Zürich gingen 2020 insgesamt weit mehr Anzeigen als an jene des Kantons Genf (19 % gegenüber 12 %) Bisher hatten die beiden Kantone etwa gleich viele Anzeigen der MROS zu behandeln, Genf sogar etwas mehr als Zürich.
Ein weiteres Novum stellt die Tatsache dar, dass mehr Anzeigen an die Strafverfolgungsbehörden der Kantone Waadt, Bern und Aargau gingen als an jene des Kantons Tessin.
Zusammengenommen erhielten die anderen 17 Kantone mehr Anzeigen der MROS als Zürich (420 gegenüber 366 Anzeigen). Dies steht im Kontrast zur Entwicklung bis 2019, als die 17 oder 18 Kantone mit der geringsten Anzahl jährlicher Anzeigen der MROS insgesamt kaum je mehr als 15 Prozent aller Meldungen auf sich vereinten.
Neben den Veränderungen, die auf die Einführung des Informationssystems goAML zurückzuführen sind und deshalb den Vergleich mit den Vorjahren erschweren, gehen die Entwicklungen auch auf die zahlreichen Verdachtsmeldungen an die MROS mit Bezug auf COVID-Kredite zurück. Dies erklärt auch teilweise den niedrigeren Prozentsatz bei den Anzeigen an die BA, da Letztere in der Regel nicht für solche Fälle zuständig ist. Ausserdem liefert dieser Umstand auch eine Erklärung dafür, weshalb die Kantone Waadt, Bern und Aargau mehr Anzeigen verzeichnet haben als das Tessin.

[19] Ab diesem Datum wurden die eingegangenen Meldungen im Informationssystem goAML der MROS erfasst. 76 der 179 im Jahr 2019 eingegangenen Meldungen hatten eine Anzeige der MROS an eine Strafverfolgungsbehörde zur Folge. Diese 76 Meldungen betrafen 153 Geschäftsbeziehungen; somit waren es insgesamt 256 Geschäftsbeziehungen, die 2019 bei der MROS gemeldet wurden und im Jahr 2020 zu einer Anzeige bei einer Strafverfolgungsbehörde geführt haben.

Zum Vergleich: Jahre 2011 bis 2020 (in %)

Behörde	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2020 in absolute numbers	Durchschnitt 2011–2020
ZH	19,7	14,4	18,4	12,4	13,5	12,0	10,2	12,8	14,3	18,9	366	14,7
GE	12,6	15,1	15,0	12,7	8,4	14,9	12,8	14,1	15,0	11,5	223	13,2
VD	4,7	2,1	2,4	2,5	2,6	3,1	1,8	4,3	5,5	11,1	216	4,0
CH	31,9	35,8	34,2	44,7	53,4	38,1	52,6	48,4	39,9	9,0	175	38,8
BE	3,2	3,8	1,6	4,6	1,8	3,0	1,6	1,8	3,3	7,5	145	3,2
AG	3,3	2,0	1,3	1,8	1,5	2,6	1,2	1,6	1,5	5,3	103	2,2
TI	8,5	13,6	12,5	7,3	6,5	6,0	6,0	3,3	3,3	5,0	97	7,2
SG	4,5	2,2	1,7	3,0	2,0	2,2	2,4	1,3	1,2	3,5	68	2,4
LU	0,6	1,1	1,5	1,8	1,0	1,4	1,4	0,8	1,8	3,5	68	1,5
TG	0,6	1,1	0,7	1,1	0,8	1,5	0,7	0,8	1,3	3,0	58	1,2
FR	0,7	1,2	0,5	0,2	0,6	0,6	1,4	1,6	1,5	2,7	53	1,1
VS	0,5	0,4	1,1	1,0	0,5	1,0	1,2	1,4	0,8	2,7	53	1,1
BS	3,4	2,7	2,2	1,2	1,3	3,3	2,0	0,9	0,9	2,6	50	2,0
ZG	1,3	0,6	1,2	1,3	1,5	1,2	0,6	1,9	1,9	2,5	49	1,4
NE	0,7	0,6	0,7	0,9	1,1	0,9	1,0	1,2	1,4	2,3	44	1,1
BL	0,5	1,3	0,8	0,5	1,5	1,5	1,2	0,8	2,9	2,1	41	1,3
SO	0,9	0,1	1,1	0,7	0,4	4,2	0,4	1,1	1,2	1,9	37	1,2
GR	0,5	0,5	0,9	1,0	0,6	0,3	0,5	0,3	0,4	1,5	29	0,7
SZ	0,6	0,6	0,6	0,2	0,5	0,8	0,5	0,3	0,4	1,0	20	0,6
AR	0,1	0,1	0,2	0,2	0,1	0,3	0,2	0,2	0,3	0,6	12	0,2
SH	0,5	0,4	0,6	0,3	0,1	0,5	0,3	0,1	0,3	0,5	10	0,4
UR	0,0	0,0	0,0	0,1	0,0	0,2	0,0	0,0	0,0	0,3	6	0,1
NW	0,3	0,0	0,4	0,1	0,1	0,0	0,0	0,7	0,2	0,3	5	0,2
JU	0,1	0,1	0,2	0,6	0,0	0,3	0,1	0,1	0,1	0,3	5	0,2
GL	0,0	0,0	0,1	0,0	0,0	0,1	0,1	0,2	0,0	0,2	3	0,1
OW	0,1	0,2	0,0	0,0	0,1	0,0	0,0	0,0	0,3	0,2	3	0,1
AI	0,1	0,1	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0	0,0
Total	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**0**	**100,0**

4.13 Pendente Meldungen aus den Jahren 2016–2019

Ende des Geschäftsjahrs 2019 waren 6 095 der MROS zwischen 2016 und 2019 gemeldeten Geschäftsbeziehungen noch im Stadium der Analyse (10 von 2016, 737 von 2017, 1 717 von 2018 und 3 631 von 2019). Im Berichtszeitraum unternahm die MROS besondere Anstrengungen, um diese gemeldeten Geschäftsbeziehungen zu bearbeiten. Die meisten dieser Fälle wurden nicht an eine Strafverfolgungsbehörde übermittelt (94,5 %), 4,9 Prozent wurden zur Anzeige gebracht. Ende 2020 sind nur noch 37 dieser Geschäftsbeziehungen (0,6 %) pendent. Weitere Einzelheiten dazu finden sich in der nachfolgenden Tabelle, geordnet nach Eingangsjahr der gemeldeten Geschäftsbeziehungen.

Eingangsjahr	2016	2017	2018	2019	Total
Keine Übermittlung	10	730	1,680	3,342	5,762
Anzeige		6	34	256	296
In Bearbeitung		1	3	33	37
Total	**10**	**737**	**1,717**	**3,631**	**6,095**

4.14 Austausch mit ausländischen Meldestellen (FIUs)

Im Kampf gegen die Terrorismusfinanzierung, die Geldwäscherei und deren Vortaten sowie die or-

ganisierte Kriminalität können die MROS und ihre ausländischen Partnerbehörden – die ausländischen FIUs – über das Instrument der internationalen Amtshilfe Informationen austauschen. Gehen bei der MROS Verdachtsmeldungen ein, die ausländische natürliche oder juristische Personen betreffen, kann die Schweizer Meldestelle bei den FIUs der entsprechenden Länder Informationen über diese Individuen oder Unternehmen einholen. Diese Informationen sind für die Analysen der MROS von grosser Bedeutung, denn die Mehrzahl der eingehenden Verdachtsmeldungen weisen einen Auslandsbezug auf. Umgekehrt gingen im Jahr 2020 bei der MROS 795 Anfragen aus 95 Ländern ein, was ein leichter Rückgang gegenüber dem Vorjahr darstellt (2019: 844 Anfragen aus 103 Ländern). 684 oder 86 Prozent dieser Anfragen konnte die MROS 2020 behandeln. Die Behandlung dieser Anfragen beanspruchte im Schnitt 41 Arbeitstage. 2020 beantwortete die MROS zudem 173 im Vorjahr eingegangene Informationsanfragen.
Im Jahr 2020 wurden Informationsanfragen aus dem Ausland über 5 212 natürliche und juristische Personen behandelt (2 733 natürliche und 2 479 juristische Personen). Davon waren 4 169 (2 155 natürliche und 1 994 juristische Personen) Gegenstand einer Informationsanfrage, die 2020 einging und im gleichen Jahr behandelt wurde.
Spontaninformationen sind Informationen einer ausländischen FIU, die eine Verbindung zur Schweiz aufweisen und keine Anfrage beinhalten, oder die umgekehrt von der MROS an eine ausländische FIU ergehen. Seit 2015 werden die im jeweiligen Jahr behandelten Spontaninformationen separat von den Informationsanfragen aufgeführt. Im Berichtsjahr gingen 504 Spontaninformationen aus 47 Ländern bei der MROS ein, die ihrerseits 365 solche Informationen an 76 ausländische FIUs sandte.
Im Jahr 2020 richtete die MROS 126 Informationsanfragen an 24 verschiedene ausländische FIUs. Diese Anfragen betrafen 364 juristische und 303 natürliche Personen. Die kontaktierten FIUs antworteten durchschnittlich innerhalb von 30 Tagen.

4.15 Austausch mit schweizerischen Behörden

Die MROS tauscht nicht nur mit ihren ausländischen Pendants Informationen aus, sondern auch mit anderen Behörden in der Schweiz, die im Kampf gegen die Geldwäscherei und deren Vortaten, die organisierte Kriminalität oder die Terrorismusfinanzierung tätig sind. Der Informationsaustausch zwischen der MROS und anderen schweizerischen Behörden richtet sich nach Art. 29 GwG. In den bisherigen Geschäftsberichten wurde keine Statistik zu diesem Austausch publiziert. Mittlerweile hat der Austausch innerhalb der Schweiz an Bedeutung gewonnen, sowohl in Bezug auf die Inhalte als auch die Arbeitsbelastung für die MROS.
Im Jahr 2020 wurde die MROS in 392 Fällen von insgesamt 26 Behörden um Informationen über bestimmte Personen oder Unternehmen im Rahmen von Untersuchungen zu Geldwäscherei, organisierter Kriminalität oder Terrorismusfinanzierung ersucht. In ungefähr 80 Prozent der Fälle kamen diese Anfragen von einer Kantonspolizei oder von der Bundeskriminalpolizei. Die 392 Informationsanfragen entsprechen einer Zunahme von mehr als 200 Prozent gegenüber den Vorjahren: 2018 und 2019 gab es je 117 solche Anfragen an die MROS.
Im Kampf gegen die Geldwäscherei und deren Vortaten, die organisierte Kriminalität und die Terrorismusfinanzierung ist die Rolle der MROS gegenüber anderen schweizerischen Behörden jedoch nicht auf die Beantwortung von Informationsanfragen beschränkt. Im Rahmen ihrer Analysen kann die MROS auch unaufgefordert Informationen an andere Behörden übermitteln, die in der Überwachung von Finanzoperationen und im Kampf gegen die Geldwäscherei, deren Vortaten, die organisierte Kriminalität oder die Terrorismusfinanzierung tätig sind. 2020 erfolgten 69 solche Spontaninformationen vonseiten der MROS. Die MROS kann auch für ihre Analysen bei anderen Bundes-, Kantons- und Gemeindebehörden Informationen anfragen. Solche Anfragen sind in den vorgängig aufgeführten Zahlen nicht erfasst.

