Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Praxis der Meldestelle für Geldwäscherei MROS

Negativtypologien

August 2025

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Praxis der Meldestelle für Geldwäscherei MROS

Negativtypologien

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

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

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

Inhaltsverzeichnis

1 Hintergrund und Ziel der Negativtypologien

Das schweizerische Geldwäschereiabwehrdispositiv fusst darauf, dass der Finanzintermediär die ersten grundlegenden Abklärungen hinsichtlich möglicher illegaler Vermögenswerte oder Transaktionen trifft. Der Gesetzgeber hat sich klar für ein qualitatives Meldewesen ausgesprochen. Auf sogenannte «schwellenwertbasierte» Meldungen, die beispielsweise eine bestimmte Transaktionssumme oder einen anderen quantitativen Trigger voraussetzen, wurde im Schweizer Recht bisher bewusst verzichtet. Die im Geldwäschereigesetz verankerten Sorgfaltspflichten sind kaskadenartig und repetitiv aufgebaut. Ausgangspunkt bilden die Art. 3 – 5 GwG[1] mit der Identifizierung der Vertragspartei, der Feststellung des wirtschaftlich Berechtigten sowie der periodischen Wiederholung dieser Pflichten. Die besonderen Abklärungspflichten in Art. 6 GwG sehen vor, Hintergründe sowie den Zweck von Transaktionen und Geschäftsbeziehung risikobasiert zu prüfen. Die Finanzintermediäre sollen Hinweisen und Verdachtsmomenten nachgehen und diese sauber abklären. Erst wenn diese Abklärungen zu keinem Erfolg führen, bzw. Verdachtsmomente nicht ausgeräumt werden können und sich ein begründeter Verdacht manifestiert, ist eine Verdachtsmeldung an die Meldestelle für Geldwäscherei (MROS) im Sinne von Art. 9 GwG zu erstatten. Die Verdachtsmeldung stellt somit das Ergebnis einer qualifizierten Beurteilung und nicht lediglich einer risikobasierten Vermutung dar.

In der Praxis stellt die MROS immer wieder qualitative Unterschiede beim Inhalt eingehender Verdachtsmeldungen fest. Teilweise werden kaum abgeklärte Sachverhalte übermittelt oder es ist für die MROS nicht erkennbar, ob die pflichtgemässen Abklärungen gemäss Art. 6 GwG stattgefunden haben.

Auswertungen der MROS zeigen klar, dass derzeit Tendenzen zu einem «defense reporting» erkennbar sind. Konkret heisst dies:

- Verdachtsmeldungen erfolgen nicht primär aufgrund eines substanziellen Verdachts auf einen geldwäschereirechtlich relevanten Sachverhalt, sondern zur Absicherung gegenüber straf- oder aufsichtsrechtlichen Risiken.
- Die Meldeschwelle wird vom Finanzintermediär bewusst deutlich unterhalb des gesetzlich geforderten und aus Sicht der Kriminalitätsbekämpfung angemessenen Niveaus angesetzt.
- Der Informationsgehalt der Meldungen ist gering oder gar irrelevant. Ein Mehrwert für die Kriminalitätsbekämpfung ist nicht erkennbar.

Solche Meldungen leisten keinen Beitrag zur Bekämpfung der Finanzkriminalität. Eine effektive Bearbeitung durch die MROS erfordert nicht nur einen hinreichenden Anfangsverdacht, sondern auch eine inhaltlich fundierte, strukturierte und dokumentierte Sachverhaltsdarstellung. Nur so können die Daten analysiert, priorisiert und – wo nötig – den Strafverfolgungsbehörden zugeführt werden.

Die von der MROS vorliegend veröffentlichten Negativtypologien haben zum Ziel, den Finanzintermediären anhand von Beispielen exemplarisch Anhaltspunkte («Negativtypologien») aufzuzeigen, bei denen die MROS wiederholt ungenügend oder gar nicht abgeklärte Sachverhalte in einer Verdachtsmeldung festgestellt hat. Sie dienen dazu die Finanzintermediäre zu sensibilisieren, die Datenqualität sowie die Informationen der eingehenden Meldungen zu verbessern, und damit einen Beitrag zur effizienten Bearbeitung der Verdachtsmeldungen durch die MROS zu leisten.

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

2 Negativtypologien - Prüfung des Einzelfalles

Die nachfolgenden Fallbeispiele basieren auf Erkenntnissen der MROS aus der Praxis. Es handelt sich typischerweise um Fallkonstellationen, in welchen die MROS ungenügend abgeklärte Sachverhalte übermittelt erhält und keine ausreichenden Anhaltspunkte auf Geldwäscherei, deren Vortaten, organisierte Kriminalität oder Terrorismusfinanzierung im Sinne von Art. 9 GwG vorliegen.