5. Typologien (zur Sensibilisierung der Finanzintermediäre)

Die nachfolgenden Typologien beziehen sich bewusst nicht auf repräsentative Verdachtsmeldungen des Jahres 2020, sondern auf Sachverhalte, die – mit Ausnahme der Fälle rund um die COVID-Pandemie (siehe Kapitel 5.1) – vergleichsweise selten gemeldet werden. Im Jahr 2020 entsprachen beispielsweise Verdachtsmeldungen in Zusammenhang mit kriminellen Organisationen und Terrorismusfinanzierung nur gerade 7,8 % der gesamten Anzahl von den an die MROS abgesetzten Verdachtsmeldungen. Beides sind Deliktsfelder, welche im Fokus der Strategie Kriminalitätsbekämpfung 2020–2023 vom EJPD stehen.
Diese Typologien zeigen anhand konkreter Beispiele, wie die Erträge aus den mutmasslichen Straftaten gewaschen werden. Die ausgewählten Fälle reflektieren auch die neuen Tendenzen und verwendeten Methoden. Daneben werden zusammenhängende Rückschlüsse gezogen. Diese Typologien dienen der Sensibilisierung der Finanzintermediäre indem aufgezeigt wird, welche Kontoarten, Finanzinstrumente und Verhaltensmuster gemäss den von der MROS festgestellten Risiken mehr Aufmerksamkeit erfordern.

5.1 Fälle rund um die COVID-Pandemie

Ein wesentlicher Teil der Zunahme der Zahl der bei der MROS im Jahr 2020 eingegangenen Verdachtsmeldungen – nahezu ein Drittel der im Berichtsjahr erstatteten Meldungen – ist auf Geldwäschereiverdachtsfälle zurückzuführen, die einen Bezug zur COVID-Pandemie aufweisen. Die besondere Situation, die durch die Pandemie entstanden ist, hat Kriminellen eine Reihe von Möglichkeiten zur illegalen Bereicherung eröffnet und damit das Risiko der Geldwäscherei erhöht. Die auf internationaler Ebene identifizierten Risiken im Zusammenhang mit der Bekämpfung von Geldwäscherei, kriminellen Organisationen und Terrorismusfinanzierung sind sehr unterschiedlicher Natur.[20] Das Spektrum reicht von der Veruntreuung von Geldern, die von staatlichen oder supranationalen Organisationen für den Kampf gegen die Pandemie zur Verfügung gestellt werden, über Risiken durch die Zunahme von Cyberkriminalität, die durch das weit verbreitete Arbeiten im Home Office noch zusätzlich akzentuiert werden, bis zu Risiken im Zusammenhang mit Betrügereien bei der Vermarktung von Sanitätsartikeln und mit der Infiltration illegaler Vermögenswerte in die in Schwierigkeiten geratenen Wirtschaftssektoren. Zur Prävention machte die MROS am 2. und 29. April 2020 ausserdem die Schweizer Finanzintermediäre via goAML über die mit der Pandemie beziehungsweise mit der Vergabe von COVID-Krediten verbundenen Risiken aufmerksam.
Unter den bei der MROS eingegangenen Verdachtsmeldungen haben sich drei spezifische Geldwäschereirisiken herauskristallisiert, die sich mit der aufkommenden Pandemie abzeichneten. Das erste betrifft die Veruntreuung oder

[20] Seit dem Frühjahr 2020 haben mehrere nationale und internationale Organisationen Analysen und Warnungen zu diesem Thema veröffentlicht. Siehe dazu beispielsweise die FATF-Publikation vom Mai 2020 (im Dezember aktualisiert): www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html.

den Missbrauch von Darlehen, die Unternehmen unter der Garantie der öffentlichen Hand gewährt wurden. Am 25. März 2020 verabschiedete der Bundesrat eine Notverordnung zur Gewährung von Krediten mit Solidarbürgschaft des Bundes. Einzelunternehmen, Personengesellschaften oder juristische Personen mit Sitz in der Schweiz sollten so von schweizerischen Kreditinstituten zu vorteilhaften Bedingungen vom Bund abgesicherte Kredite erhalten.[21] Diese Verordnung wurde am 19. Dezember 2020 durch das Bundesgesetz über Kredite mit Solidarbürgschaft infolge des Coronavirus (Covid-19-SBüG)[22] ersetzt. Das Risiko, dass diese Kredite veruntreut werden, liegt auf der Hand. Alarmiert durch Bargeldbezüge, Transfers auf persönliche Konten von Geld, das aus diesen Krediten stammte, sichtlich gesteigerte Umsätze oder die Verwendung von Krediten entgegen den in der Bundesratsverordnung festgelegten Bedingungen, erstatteten Finanzintermediäre im Laufe des Jahres 2020 mehr als tausend Verdachtsmeldungen im Zusammenhang mit 1100 Krediten.[23] Die MROS leitete über 800 Verdachtsmeldungen an die zuständigen Strafverfolgungsbehörden weiter, insbesondere wegen Verdachts auf Betrug und/oder Urkundenfälschung und unlautere Geschäftsführung. Im Anschluss daran eröffneten die Strafverfolgungsbehörden mehrere hundert Strafuntersuchungen.
Eine andere von der Pandemie begünstigte Form der Wirtschaftskriminalität betrifft Internet-Betrügereien wie *Phishing* oder *Social Engineering*. Zwar weisen die Vortaten nicht zwangsläufig einen unmittelbaren Bezug zur COVID-Pandemie auf, sind aber aufgrund der in zahlreichen Ländern angeordneten Lockdowns vermehrt aufgetreten. In ihrer Bewegungsfreiheit eingeschränkt sahen sich auch Menschen praktisch dazu gezwungen, sich des Internets zu bedienen, die es für gewöhnlich eher nicht nutzen. Ungewohnt im Umgang mit dem Internet, fallen diese Menschen entsprechend leicht Betrügereien zum Opfer. Die Zunahme von Internet-Betrügereien – nicht ein allein auf die Schweiz beschränktes Phänomen – hat zu einer leicht erhöhten Zahl an die MROS gerichteter Verdachtsmeldungen in diesem Zusammenhang geführt.
Während die Summen bei Internet-Betrugsfällen in der Regel bescheiden sind, ist dies bei den Delikten, die im Rahmen des Handels mit Sanitätsartikeln begangen werden, nicht der Fall. Hier geht es meist um mehrere Millionen Franken. Massenbestellungen von Atemschutzmasken, hydroalkoholischer Flüssigkeit oder anderen Sanitätsprodukten durch staatliche Behörden und bisweilen auch durch private Unternehmen wurden in einer Notsituation aufgegeben, die Missbrauch und manchmal auch Betrug begünstigt hat. Das verkaufte Produkt kann unbrauchbar, von schlechter Qualität oder der Preis überhöht sein oder man wartet vergeblich auf die Lieferung. Darüber hinaus hat die durch die Pandemie ausgelöste Angst die Bevölkerung häufig dazu verleitet, sich solche Produkte selbst zu beschaffen, oft über das Internet. Vermehrt werden mit irreführender Werbung in betrügerischer Weise die Vorzüge von Medikamenten angepriesen, die angeblich eine Ansteckung mit dem Virus verhindern. Fälle dieser Art umfassen ein paar Dutzend Meldungen. Sie betreffen häufiger den Verdacht auf Betrug im Ausland als in der Schweiz. Die Hauptelemente, die Anlass für einen Verdacht gegeben haben, sind Verträge zweifelhafter Authentizität, die als Beleg für die Transaktionen vorgelegt werden, der plötzliche Wechsel des Tätigkeitsfeldes von Unternehmen, die zuvor nicht mit Sanitätsprodukten gehandelt haben, die verdächtige Zunahme der Zahl von Händlern zwischen dem Lieferanten und dem Käufer, aber auch Presseartikel, die sich gegen Unternehmen richten, die zu hohe Preise für die gelieferten Produkte verlangen, oder Forderungen nach Rückgabe von Geldern von den Banken der geschädigten Käufer.

---

[21] Vgl. Fussnote 15

[22] Vgl. Fussnote 15

[23] Vgl. die zu diesem Thema auf der MROS-Internetseite veröffentlichten Statistiken: *COVID-19-Überbrückungskredite.*

Vermeintliche Geldwäscherei im Rahmen der Vermarktung von Sanitätsprodukten
Ein Finanzintermediär stellt auf einer Geschäftsbeziehung im Namen einer Domizilgesellschaft, ansässig in einer pazifischen Gerichtsbarkeit, drei Zahlungseingänge aus einem Drittland in der Höhe von insgesamt mehreren zehn Millionen Franken fest. Die betreffende Domizilgesellschaft gehört einem europäischen Staatsbürger, der im Rohstoffsektor tätig und in einem Golfstaat ansässig ist. Gemäss dem Kunden würden diese Mittel dem Verkauf von 10 Millionen medizinischen Atemschutzmasken entsprechen, einer Menge, die den Bedarf eines Staates deckt. Die Mittel stammen von einem Konto, das auf den Namen einer öffentlichen Einrichtung eröffnet wurde. Der Kunde agiere angeblich als Vermittler zwischen der Regierung und ausländischen Lieferanten. Ein Teil der auf dem Konto eingegangenen Beträge wird kurz darauf auf verschiedene Bankverbindungen im Land dieser Lieferanten überwiesen. Der Finanzintermediär stellt mehrere Unstimmigkeiten zwischen den vom Kunden erhaltenen Informationen und der im Bestellerstaat vorherrschenden Lage fest. Ihm kommen Zweifel an der Plausibilität der geschäftlichen Transaktionen auf und er vermutet Betrug oder unlautere Geschäftsführung und betrügerische Handlungen gegen öffentliche Interessen. Die von der MROS vorgenommenen Abklärungen ergaben, dass die fragliche Transaktion trotz ihrer Ungewöhnlichkeit ordnungsgemäss bewilligt worden war und die bestellten Atemschutzmasken auch tatsächlich geliefert wurden. Die FIU des Landes, in dem die Masken bestellt worden waren, wurde über den ungewöhnlichen Charakter dieser Transaktion informiert.

Neben diesen drei Arten von Risiken im Zusammenhang mit der COVID-Pandemie, die sich in den von der MROS erhaltenen Mitteilungen widerspiegeln, wurden weitere Risiken identifiziert, deren Intensität jedoch schwer zu beziffern ist. Dies gilt insbesondere für Geldwäscherei, die von kriminellen Organisationen begangen wird, die die aktuelle Gesundheitskrise und ihre wirtschaftlichen Folgen ausnutzen, um ihren Einfluss auszuweiten, indem sie beispielsweise verschuldete Schweizer Unternehmen oder Immobilien von finanziell angeschlagenen juristischen oder natürlichen Personen erwerben. Mehrere internationale Einrichtungen haben auf dieses erhöhte Risiko der Unterwanderung der Wirtschaft durch kriminelle Organisationen hingewiesen – ein Risiko, das auch in zahlreichen Recherchen von Journalisten dokumentiert wurde. Die MROS erhielt indessen lediglich zwei Verdachtsmeldungen, die einen Bezug zu diesem Risiko erkennen liessen. Es ist jedoch anzumerken, dass in einigen Fällen die gemeldeten Kreditbetrügereien anscheinend von miteinander verbundenen Personen oder zumindest mit einem ähnlichen Modus Operandi begangen wurden. Zum jetzigen Zeitpunkt liegen der MROS jedoch keine Hinweise auf die Beteiligung bekannter krimineller Organisationen an solchen Machenschaften vor.

Ein COVID-Kredit für die Firma einer Person, die einer kriminellen Organisation angehört?
Ein Finanzintermediär stellt fest, dass ein in der Fahrzeugwartung und –reparatur tätiges Unternehmen einen COVID-Kredit beantragt hatte und daraufhin ein Privatdarlehen zurückzahlte– was nach Art. 2 Abs. 2 Bst. b des Covid-19-SBüG verbotenen ist. Bei weiteren Abklärungen stösst der Finanzintermediär auf Presseartikel, welche die Verhaftung des Firmeninhabers in einem Drittland wegen Mitgliedschaft in einer kriminellen Organisation erwähnen. Die betroffene Geschäftsbeziehung weisst hauptsächlich Bareinlagen und Transaktionen mit Konten Dritter auf, die im erwähnten Drittland eröffnet wurden. Es handelt sich um Summen von mehreren zehntausend Franken.

5.2 Kriminelle Organisationen

Die bisher der MROS gemeldeten Sachverhalte in Zusammenhang mit kriminellen Organisationen deuten darauf hin, dass Presseartikel oder Einträge aus privaten Datenbanken am häufigsten die Verdachtsmomente der meldenden Institute begründen.
Die Konten von Mitgliedern von kriminellen Organisationen weisen oftmals keine auffälligen Transaktionen / Transaktionsmuster auf und werden somit auch nicht als «verdächtig»qualifiziert und somit nicht gemeldet.
Die Gründe, warum die Finanzintermediäre Angehörige einer mutmasslichen kriminellen Organisation i. S. v. Art. 260ter StGB nur schwer erkennen, sind wahrscheinlich mannigfaltig. So dürfte die Verschiebung von inkriminierten Geldern in bar ebenso eine Rolle spielen, wie der Umstand, dass die Geldtransaktionen unter einem gewissen Schwellenwert bleiben. Zudem sind die gemeldeten Firmen oft in einem Bereich tätig, wo Bartransaktionen bis zu einem gewissen Grad charakteristisch sind (Restauration, Garagen, etc.). Allerdings könnten auch andere Sektoren (wie z. B. Intermediation im Immobilienbereich, Baugewerbe, etc.) betroffen sein.

Zugehörigkeit zu einer kriminellen Organisation und Bartransaktionen
Im Jahr 2020 meldete ein Finanzintermediär zwei Kreditkartenanträge nach Art. 9 Abs. 1 Bst. b GwG (versuchte Geldwäscherei), aufgrund eines World-Check Eintrags einer der beiden Antragssteller. Gemäss diesem Eintrag sollte einer der beiden Antragssteller Mitglied der kriminellen Organisation «'Ndrangheta» sein. Die Kreditkarten beider Antragsteller sollten über dasselbe Firmenkonto, einer Eisdiele, laufen. Beide Antragssteller seien in einem Schweizer Kanton wohnhaft, wobei die Gesellschaft ihren Sitz in einem Grenzkanton hat.
Gestützt auf die Informationen in der Meldung war es der MROS möglich, die nach Art. 11a Abs. 2 und 3 GwG notwendigen Informationen zu den Bankkonten der natürlichen Personen und das Bankkonto der Eisdiele einzufordern. In der Folge reichte der ersuchte Finanzintermediär ebenfalls eine Verdachtsmeldung ein, insbesondere gestützt auf öffentlich zur Verfügung stehende Quellen sowie auf die Anfrage der MROS.
Die MROS-Analyse in Bezug auf die untersuchten Bankbeziehungen ergab nachfolgendes Bild:
80 % der gemeldeten Geschäftsbeziehungen wiesen ungewöhnlich häufig Einzahlungen in bar auf. Alle Inhaber der gemeldeten Gesellschaften oder Vertragspartner besitzen die italienische Staatsangehörigkeit. 80 % der Geschäftsbeziehungen wiesen mehrere Transaktionen entweder von oder nach Italien auf.
Über das Transaktionsverhalten konnte die MROS weiter feststellen, dass 60 % der Geschäftsbeziehungen eine Verbindung entweder zu Kalabrien oder zu Neapel in Italien aufwiesen.
Darüber hinaus ergab die Auswertung der Kontounterlagen der Eisdiele, dass diese wahrscheinlich nicht operativ tätig war. Im Laufe der Pandemie wurde diese anscheinend – gemäss Aussagen des Besitzers – neu auf die Restauration ausgerichtet.

Wie oben aufgezeigt wurde, gibt es aber Faktoren, die kumulativ betrachtet ein Zeichen sein können, dass über eine Geschäftsbeziehung inkriminierte Gelder fliessen. Vor allem das Zusammenspiel von Bartransaktionen, nicht operativ tätigen Gesellschaften und spezifische auf die jeweilige kriminelle Organisation bezogene Risikofaktoren (wie im Beispiel oben der Bezug zu Kalabrien in Italien), können als Wegweiser dienen, um Konten von möglichen Mitgliedern einer kriminellen Organisation zu ermitteln.

5.3 Terrorismusfinanzierung

Die Attraktivität von Kryptowährungen für die Terrorismusfinanzierung
Ein Finanzintermediär stellt seinen Kunden die Dienstleistung Crypto ATM zur Verfügung. Dieser Service macht es möglich, dass Schweizer Franken an einem Bankomaten einbezahlt und anschliessend vom anbietenden Finanzintermediär in Bitcoin umgetauscht werden. Für den Umtausch der CHF in Bitcoin arbeitete dieser Finanzintermediär mit einer südeuropäischen Börse für Kryptowährungen zusammen. Diese Börse machte den Finanzintermediär darauf aufmerksam, dass eine Transaktion von BTC 0,00897707 (CHF 100) aus der Schweiz an eine Bitcoinadresse getätigt wurde, welche der Gruppierung Al-Qaïda zuzuordnen sei. Diese Bitcoinadresse sei Gegenstand von Untersuchungen einer Staatsanwaltschaft in einem Drittland gewesen.
Der an die MROS gemeldete Überweiser konnte durch die Einzahlung am Crypto ATM anonym bleiben und musste nur eine Kontaktinformation angeben. Die MROS konnte den Überweiser aufgrund dieser Angabe jedoch identifizieren. Abklärungen zur Person zeigten, dass diese vor vier Jahren in sozialen Medien durch das Teilen von gewalttätiger jihadistischer Propaganda aufgefallen war. Neben der bereits erwähnten Transaktion wurden im Rahmen der Transaktionsanalyse weitere 17 Transaktionen – im Gesamtwert von fast CHF 3 000 – an dieselbe Bitcoin-Adresse identifiziert. Die Adresse soll gemäss einem Blockchain-Analysetool zum al Qaeda Bitcoin Transfer Office gehören.

Der vorliegende Fall zeigt exemplarisch auf, dass terroristische Gruppierungen auch neue Technologien für ihre Finanzierung verwenden. Die Überwachung und auch die nachträgliche Verfolgung von Kryptotransaktionen sowie die damit zusammenhängenden Abklärungen i. S. v. Art. 6 Abs. 2 GwG sind eine wichtige Aufgabe der Finanzintermediäre. Das vorliegende Beispiel zeigt ausserdem, dass eine einfache Kontaktangabe für die MROS entscheidend war, damit sie die nötigen Verbindungen feststellen konnte.

Fokussierung auf die Angaben zu den Geldüberweisern / Geldempfängern statt den Beträgen
Ein in der Schweiz bewilligter Finanzintermediär erhielt über seine ausländische Muttergesellschaft Informationen einer ausländischen Strafverfolgungsbehörde, wonach bestimmte Personen angeblich verdächtige Transaktionen zwecks Terrorismusfinanzierung über den Finanzintermediär tätigten.
Die Arbeit der MROS wurde durch die vom Finanzintermediär gut dokumentierte Analyse der Transaktionen und der involvierten Personen erheblich erleichtert. In der Meldung wurden auch die Geldempfänger namentlich erwähnt, was der MROS weitere Anhaltspunkte lieferte. Dabei wurde ersichtlich, dass zwei Personen aus dem gewaltbereiten islamistischen Kreis, wovon einer mit einem schweizerischen Foreign Terrorist Fighter verwandt ist, Beträge im drei- bis vierstelligen Bereich insbesondere in zwei südosteuropäische Länder, aber auch in ein asiatisches Land überwiesen, wo der Bruder der einen Person die Geldüberweisungen entgegennahm. Ein weiterer Geldempfänger hatte sich gemäss öffentlichen Medienquellen bereits in einem kritischen Land aufgehalten und wurde nach seiner Rückkehr von einem Gericht verurteilt.

Das Transaktionsmuster ist charakteristisch für die zwei Formen der Terrorismusfinanzierung gemäss FATF[24], welche auch in der Schweiz seit mehreren Jahren vorkommen, aber immer noch häufig unentdeckt bleiben. Die eine Form betrifft die Überweisung von Geldmitteln aus einem Land an teilweise sogar medial bekannte Extremisten, welche diese im Empfängerland entweder für ihren Lebensunterhalt verwenden oder allenfalls für die Planung von Anschlägen

[24] Vgl. die Publikation der FATF *Terrorist Financing Risk Assessment Guidance.*

weiterüberweisen. Die zweite in diesem Fall erkennbare Form ist, dass Geldmittel, welche mutmasslich für extremistisch motivierte Anschläge aufgewendet werden können, über verschiedene Länder weitertransferiert werden, um den Ursprung der Finanzierungsquelle zu verschleiern. Die Schweiz ist in einer solchen (Geld)überweisungs-Kette Ausgangspunkt oder lediglich Zwischenstation. Aufgrund der sehr niedrigen Beträge, die im Rahmen von Überweisungen bei Zahlungsverkehrsdienstleistern oder auch ab Retail-Konten keinen Verdacht erwecken, bleiben solche Zahlungen schwierig zu entdecken. Der Hauptgrund dafür ist, dass bei der Transaktionsüberwachung häufig vor allem die Höhe der überwiesenen Beträge im Fokus steht. Während dies für die Entdeckung von Transaktionsflüssen im Rahmen von mutmasslichen Geldwäschereihandlungen der richtige Ansatz sein mag, kann Terrorismusfinanzierung vor allem dann erkannt werden, wenn man die Geldüberweiser und -empfänger genauer unter die Lupe nimmt.

5.4 Menschenhandel

Smurfing, Rotlichtmilieu, Risikoländer und präzise Angaben über Geldempfänger

Ein Zahlungsverkehrsdienstleister meldete innert einer Zeitspanne von zwei Monaten fünf individuelle Kundenbeziehungen, welche Überschneidungen im Transaktionsmuster sowie bei den demografischen Merkmalen der involvierten Personen (z. B. Alter, Geschlecht, Herkunft, Beruf, etc.) aufwiesen und Hinweise auf Menschenhandel (Art. 182 StGB) und/oder Förderung der Prostitution (Art. 195 StGB) beinhalteten.

*Die fünf gemeldeten Kundinnen tätigten mehrfache, identisch hohe Zahlungen im selben Zeitraum an verschiedene Privatpersonen, die diese Zahlungen in einem karibischen und einem europäischen Staat entgegennahmen. Es ist davon auszugehen, dass dabei darauf geachtet wurde, die Zahlungen aufzuteilen, um die Grenze von CHF 5 000 nicht zu überschreiten, beziehungsweise um vertiefte Abklärungspflichten zu vermeiden. Teilweise konnten bei den Zahlungen der verschiedenen Kundinnen Übereinstimmungen bei den Zahlungsempfängern*innen festgestellt werden. Somit konnte der Finanzintermediär eine eindeutige Verbindung zwischen den verschiedenen Kundenbeziehungen herstellen. In einem Fall wurde zwischen den gemeldeten Kundinnen eine Zahlung getätigt, welche danach in dasselbe karibische Land weitervergütet wurde.*

Die Mehrheit der Kundinnen arbeitet im Rotlichtmilieu oder hat Verbindungen dazu. Mit wenigen Ausnahmen wurden alle Zahlungen von derselben Agentur in der Nähe eines bekannten Schweizer Rotlichtviertels getätigt. Der meldende Finanzintermediär hat über die einzelne Kundenbeziehung hinaus Transaktionsmuster untersucht und verfolgt und so wichtige Verbindungen zwischen oberflächlich betrachtet unzusammenhängenden Geschäftsbeziehungen entdeckt.

Dadurch, dass der Finanzintermediär für alle beteiligten Personen Name, Vorname, Geburtsdatum und Adresse übermittelte, konnte die MROS vertiefte und gezielte Personenrecherchen durchführen und so verschiedene Elemente identifizieren, welche den Verdacht des Finanzintermediärs erhärteten. Insbesondere die detaillierten Angaben zu den Geldempfängern im Ausland ermöglichten es der MROS, gezielte Ersuchen an ausländische Meldestellen zu richten – eine Massnahme, die bei transnationalen Verbrechen wie Menschenhandel essentiell sein kann.

Im vorliegenden Fall haben zwei Kundinnen Adressen angegeben, welche sich in einem Rotlichtviertel befinden. Bei zwei weiteren, von den Kundinnen angegebenen Adressen, handelte es sich um Falschadressen. Dies lieferte einen weiteren Hinweis darauf, dass die getätigten Überweisungen möglicherweise deliktischen Ursprungs waren. Die Herkunftsländer der potentiellen Opfer bzw. die Nationalität einiger der Vertragspartnerinnen werden in Kombination mit anderen Elementen, als Hochrisikoländer betrachtet.

Der meldende Finanzintermediär bezieht sich in seiner Analyse auf verschiedene Indikatoren, welche gemäss dem 2019 erschienenen Bericht der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) *Following the Money:*

Compendium of Resources and Step-by-step Guide to Financial Investigations Into Trafficking in Human Beings[25] indikativ sind für mögliche Aktivitäten bzw. Handlungen im Bereich des Menschenhandels:

- Verwendung von Adressen in bekannten Rotlichtvierteln oder Gebäuden, in denen bekanntermassen kommerzielle Sexarbeit stattfindet;
- Verwendung von Strohpersonen;
- Nutzung von Instituten, die nicht zum traditionellen Finanzsystem gehören;
- Überweisungen aus verschiedenen Regionen an dieselben Personen in Ländern, von denen bekannt ist, dass sie ein höheres Risiko für Menschenhandel darstellen;
- Strukturierte Überweisungen *Smurfing*;
- Hohe und/oder häufige Zahlungen [...], die nicht mit dem persönlichen Gebrauch oder dem angegebenen Geschäft des Einzelnen vereinbar sind (Geld wird von einem Dritten genutzt).

Für die komplette Auflistung der verschiedenen, vom OSZE Sonderbeauftragten und Koordinator für die Bekämpfung des Menschenhandels zusammengeführten Indikatoren sowie Mittel zu Finanzanalysen im Bereich des Menschenhandels, verweisen wir auf die besagte Publikation der OSZE.

5.5 Meldungen in Zusammenhang mit Virtual Asset Service Providers (VASPs)

Phishing-Betrüger nutzen schweizerische Kryptowährungsbörse zum Waschen betrügerisch erlangter Vermögenswerte

Ein Finanzintermediär meldete das Geschäftskonto einer schweizerischen Kryptowährungsbörse, auf welches innerhalb weniger Tage insgesamt etwa CHF 30 000 an Kundengeldern von diversen Banken eingegangen sind. Die Kunden dieser Finanzinstitute wurden mittels fingierten E-Mails dazu gebracht, ihre persönlichen Zugangsdaten fürs E-Banking offenzulegen (sog. Phishing). Die entsprechenden Zahlungsaufträge wurden dann von unbekannten Dritten ausgelöst. Die Finanzinstitute, deren Kunden von den Phishing-Attacken betroffen waren, setzten den meldenden Finanzintermediär über Gelder aus Staftaten in Kenntnis. Daneben meldete auch die schweizerische Kryptowährungsbörse an die MROS den Kauf von Bitcoins auf ihrer Handelsplattform, welcher mit diesen Geldern getätigt wurde. Diese teilte der MROS die involvierten Bitcoinadressen sowie die IP-Adressen der mutmasslichen Täter mit, welche die Käufe in Auftrag gegeben hatten. Diese Transaktionen wurden über einen sog. API (Application Programming Interface, d. h. eine Softwareschnittstelle) getätigt, welche die Kryptowährungsbörse auf ihrer Website den Kunden zur Verfügung stellt. Dabei dient der API als Softwareschnittstelle mit Verbindung zur Handelsplattform der Börse und erlaubt den Kunden vereinfachte und automatisierte Kauf-/Verkaufstransaktionen bis zu CHF 5 000 pro Tag, ohne dass die Kunden bei ihrer Registrierung detaillierte Angaben zu ihrer Identität machen müssen. Die Börse verlangt bei Kauf-/Verkaufstransaktionen über seinen API vom Kunden lediglich die Angabe eines Mittelherkunftskontos, das im Normalfall unter der Kontrolle des legitimen Auftraggebers steht, sowie eine Kryptowährungsadresse, an welche die gekauften Kryptowährungen überwiesen werden sollen. Beim Abschluss eines über die Softwareschnittstelle generierten Kaufauftrags erhalten die Kunden eine Referenznummer, welche sie bei der Banküberweisung auf das Geschäftskonto der Börse angeben müssen. Sämtliche Kaufaufträge erfolgten genau in der Höhe von CHF 5 000 oder knapp darunter (sog. Smurfing), sodass die Kryptowährungsbörse von den Auftraggebern keine weitere Know Your Customer (KYC)-Dokumente verlangte.

[25] Vgl. die Publikation der OSZE auf folgender Internetseite: https://www.osce.org/cthb/438323 (Dokument auf Englisch).

Betrügerisch erlangte Kryptoassets über eine schweizerische Kryptowährungsbörse gewaschen

2019 erfolgte ein Cyberangriff auf eine ausländische Kryptowährungsbörse, wobei Vermögenswerte in Form der Kryptowährung «F» im Wert von mehreren Millionen Schweizerfranken gestohlen wurden. Von den mutmasslichen Tätern wird vermutet, dass sie einer Hackergruppe angehören. Um ihre Spuren zu verwischen, tauschten die Hacker die gestohlenen Kryptomittel in Bitcoin um (sog. Chain-Hopping, d. h. der Wechsel von der «F»-Blockchain auf die Bitcoin-Blockchain, welcher die Rückverfolgbarkeit mittels Tracing Software erschwert). Dafür wählten sie scheinbar gezielt Kryptowährungsbörsen auf der ganzen Welt aus, welche für einen solchen Umtausch ein vereinfachtes Kundenidentifizierungs-Verfahren anwendeten, also bei der Registrierung des Kunden lediglich dessen E-Mailadresse oder Telefonnummer verlangten, sofern die umgetauschten Vermögenswerte eine gewisse Wertgrenze nicht überschreiten. Die Täter spalteten die gestohlene Menge an «F» in kleine Beträge auf und sendeten diese über unzählige «F»-Adressen (sog. Hops), bevor sie auf den verschiedenen Kryptowährungsbörsen für den Umtausch deponiert wurden. Auf diese Weise konnten sie einerseits die Nachverfolgung erschweren und gleichzeitig die Frühwarnsysteme der Kryptowährungsbörsen umgehen, da nun nicht mehr direkt ersichtlich war, dass es sich um die gestohlenen Kryptomittel aus der Hacking Attacke handelte.

Auch in diesem Fall wurde die bereits erwähnte Softwareschnittstelle API einer Schweizer Kryptowährungsbörse missbraucht. Die Täter erstellten bei der besagten Börse mehrere Konten und wechselten die erbeuteten Einheiten der Kryptowährung «F» in Bitcoin um, wobei sie darauf achteten, den jeweiligen Gegenwert von CHF 5 000 nicht zu überschreiten, um nicht vertieften KYC-Anforderungen zu unterliegen. Die Kryptowährungsbörse war nun im Besitz dieser Einheiten der Kryptowährung «F», deren Spur(en) sich auf der betroffenen Blockchain mittels Tracing-Software trotz aller Bemühungen der Täter auf den Cyberangriff auf den ausländischen Kryptowährungshandelsplatz zurückverfolgen liess. Die Bitcoins, welche die Kryptowährungsbörse den Cyberkriminellen zum Umtausch überwies, weisen auf der Bitcoin-Blockchain jedoch keinen Bezug zum Angriff auf den ausländischen Handelsplatz auf, sondern lediglich zur schweizerischen Börse. Nach Entdeckung dieses Missbrauchs konnte die betroffene schweizerische Kryptowährungsbörse einige ausgehende Bitcoin-Transaktionen stoppen, und meldete den Vorfall der MROS.

Im Jahr 2019 wurden mehr Kryptowährungsbörsen *gehackt* als in jedem anderen Jahr zuvor.[26] Da Kryptowährungen (z. B. Bitcoin) direkt zwischen Sender und Empfänger weltweit und relativ anonym transferiert werden können, spielt es keine Rolle, wo auf der Welt eine Börse *gehackt* wird – die inkriminierten Kryptowährungen können innerhalb von wenigen Sekunden auf einem anderen Finanzplatz landen und über diesen gewaschen werden.

Diese zwei Fälle zeigen auf, wie wichtig *Smurfing* und die Umgehung von Identifikationspflichten[27] in Zusammenhang mit VASPs sind. Zur Vorbeugung solcher Vorfälle ist der Einsatz von Tracing-Software notwendig, welche es erlaubt, Transaktionen zurückzuverfolgen. Hacker versuchen wiederum, diese Frühwarnsysteme zu umgehen, indem sie Kryptowährungen mit kriminellem Ursprung über mehrere Kryptowährungsadressen

[26] Vgl. die Publikation vom Januar 2020 von Chainalysis *The 2020 State of Crypto Crime.* Zahlenmässig gab es 2019 mehr *Hacks* von Kryptobörsen als in jedem Jahr zuvor (Chainalysis zählt 11 Hacks für das Jahr 2019), die Summe der dabei erbeuteten Vermögenswerte ist allerdings kleiner als in den vorangehenden Jahren (2019: USD 282,6 Mio.; 2018: USD 875,5 Mio.; 2014: USD 483,1 Mio).

[27] Es ist allerdings darauf hinzuweisen, dass mit dem am 1. Januar 2021 in Rechtkraft getretenen Art. 51a Geldwäschereiverordnung-FINMA vom 3. Juni 2015 (GwV-FINMA, SR **955.033.0**) der Schwellenwert für Wechselgeschäfte in Kryptowährungen von derzeit CHF 5 000 auf CHF 1 000 gesenkt- und somit eine Mitte 2019 publizierte Auslegungsnote zu Empfehlung 15 der FATF zum Umgang mit sog. VASPs umgesetzt wurde. Diese Regeln wurden auch von den SRO übernommen, welche unter ihren Mitgliedern Anbieter von Kryptowährungen zählen.

fliessen lassen, bevor sie an die eigentliche Zieladresse gelangen. Eine Kryptowährungsadresse in einer solchen Transaktionskette stellt also lediglich eine Zwischenstation dar (sog. *Hop*). Ein effektives *Tracing* bedingt also, dass Transaktionen über mehrere *Hops* hinweg zurückverfolgt werden.
Diese Beispiele zeigen ferner einmal mehr auf, wie wichtig *Tracing*-Analysetools in Zusammenhang mit Kryptowährungs-Transaktionen sind. Damit die MROS die eigenen Analysemöglichkeiten einsetzen kann, ist die Dokumentierung der Abklärungen i. S. v. Art. 6 GwG seitens der Finanzintermediäre und die damit zusammenhängende Analyse betreffend Verfolgung von Kryptotransaktionen verlangt (Art. 3 Abs. 1 Bst. h MGwV).

5.6 Online- und Video-Identifizierung

Im März 2016 veröffentlichte die Eidgenössische Finanzmarktaufsicht (FINMA) das Rundschreiben 2016 / 7. Es handelt von den Sorgfaltspflichten der Finanzintermediäre bei der Aufnahme von Geschäftsbeziehungen über digitale Kanäle. Im Jahr 2018[28] wurde aufgrund der technologischen Entwicklung das Rundschreiben Video- und Online-Identifizierung teilrevidiert, und im Jahr 2020 schlug die FINMA weitere Änderungen vor. Sie wurden bis zum 1. Februar 2021 einer Anhörung unterzogen.[29] Die Möglichkeit, online eine Geschäftsbeziehung aufzunehmen, wird mittlerweile von den meisten Schweizer Bankinstituten angeboten. Einige Finanzintermediäre, insbesondere jene, die im Handel mit virtuellen Währungen tätig sind, machen sogar systematisch davon Gebrauch. Entsprechend nimmt die Zahl der an die MROS gemeldeten Fälle zu, bei welchen die Finanzintermediäre bei der Eröffnung einer Geschäftsbeziehung im Zuge der Online-Identifikation ihrer Kunden einen Verdacht schöpfen. Nahezu zwei Drittel der Fälle stehen in Verbindung mit der Verwendung von Kryptowährungen. Einer der grossen Fälle, die in der Vergangenheit gemeldet wurden, betraf beispielsweise die Online-Identifikation von potenziellen Investoren im Rahmen eines *Initial Coin Offering*.[30]
Der Aufbau von Geschäftsbeziehungen über digitale Kanäle ist nicht ohne Risiko. Kriminellen, die auf diese Weise Geschäftsbeziehungen aufbauen möchten, bietet es zwei Hauptmöglichkeiten, um ihr unrechtmässig erworbenes Geld zu waschen: Sie können entweder gefälschte oder widerrechtlich angeeignete, oft gestohlene Identitätsdokumente verwenden.[31] Beide Arten von Fällen tauchen häufig in den bei der MROS eingegangenen Verdachtsmeldungen auf. Die Meldungen, die nach der Identifizierung von gefälschten Dokumenten erstattet werden, überwiegen – wahrscheinlich, weil Fälschungen leichter erkennbar sind als gestohlene Dokumente. So erhielt die MROS im Jahr 2020 die Meldung eines Finanzintermediärs, der die Möglichkeit anbot, nach einem Identifikationsprozess durch Einreichen von Kopien von Ausweispapieren über das Internet online Konten zu eröffnen.
Er schöpfte Verdacht, nachdem er in offenen Quellen auf negative Informationen gestossen war: Die fraglichen Klienten wurden beschuldigt, Investoren bei der Einführung einer technologischen Innovation zu betrügen. Bei der Untersuchung dieses Falles konnte die MROS feststellen, dass eine der verwendeten Identitätskarten drei Tage vor der Kontoeröffnung als gestohlen gemeldet worden war. Es handelte sich um das Ausweisdokument, welches von einem der Mehrheitsaktionäre einer der Gesellschaften benutzt wurde, welche Inhaberin eines der vom Finanzintermediär gemeldeten Konten war. Gerade weil die Verwendung gefälschter oder widerrechtlich angeeigneter Dokumente bei der Eröffnung einer Online-Geschäftsbeziehung keine Identifizierung der tatsächlich kontrollierenden Gesellschafter oder der wirtschaftlich Berechtigten ermöglicht, ist es besonders schwierig, verdächtige Vermögenswerte mit Vortaten der Geldwäscherei in Verbindung zu bringen. Die Zusammenarbeit der

---

28 Vgl. die Medienmitteilung https://www.finma.ch/de/news/2018/07/20180717-mm-video-online-id/

29 Vgl. die Medienmitteilung https://www.finma.ch/de/news/2020/11/20201116-mm-online-identifizierung/

30 Eine Methode der Kapitalbeschaffung, die auf der Ausgabe von digitalen Vermögenswerten basiert, die in der Startphase eines Projekts in Kryptogeld oder Fiat-Währung umgetauscht werden können.

31 Vgl. auch die FATF-Publikation *Guidance on digital identity* vom März 2020.

MROS mit den schweizerischen Polizeibehörden und mit den ausländischen FIUs erweist sich deshalb als entscheidend. Schliesslich ist es aber die Genauigkeit der Angaben des meldenden Finanzintermediärs, die für die Effektivität der Zusammenarbeit ausschlaggebend ist.

Abbruch der Verhandlungen
Ein Finanzintermediär, der im Handel mit virtuellen Währungen tätig ist, erhielt am selben Tag drei Anträge auf Eröffnung eines Kontos auf seiner IT-Plattform. Er stellte fest, dass in allen drei Fällen das von den potenziellen Kunden vorgelegte ausländische Ausweisdokument dasselbe Foto enthielt. Die Angaben zu den Namen und Geburtsdaten waren allerdings verschieden. Der Finanzintermediär brach daraufhin die Verhandlungen zur Eröffnung einer Geschäftsbeziehung ab und führte weitere Abklärungen zu kürzlich eröffneten Konten durch. Seinen Verdacht meldete er der MROS gemäss Art. 9 Abs. 1 Bst. b GwG (versuchte Geldwäscherei). In der Folge wurden drei weitere Kunden identifiziert, deren Ausweisdokumente ebenfalls das gleiche Foto enthielten. Auch diese Geschäftsbeziehungen wurden der MROS gemeldet. Dank der MROS-Analyse konnten die ausländischen Konten identifiziert werden, von denen die drei bereits bestehenden Klienten zum Kauf von Kryptowährungen Überweisungen auf das Konto des Finanzintermediärs vorgenommen hatten. Aufgrund von Informationen der FIU des Landes, aus dem diese Überweisungen getätigt wurden, konnte die MROS bestätigen, dass die zum Kauf von Kryptowährungen überwiesenen Gelder aus im Ausland begangenen Betrügereien stammten. Ausserdem konnten der ausländischen FIU aufgrund der vom meldenden Finanzintermediär gelieferten Informationen die IP-Adressen der Computer übermittelt werden, von denen aus die Überweisungen getätigt wurden. Dies ermöglichte der ausländischen FIU, die Täter bei der zuständigen Strafverfolgungsbehörde wegen Betrugs und anschliessender Geldwäscherei anzuzeigen.

Den FATF-Empfehlungen entsprechend, haben mehrere Finanzintermediäre, die mit den Risiken von Online-Identifizierungsverfahren konfrontiert sind, diese verbessert. Sie sind von der manuellen Prüfung durch Compliance-Beauftragte zum Einsatz von Computerprogrammen übergegangen, welche die Echtheit der eingereichten Dokumente zuverlässiger prüfen.
Die MROS erhält vergleichsweise wenig Meldungen, die in Folge eines Abbruchs der Verhandlungen zur Eröffnung einer Geschäftsbeziehung erstattet werden. Die Verwendung falscher Ausweispapiere könnte unseres Erachtens durchaus Anlass zu Meldungen auf der Grundlage von Art. 9 Abs. 1 Bst. b GwG geben.

6. Aus der Praxis der Meldestelle

6.1 Übermittlung von Informationen – und nicht von Verdachtsmeldungen

Mit der am 1. Januar 2020 erfolgten Anpassung der MGwV werden keine Meldungen mehr an die Strafverfolgungsbehörden übermittelt. Um den Quellenschutz zu gewährleisten, werden auch keine Angaben zur Herkunft oder zum Verfasser der Verdachtsmeldung geliefert (Vgl. Art. 8 Abs. 1 MGwV). Die relevanten Informationen und die Einschätzung der MROS zu diesen Informationen werden vielmehr in Berichtsform elektronisch an die Staatsanwaltshaften übermittelt. Die Anzeigen an die Strafverfolgungsbehörden können Informationen aus verschiedenen Quellen und aus mehreren Verdachtsmeldungen enthalten (Vgl. Art. 1 Abs. 2 Bst. a–e MGwV). Die Gesamtheit der Informationen, die der Meldestelle zur Verfügung stehen, entscheidet, ob Anzeige erstattet wird. Wie bereits erwähnt (siehe Kapitel 4.12), hat damit das Konzept der «Weiterleitungsquote» von Verdachtsmeldungen in ihrer alten Form ausgedient.
Der zweite Punkt, der betont werden muss, hängt mit dem ersten zusammen. Nach Abschluss der Bearbeitung von Informationen aus einer Verdachtsmeldung informiert die MROS die Finanzintermediäre gemäss Art. 23 Abs. 5 und Abs. 6 GwG, ob die gemeldeten Informationen übermittelt werden oder nicht. Mit dieser Information werden zwei praktische Zwecke verfolgt: Im Falle einer Übermittlung der gemeldeten Informationen sind die Finanzintermediäre verpflichtet, die gemeldeten Vermögenswerte gemäss den Bestimmungen von Art. 10 GwG zu sperren. Falls entschieden wird, die Informationen nicht an eine Strafverfolgungsbehörde zu übermitteln, kann der Finanzintermediär nach eigenem Ermessen entscheiden, ob er die gemeldete Geschäftsbeziehung gemäss den Bestimmungen von Art. 30 GwV-FINMA weiterführt. Wie in der Vergangenheit lassen diese Entscheidungen keine Rückschlüsse auf die Rechtmässigkeit der Vermögenswerte auf einer gemeldeten Geschäftsbeziehung zu. Entscheide seitens MROS, Informationen zu einem gegebenen Zeitpunkt nicht an eine Strafverfolgungsbehörde zu übermitteln, können unter anderem erfolgen, nachdem die Informationen an andere FIUs oder an eine nationale Verwaltungsbehörde übermittelt worden sind. Es ist auch möglich, dass ein Teil der aus der Verdachtsmeldung stammenden Informationen im Rahmen eines Berichts an die Strafverfolgungsbehörden übermittelt wurde. Die Übermittlung aller Informationen der Meldung jedoch nicht gerechtfertigt gewesen wäre.

6.2 Neue Befugnisse i. Z. m. Art. 11a Abs. 2bis GwG

6.2.1 Der neue Art. 11a Abs. 2bis GwG

Am 25. September 2020 hat das Parlament den Bundesbeschluss über die Genehmigung und die Umsetzung des Übereinkommens des Europarats zur Verhütung des Terrorismus mit dem dazugehörigen Zusatzprotokoll sowie über die Verstärkung des strafrechtlichen Instrumentariums

gegen Terrorismus und organisierte Kriminalität[32] verabschiedet. Mit diesem Beschluss wird das GwG geändert, insbesondere durch die Einführung eines neuen Art. 11a Abs. 2bis. Er lautet wie folgt:

«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.»

Am 31. März 2021 beschloss der Bundesrat, dass diese neuen Bestimmungen am 1. Juli 2021 in Kraft treten.[33] Mit Inkrafttreten dieser Änderung des GwG erhält die MROS neue Befugnisse zur Bekämpfung der Geldwäscherei, der Vortaten zur Geldwäscherei, der organisierten Kriminalität und der Terrorismusfinanzierung. Bereits seit dem 1. November 2013 kann die MROS gestützt auf eine Transaktionsanalyse bei Schweizer Finanzintermediären zusätzliche Informationen anfordern, die für ihre Analysen notwendig sind in Bezug auf Drittkonten, mit denen über die gemeldete Geschäftsbeziehung Transaktionen getätigt worden sind. Ziel des Gesetzgebers war es, der MROS zusätzliche Mittel an die Hand zu geben, um ihre Analysen zu vertiefen und unter bestimmten Voraussetzungen der Papierspur (*paper trail*) folgen zu können. Innerhalb weniger Jahre ist diese Bestimmung zu einem der wichtigsten Instrumente für die Arbeit der MROS geworden. Die Möglichkeit, gestützt auf Art. 11a GwG zusätzliche Informationen einzuholen und mit ausländischen FIUs und anderen nationalen Behörden Informationen auszutauschen, hat dazu beigetragen, dass die MROS ihre Analysen verbessern und eine Überlastung der Strafverfolgungsbehörden vermieden werden konnte.

Bisher waren Anfragen nach Art. 11a GwG bei Fällen möglich, in denen der MROS bereits eine Verdachtsmeldung eines Schweizer Finanzintermediärs vorlag. Im Rahmen der Analyse von Anfragen ausländischer Partner-FIUs konnte die MROS folglich solche Anfragen bezüglich zusätzlicher Informationen nur stellen, wenn sie eine Verbindung zu Finanzinformationen aufwiesen, die der MROS von einem Schweizer Finanzintermediär gemeldet worden waren. Wenn diese einen Zusammenhang mit einer Meldung aufwiesen, konnte die MROS darauf antworten. Andernfalls konnte die Meldestelle der anfragenden FIU keine Finanzinformationen zur Verfügung stellen. Diese Lücke wurde bei der FATF-Evaluation der Schweiz im Jahr 2016 kritisiert. Infolgedessen wurde die Schweiz als nur «partiellement conforme» – teilweise konform – mit der FATF-Empfehlung 40 eingestuft (eine unzureichende Bewertung). Die von der Schweiz erreichte Effizienz in der internationalen Zusammenarbeit (RI 2) wurde mit «modéré» – mässig – bewertet (was ebenfalls nicht ausreichend ist).[34] Die Behebung dieser schwerwiegenden Mängel war denn auch eine der acht prioritären Massnahmen, die die Evaluatoren von der Schweiz forderten. Begründet wurde diese Aufforderung unter anderem mit der starken Internationalisierung des Schweizer Finanzplatzes.
Aufgrund dieser nicht zufriedenstellenden Bewertung der Schweiz leitete die Egmont-Gruppe – das operative Austauschforum für FIUs – ein Non-Compliance-Verfahren gegen die Schweiz ein. Gemäss den Regeln zur Anwendung der Grundsätze dieser Gruppe unterliegt die MROS einem *Follow-up*-Prozess und ist verpflichtet, über die Massnahmen zu berichten, die zur Behebung der bei der FATF-Evaluation festgestellten Mängel getroffen wurden. Sollten die einschlägigen Schweizer Gesetze nicht innerhalb einer bestimmten Zeit entsprechend angepasst werden, könnte die MROS von der Egmont Gruppe ausgeschlossen werden. Vor diesem Hintergrund sei daran erinnert, dass die Mehrzahl der Verdachtsmeldungen, die bei der MROS

[32] BBl **2020** 7891, 7902.

[33] Vgl. die Medienmitteilung *Terrorismusbekämpfung: Bundesrat setzt verschärftes Strafrecht in Kraft.*

[34] Vgl. mer-suisse-2016.pdf (fatf-gafi.org).

eingehen, einen Auslandsbezug aufweisen. In solchen Fällen ist die Möglichkeit, Informationen anderer FIUs der Egmont-Gruppe beizuziehen, von wesentlicher Bedeutung. Die neuen Bestimmungen von Art. 11a Abs. 2bis GwG und die damit verbundenen Kompetenzen sollten den internationalen Standards entsprechen und es der MROS ermöglichen den *Follow-up*-Prozess innerhalb der Egmont-Gruppe abzuschliessen.
Dank der neuen Bestimmung von Art. 11a Abs. 2bis GwG kann die MROS künftig auch ohne Verdachtsmeldung eines Schweizer Finanzintermediärs bei Finanzintermediären Auskunft über eine oder mehrere Transaktionen oder Geschäftsbeziehungen verlangen, welche Gegenstand einer Anfrage oder Spontaninformation einer anderen FIU sind. Diese erweiterte Kompetenz kommt auch den Schweizer Finanzintermediären zugute, da sie auf bislang unerkannte potenzielle Risiken in ihren Geschäftsbüchern aufmerksam gemacht werden und erhöht somit die Sicherheit in der Schweiz. Damit trägt der verbesserte Informationsaustausch (*financial intelligence*) zwischen den FIUs dazu bei, die internationale Rechtshilfe und die Strafverfolgung zu stärken.

6.2.2 Informationsaustausch mit ausländischen Meldestellen

Die internationale Amtshilfe zwischen der MROS und ihren ausländischen Partner-FIUs ist in den Art. 30 bis 31 GwG geregelt. Die MROS wird somit die gemäss dem neuen Art. 11a Abs. 2bis GwG erhaltenen Finanzinformationen unter den gleichen Bedingungen wie bisher mit ihren ausländischen Partner-FIUs austauschen. Der Bundesrat hat sich mehrfach zu diesem Thema geäussert.[35] Bevor die MROS mit einer ausländischen FIU Informationen austauscht, prüft sie, ob die Voraussetzungen gemäss Art. 30 GwG erfüllt sind. Geprüft wird unter anderem, ob dem Spezialitätsprinzip, dem Grundsatz der Gegenseitigkeit und des Amtsgeheimnisses Genüge getan wird. Ersuchen von ausländischen FIUs müssen schliesslich auch den Anforderungen des Art. 31 GwG genügen. Auf *fishing expeditions*-Ersuchen, die eindeutig keinen Bezug zur Schweiz aufweisen – tritt die MROS nicht ein, ebenso wenig auf Ersuchen, die darauf abzielen, den Weg der internationalen Rechtshilfe in Strafsachen zu umgehen. Die MROS erteilt auch keine Auskünfte, falls dadurch die nationalen Interessen oder die Sicherheit und öffentliche Ordnung der Schweiz beeinträchtigt werden könnten. Die Informationen dürfen von der FIU, die sie erhält, nur im Rahmen ihrer Analysen in Bezug auf Geldwäscherei, deren Vortaten, organisierte Kriminalität und Terrorismusfinanzierung verwendet werden. Mit vorheriger Zustimmung der MROS können die an eine ausländische FIU übermittelten Informationen auch an Drittbehörden im gleichen Land weitergegeben werden. Die MROS stützt ihre Bewilligung auf die Bedingungen von Art. 30 Abs. 4 und Abs. 5 GwG. Dabei ist zu beachten, dass die übermittelten Informationen nur zu Informationszwecken (*Intelligence*) und nicht als Beweismittel verwendet und nur in Berichtsform weitergegeben werden dürfen (Art. 30 Abs. 3 GwG).

6.2.3 Erste praktische Fragen zur Anwendung des neuen Art. 11a Abs. 2bis GwG

Das Inkrafttreten dieser neuen gesetzlichen Bestimmung wirft bei Finanzintermediären einige praktische Umsetzungsfragen auf, die hier beantwortet werden sollen. Die Regeln, die Finanzintermediäre beachten müssen, wenn die MROS gestützt auf den neuen Art. 11a Abs. 2bis und 3 GwG die Herausgabe von zusätzlichen Informationen verlangt, sind dieselben, die seit 2013 für Anfragen gestützt auf Art. 11a Abs. 2 GwG gelten.[36] Um zusätzliche Informationen zu erhalten, verwendet die MROS an Art. 11a Abs. 1 respektive Abs. 2 GwG angepasste Formulare. Eine Liste der einzureichenden Dokumente / Informationen ist darin vorgesehen. Die MROS wählt diejenigen

---

[35] Siehe beispielsweise die Botschaft zur Genehmigung und zur Umsetzung des Übereinkommens des Europarats zur Verhütung des Terrorismus mit dem dazugehörigen Zusatzprotokoll sowie zur Verstärkung des strafrechtlichen Instrumentariums gegen Terrorismus und organisierte Kriminalität vom 14. September 2018, BBl **2018** 6427 ff. und die Botschaft zur Änderung des Geldwäschereigesetzes vom 27. Juni 2012, BBl **2012** 6941, 6487 ff.

[36] Siehe hierzu den *MROS-Jahresbericht 2013*, S. 56 ff.

aus, die nach der entsprechenden Rechtsgrundlage (Art. 11 Abs. 1 oder Art. 11a Abs. 2 oder 2bis GwG) relevant sind. Der Inhalt des Formulars für Ersuchen nach Art. 11a Abs. 2bis wird identisch sein mit demjenigen für Ersuchen nach Art. 11a Abs. 2 GwG. Finanzintermediäre, die in goAML registriert sind und solche Informationsanfragen erhalten, werden gebeten, entsprechend der im goAML-Handbuch dokumentierten Vorgehensweise über diesen Kanal zu antworten.[37]
Dabei ist zu beachten, dass ein solches Ersuchen nicht automatische zu einer Verdachtsmeldung an die MROS führen muss. Der Finanzintermediär, der ein solches Ersuchen erhält, muss es beantworten. Er kann dabei nicht ignorieren, dass es sich um eine behördliche Aufforderung handelt, die auf dem Verdacht Geldwäscherei, Vortaten zur Geldwäscherei, organisierter Kriminalität oder Terrorismusfinanzierung beruht. Der Finanzintermediär muss deshalb zusätzliche Abklärungen gemäss Art. 6 GwG vornehmen und bei einem einfachen oder begründeten Verdacht der MROS eine Meldung erstatten. Ergeben sich keine Verdachtsmomente, so übermittelt der Finanzintermediär die gemäss Art. 11a Abs. 2bis GwG verlangten Informationen einfach an die MROS und dokumentiert seine Abklärungen (vgl. Art. 7 GwG und 31 GwV-FINMA).
Wie in der Vergangenheit kann ein Finanzintermediär, der sich entschliesst, die Geschäftsbeziehung, die Gegenstand einer MROS-Anfrage ist, zu melden, dies tun, indem er seiner Verdachtsmeldung die angefragten Dokumente und die verlangten Informationen beifügt, sofern die Verdachtsmeldung innerhalb der für die Beantwortung der MROS-Anfrage gesetzten Frist eingereicht wird. Diese Frist wird von der MROS nach Massgabe von Art. 11a Abs. 3 GwG gesetzt. Der aufgeforderte Finanzintermediär stellt der MROS die in seinem Besitz befindlichen Informationen zur Verfügung. Bezüglich des Art. 11a GwG präzisierte der Bundesrat wie folgt: «Als verfügbar gelten alle Informationen, welche in den Entitäten eines Unternehmens vorhanden sind oder beschafft werden können, soweit diese Entitäten der schweizerischen Jurisdiktion unterliegen.»[38]

6.3 Editionsverfügungen der Strafverfolgungsbehörden und Meldepflicht

Ist es notwendig, eine Verdachtsmeldung zu erstatten, sobald eine strafrechtliche Beschlagnahme durch eine Strafverfolgungsbehörde angeordnet wurde? Diese Frage wird der MROS von Finanzintermediären und auch von anderen interessierten Kreisen immer wieder gestellt. Die MROS hat dazu bereits vor mehr als zehn Jahren[39] eine Antwort gegeben, welche durch die Rechtsprechung des Bundesgerichts im Jahr 2018 bestätigt wurde. In seiner Botschaft zur Verabschiedung des GwG präzisiert der Bundesrat den Sinn und Zweck des GwG:

«Im Zentrum dieser Anstrengungen steht die Bekämpfung der organisierten Kriminalität. Es kann somit nicht nur darum gehen, inkriminierte Gelder aufzuspüren und zu konfiszieren. Vielmehr sollen die dokumentarischen Grundlagen (paper trail) geschaffen und Informationen bereitgestellt (Meldepflicht) werden, damit die für die Geldwäscherei verantwortlichen Personen ermittelt und strafrechtlich belangt werden können.»[40]

Die Bestimmungen des GwG zielen also in erster Linie auf die generelle Bekämpfung der Geldwäscherei und auf die strafrechtliche Verfolgung derjenigen ab, die dieser Straftat beschuldigt werden. Die Sperrung und Beschlagnahme des möglicherweise inkriminierten Vermögens ist zwar nicht von untergeordneter Bedeutung, ist aber weder ausschliessliches noch vorrangiges Ziel. Es soll daher betont werden, dass das GwG beide Zwecke gleichermassen verfolgt. Das Erreichen des ersten Zwecks impliziert nicht

---

37 Siehe *goAML Web-Handbuch*, S. 22 und 47.

38 BBl **2018** 6427, 6509.

39 Siehe Kapitel 5.5 «Editionsverfügungen der Strafverfolgungsbehörden und Meldepflicht» im *MROS-Jahresbericht 2007*, S. 88 ff. und Kapitel 4.1 im *MROS-Jahresbericht 2017* (S. 57), wo die 2007 veröffentlichte Praxis bekräftigt wird. Siehe auch die an derselben Stelle veröffentlich Praxis der MROS; vgl. *Publikationen der Meldestelle für Geldwäscherei (MROS).*

40 BBl **1996** III 1101, 1116.

notwendigerweise das Erreichen des zweiten oder, mit anderen Worten, die beiden genannten Zwecke sind voneinander unabhängig, sollen jedoch soweit möglich, auf koordinierte Weise erreicht werden.
Was die Meldepflicht der Finanzintermediäre bei Erhalt eines Editions- und/oder einer Beschlagnahmeverfügung betrifft, hat die MROS den Zweck des GwG bereits 2007 in ihre administrative Praxis integriert. Die MROS betonte damals, dass diese Frage nicht abschliessend beurteilt werden sollte.
Sie ist vielmehr von Fall zu Fall und unter Berücksichtigung der Ergebnisse der zusätzlichen Abklärungen zu beurteilen, die der Finanzintermediär in solchen Fällen gemäss Art. 6 Abs. 2 GwG in Verbindung mit Art. 15 ff. der GwV-FINMA vornehmen muss: «Grundsätzlich ist hierzu zu sagen, dass eine Editions- und/oder Beschlagnahmeverfügung immer die besondere Abklärungspflicht [...] auslöst.»[41]
Wenn der Finanzintermediär aufgrund der Ergebnisse der zusätzlichen Abklärungen, die durch den Erhalt einer Editions- und/oder einer Beschlagnahmeverfügung ausgelöst wurden, zusätzliche Verdachtsmomente sowohl auf Transaktionsebene als auch auf der Ebene der Geschäftsbeziehung feststellt und diese Verdachtsmomente einen begründeten Verdacht im Sinne von Art. 9 Abs. 1 Bst. a GwG darstellen, dann muss er der MROS eine Verdachtsmeldung erstatten.
Dies ist zum Beispiel dann der Fall, wenn die zusätzlichen Abklärungen zur Identifikation von weiteren Geschäftsbeziehungen führen, die nicht Gegenstand der erhaltenen Editions- und/oder der Beschlagnahmeverfügung waren. Der Finanzintermediär kann in der Verfügung auf die Namen von Personen stossen, die als Inhaber, wirtschaftlich Berechtigte, Zeichnungsberechtigte, Kontrollinhaber oder Auftraggeber und Begünstigte von inländischen oder internationalen Überweisungen involviert sind. Der Finanzintermediär soll zum gleichen Ergebnis kommen und melden, wenn die Transaktionsanalyse der von der Editionsverfügung oder der Beschlagnahmeverfügung betroffenen Geschäftsbeziehung das Vorliegen verdächtiger Transaktionen ausserhalb des von der Staatsanwaltschaft angegebenen Zeitraums ergibt. Im Übrigen sei darauf hingewiesen, dass der Finanzintermediär nicht an den in der Regel kurz gefassten Sachverhalt gebunden ist, der in der Editions- und/oder Beschlagnahmeverfügung der verantwortlichen Strafverfolgungsbehörde angegeben ist.
Dies bedeutet: Wenn der Finanzintermediär im Rahmen weiterer Abklärungen im Sinne von Art. 6 Abs. 2 GwG in Verbindung mit Art. 15 ff. GwV-FINMA zusätzliche oder neue Verdachtsmomente im Zusammenhang mit den in der Editions- und/oder in der Beschlagnahmeverfügung genannten oder weiteren Personen und/oder Geschäftsbeziehungen entdeckt, und diese neuen Elemente einen begründeten Verdacht rechtfertigen, so ist der Finanzintermediär zur Meldung nach Art. 9 Abs. 1 Bst. a GwG verpflichtet. In solchen Fällen müssen die Finanzintermediäre immer die betroffene Editions- und/oder Beschlagnahmeverfügung der Meldung beilegen (Art. 3 Abs. 1 Bst. h MGwV).[42] MROS versieht eine Überprüfungstätigkeit und stellt die Koordination mit den zuständigen Strafverfolgungsbehörden sicher, was es ermöglicht, die erhaltenen Informationen zu bewerten und zu entscheiden, ob es notwendig ist, die gemeldeten Informationen an die zuständigen Behörden zu übermitteln. Im Jahr 2020 gaben Finanzintermediäre beispielsweise in 9,1 Prozent der Fälle «Informationen der Strafverfolgungsbehörden» als Grund für den Verdacht an, der sie zu einer Meldung veranlasste. In den meisten Fällen übermittelt die MROS diese Informationen an die zuständigen Strafverfolgungsbehörden, weil die neuen Informationen für die Durchführung eines laufenden Strafverfahrens nützlich sind.
Ergeben sich hingegen aus den Abklärungen des Finanzintermediärs keine Informationen, welche nicht bereits von der Editions- und/oder Beschlagnahmeverfügung der Strafverfolgungsbehörde abgedeckt sind, so braucht er der MROS keine zusätzliche Verdachtsmeldung zu erstatten.

---

41 Siehe *MROS-Jahresbericht 2007*, S. 86.

42 Vgl. *MROS-Jahresbericht 2017* (S. 57) sowie die *Erläuterungen zur Teilrevision der MGwV* vom 24. November 2019, S. 14 Fussnote 37.

Eine solche Meldung wäre eine unnötige Doppelspurigkeit.
Dasselbe gilt auch für einen dritten Finanzintermediär (Vermögensverwalter, Treuhänder etc.), der – nach Ablauf eines eventuellen Informationsverbots – von einer Bank über das Bestehen einer Herausgabepflicht gemäss Art. 265 Schweizerische Strafprozessordnung vom 5. Oktober 2007[43] informiert worden ist oder nach Massgabe von Art. 10a Abs. 3 GwG davon unterrichtet worden ist, dass eine Verdachtsmeldung nach Art. 9 GwG erstattet wurde.
Nach der Rechtsprechung des Bundesgerichts[44] endet die Meldepflicht der Finanzintermediäre nicht mit der Übergabe der Sache an die Strafverfolgungsbehörde, sondern «hält an, solange Vermögenswerte aufgespürt und eingezogen werden können».[45] Die Eröffnung eines Ermittlungsverfahrens bedeutet noch nicht, dass die Voraussetzungen für den Erlass einer strafrechtlichen Beschlagnahmeverfügung erfüllt sind. Andererseits kann die Meldung des Finanzintermediärs an die MROS gemäss Art. 9 GwG und Art. 3 MGwV sehr schnell zu einer auf der Grundlage von Art. 10 GwG verfügten vorübergehenden Vermögenssperre führen. Die Meldung verdächtiger Vorgänge ist eine besondere Pflicht des Finanzintermediärs, unabhängig von einem möglichen Strafverfahren.
Erhält der Finanzintermediär eine Editions- und/oder eine Beschlagnahmeverfügung, so ist er verpflichtet, durch die korrekte Anwendung der besonderen Sorgfaltspflichten gemäss Art. 6 Abs. 2 GwG in Verbindung mit Art. 15 ff. GwV-FINMA alle potenziell verdächtigten Vermögenswerte offenzulegen, die sich noch in seinen Geschäftsbüchern befinden oder die im Zusammenhang mit inzwischen abgeschlossenen Geschäftsbeziehungen stehen. Er ist ausserdem dazu verpflichtet, allfällige weitere Verdachtsmomente zu identifizieren. Solange diese Tätigkeit nicht abgeschlossen ist, kann der Finanzintermediär das Vorliegen eines begründeten Verdachts nicht ausschliessen.

Eine Verdachtsmeldung gemäss Art. 9 Abs. 1 GwG gefolgt von einer Übermittlung der MROS an eine Strafverfolgungsbehörde gemäss Art. 23 Abs. 4 GwG und die daraus resultierende *ex lege* Sperrung von Vermögenswerten (Art. 10 GwG) ist somit das einzig mögliche Mittel, um sicherzustellen, dass diese Vermögenswerte entdeckt werden und die zuständige Strafverfolgungsbehörde allenfalls eine neue Editions- und/oder Beschlagnahmeverfügung erlassen kann, die gegebenenfalls den Weg zur Einziehung der Vermögenswerte eröffnet. Diese Meldung ermöglicht auch die Identifizierung und strafrechtliche Verfolgung anderer Personen, die sich möglicherweise der Geldwäscherei schuldig gemacht haben.

6.4 Entgegennahme von Verdachtsmeldungen seitens MROS

Der MROS gehen regelmässig auch Eingaben zu, welche sie aufgrund fehlender sachlicher und örtlicher Zuständigkeit nicht als Meldungen i. S. des GwG oder des Bundesgesetzes vom 18. Dezember 2015 über die Sperrung und die Rückerstattung unrechtmässig erworbener Vermögenswerte ausländischer politisch exponierter Personen (SRVG)[46] entgegennehmen und somit nicht behandeln kann.
Bei den Meldenden kann es sich um natürliche- oder juristische Personen handeln, welche dem GwG nicht unterstellt sind, oder um Institute, welche zwar dem GwG unterstellt sind, im Rahmen des gemeldeten Sachverhalts aber nicht als Finanzintermediär i. S. v. Art. 2 GwG oder als Person und Institution i. S. v. Art. 7 SRVG handeln. Die MROS ist als einzige Stelle in der Schweiz befugt, Meldungen von Finanzintermediären, Händler*innen, Behörden und Organisationen gemäss GwG wegen Verdachts auf Geldwäscherei, deren Vortaten, Zugehörigkeit zu einer kriminellen Organisation und Terrorismusfinanzierung entgegenzunehmen und zu bearbeiten. Sie entscheidet darüber, ob die gemeldeten Informationen an eine Strafverfolgungsbehörde zu übermitteln

43 SR **312.0**

44 Siehe BGE 144 IV 391, E. 3.1 und 3.3–3.4; BGE 142 IV 276, E. 5.4.2

45 Siehe BGE 144 IV 391, E. 3.1

46 SR **196.1**

sind (Art. 23 Abs. 4 GwG). Daneben nimmt die MROS Informationen von Personen und Institutionen nach Art. 7 Abs. 1 und 2 SRVG entgegen und übermittelt die erhaltenen Informationen dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) und dem Bundesamt für Justiz (BJ) (Art. 7 Abs. 6 SRVG).
Falls die MROS eine Meldung aufgrund fehlender sachlicher und örtlicher Zuständigkeit nicht entgegennimmt, können die darin enthaltenen Informationen nicht von der MROS bearbeitet und an eine Strafverfolgungsbehörde i. S. v. Art. 23 Abs. 4 GwG übermittelt werden.
Aufgrund des Spezialitätsprinzips kann die MROS umgekehrt erhaltene Verdachtsmeldungen nur entgegennehmen und behandeln, wenn sie sachlich und örtlich zuständig ist.
Alle übrigen dem GwG und SRVG nicht unterstellten (natürlichen oder juristischen) Personen, welche einen solchen Verdacht haben, sind deshalb gehalten, entsprechende Hinweise direkt an die Strafverfolgungsbehörden zu richten. Üblicherweise werden Anzeigen an die Polizei am Wohnort der anzeigenden Person erstattet.
Im Jahr 2020 hat die MROS 140 Bürgerbriefe- und 8 als «Verdachtsmeldungen nach Art. 9 GwG oder 305ter StGB bezeichnete» Eingaben erhalten, für welche sie nicht sachlich und/oder örtlich zuständig war.
Die MROS prüft bei Eingang einer Eingabe ihre Zuständigkeit von Amtes wegen. Sie kann aber nur summarisch untersuchen, ob die meldende Entität dem GwG unterstellt ist oder nicht. Dies insbesondere deshalb, weil sie von Gesetzes wegen nicht die Kompetenz hat, materiell darüber zu befinden, ob eine GwG-Unterstellung gegeben ist oder nicht. Diese Aufgabe obliegt grösstenteils der FINMA, welche aufgrund ihrer Zuständigkeit, die SRO und die AO anzuerkennen, indirekt auch für diese bzw. die durch diese beaufsichtigten Entitäten zuständig ist. Die FINMA veröffentlicht denn auch auf ihrer Website die Namen von Institutionen, welche über eine bestimmte Form von Bewilligung verfügen.[47]
Gemäss Art. 12 GwG sind ausser der FINMA, die ESBK, die interkantonale Aufsichts- und Vollzugsbehörde nach Art. 105 des Bundesgesetztes über Geldspiele (BGS[48]), d. h. die interkantonale Geldspielaufsicht (Gespa), oder die anerkannten SRO und bewilligten AO zur Überwachung der Einhaltung der Verpflichtungen aus dem GwG befugt. Entsprechende Informationen sind auch auf deren Websites publiziert. Ferner kann die MROS mit der FINMA, der ESBK oder der Gespa in diesem Zusammenhang Informationen austauschen (vgl. Art. 29 Abs. 1 GwG i. V. m. Art. 7 Abs. 1 Bst. d MGwV).
Bei der Erstattung einer Verdachtsmeldung oder für die goAML-Registrierung ist u. a. auch die Angabe zu machen, welche Behörde oder Organisation gemäss Art. 12 GwG oder Art. 43a Finanzmarkaufsichtsgesetz vom 22. Juni 2007[49] den Finanzintermediär beaufsichtigt (vgl. Art. 3 Abs. 1 Bst. b MGwV).
Weiter gibt es den Fall von Entitäten, welche nicht über eine behördliche Bewilligung im engeren Sinn verfügen, sodass ihr Tätigkeitsbereich nicht aufgrund behördlicher Feststellung im Bewilligungsverfahren gesamthaft dem GwG unterstellt ist. Ob bei solchen Entitäten in einem konkreten Fall Finanzintermediation vorliegt, wird ebenfalls nur summarisch geprüft. Auch hier können mit den Aufsichtsbehörden unter den Voraussetzungen von Art. 29 Abs. 1 GwG Informationen ausgetauscht werden.

---

47 Vgl. https://www.finma.ch/de/finma-public/bewilligte-institute-personen-und-produkte/, https://www.finma.ch/de/bewilligung/selbstregulierungsorganisationen-sro/sro-mitglieder-suche/#Order=1.

48 SR **935.51**

49 SR **956.1**

7. Links

7.1 Schweiz

7.1.1 Meldestelle für Geldwäscherei

www.fedpol.admin.ch
Bundesamt für Polizei (fedpol)

www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei.html
Meldestelle für Geldwäscherei (MROS)

https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung/meldeformular.html
Meldeformular

7.1.2 Aufsichtsbehörden

www.finma.ch
Eidgenössische Finanzmarktaufsicht (FINMA)

www.esbk.admin.ch
Eidgenössische Spielbankenkommission (ESBK)

www.gespa.ch
Interkantonale Geldspielaufsicht (Gespa)

7.1.3 Nationale Verbände und Organisationen

www.vsv-asg.ch
Verband Schweizerischer Vermögensverwalter (VSV)

www.swissbanking.org
Schweizerische Bankiervereinigung (SBVg)

www.abps.ch
Vereinigung schweizerischer Privatbankiers (ABPS)

www.afbs.ch
Verband der Auslandsbanken in der Schweiz (AFBS)

www.svv.ch
Schweizerischer Versicherungsverband

www.sfama.ch
Swiss Funds & Asset Management Association (SFAMA)

www.svig.org
Schweizer Verband der Investmentgesellschaften (SVIG)

7.1.4 Selbstregulierungsorganisationen

https://www.aoos.ch/
Schweizerische Aktiengesellschaft für Aufsicht (AOOS)

www.arif.ch
Association Romande des Intermédiaires Financiers (ARIF)

http://so-fit.ch/
Organisme de Surveillance pour Intermédiaire Financiers & Trustees (SOFIT)

www.oadfct.ch
Organismo di Autodisciplina dei Fiduciari del Cantone Ticino (OAD FCT)

www.polyreg.ch
PolyReg Allg. Selbstregulierungs-Verein

www.sro-sav-snv.ch
SRO des Schweizerischen Anwaltsverbandes und des Schweizerischen Notarenverbandes SAV/SNV

www.leasingverband.ch
SRO Schweizerischer Leasingverband (SLV)

www.sro-treuhandsuisse.ch
SRO-Treuhand Suisse

www.vqf.ch
Verein zur Qualitätssicherung von Finanzdienstleistungen (VQF)

www.sro-svv.ch
Selbstregulierungsorganisation des Schweizerischen Versicherungsverbandes (SRO-SVV)

7.1.5 Aufsichtsorganisationen

https://www.aoos.ch/
Schweizerische Aktiengesellschaft für Aufsicht (AOOS)

http://www.fincontrol.ch/
FINcontrol Suisse AG

https://osif.ch/
Organisme de Surveillance des Instituts Financiers (OSIF)

http://so-fit.ch/
Organisme de Surveillance pour Intermédiaire Financiers & Trustees (SOFIT)

https://osfin.ch/fr/
Organisation de Surveillance Financière (OSFIN)

7.1.5 Weitere

www.ezv.admin.ch
Eidgenössische Zollverwaltung (EZV)

www.snb.ch
Schweizerische Nationalbank (SNB)

www.bundesanwaltschaft.ch
Bundesanwaltschaft (BA)

https://www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos.html
Staatssekretariat für Wirtschaft (SECO) (Wirtschaftssanktionen basierend auf dem Embargogesetz)

www.estv.admin.ch
Eidgenössische Steuerverwaltung (ESTV)

https://www.vbs.admin.ch/de/vbs/organisation/verwaltungseinheiten/nachrichtendienst.html
Nachrichtdienst des Bundes (NDB)

www.bstger.ch
Bundesstrafgericht

7.2 International

7.2.1 Ausländische Meldestellen

https://www.egmontgroup.org/en/membership/list
Liste aller Egmont-Mitglieder, teilweise mit Link auf deren Homepage

7.2.2 Internationale Organisationen

www.fatf-gafi.org
Financial Action Task Force on Money Laundering (FATF)

www.unodc.org
United Nations Office on Drugs and Crime (UNODC)

www.egmontgroup.org
Egmont-Gruppe

www.cfatf-gafic.org
Caribbean Financial Action Task Force (CFATF)

7.2.3 Weitere Links

www.interpol.int
Interpol

https://www.europol.europa.eu/de/about-europol
Europol