Die Verantwortung für den Entscheid, ob ein konkreter Sachverhalt unter die Meldepflicht nach Art. 9 GwG fällt, erfolgt immer im konkreten Einzelfall und obliegt ausschliesslich dem Finanzintermediär.

Im Falle einer Meldung sind die verdachtsbegründenden Elemente basierend auf den Erkenntnissen aus den Abklärungen nach Art. 6 GwG zu dokumentieren und gegenüber der MROS nachvollziehbar darzulegen.

3 Negativtypologien - Einzelne Konstellationen

3.1 Typologie 1 – «Die versuchte Kontoeröffnung»

Die MROS erhält vermehrt Verdachtsmeldungen im Zusammenhang mit abgebrochenen Online-Onboarding-Vorgängen, bei denen weder eine Geschäftsbeziehung zustande kam noch ein Geldfluss stattgefunden hat (Art. 9 Abs. 1 Bst. b GwG). Auffällig ist in diesen Konstellationen, dass die meldenden Finanzintermediäre häufig gar keinen Kundenkontakt hatten, keine vollständige Kundenidentifikation vornehmen konnten und in der Regel über keine Informationen zu wirtschaftlich Berechtigten verfügten oder Hinweise auf eine strafbare Vortat im Sinne von Art. 305bis oder Art. 260ter StGB[2] vorlagen.

Solche Meldungen basieren häufig nicht auf objektiv nachvollziehbaren Anhaltspunkten für Geldwäscherei oder Terrorismusfinanzierung im Sinne des GwG. Ein rein technischer Abbruch – etwa während des ID/Pass-Uploads, der Videoidentifikation oder der Dokumentenübermittlung – stellt keinen ausreichend begründenden Verdacht für eine Verdachtsmeldung dar. Auch ein Abbruch durch den potenziellen Kunden aus Desinteresse oder Bedienungsschwierigkeiten erfüllt nicht die Schwelle eines meldepflichtigen Verdachts, solange keine weiteren geldwäschereirelevanten Auffälligkeiten vorliegen. In diesen Fällen fehlt es an objektivierbaren, nachvollziehbaren Verdachtsmomenten, die einen begründeten Verdacht im Sinne von Art. 9 Abs. 1 Bst. b GwG stützen würden. Die zwischenzeitlich stark technologisierte Abwicklung des Onboardings, insbesondere über Mobile Apps oder Webportale, führt dazu, dass es im Rahmen des Prozesses häufig zu abbruchbedingtem Nichtzustandekommen von Geschäftsbeziehungen kommt. Es fehlt in solchen Konstellationen an konkreten, objektiv überprüfbaren Verdachtsmomenten, die auf eine strafbare Vortat im Sinne von Art. 305bis StGB oder auf eine Verbindung zu einer kriminellen oder terroristischen Organisation nach Art. 260ter Abs. 1 StGB hindeuten.

Die Ausweitung der Meldepraxis auf solche rein formalen oder technischen Fälle widerspricht dem Sinn und Zweck von Art. 9 GwG und belastet die MROS sowie die Strafverfolgungsbehörden mit nicht verwertbaren Informationen. Die MROS kann solche Meldungen inhaltlich kaum verwerten, da sie auf blossen Vermutungen oder generalisierten Risikoeinschätzungen beruhen, ohne konkrete Anhaltspunkte für Geldwäscherei oder Terrorismusfinanzierung zu begründen.

3.2 Typologie 2 – «Auffällige Kunden ohne erkennbaren Bezug zu inkriminierten Vermögenswerten»

Die MROS erhält regelmässig Verdachtsmeldungen, in denen Finanzintermediäre lediglich allgemeine Auffälligkeiten im Kundenverhalten schildern – ohne dass die konkreten Hinweise auf inkriminierte Vermögenswerte oder deren Herkunft eindeutig bezeichnet werden (Was hat zu welchem Zeitpunkt den Ausschlag für die Abklärungen gegeben und welche Hinweise oder Anhaltspunkte konnten durch die Abklärungen nicht ausgeräumt werden?). Solche Meldungen basieren oftmals auf diffusen Unstimmigkeiten oder subjektiv wahrgenommenen Risikofaktoren, wie z.B. ein «unplausibles Geschäftsmodell» ohne nachvollziehbare Erklärung, häufige Wechsel der wirtschaftlich berechtigten Personen oder überdurchschnittliche Komplexität der juristischen Struktur eines Kunden.

Obschon solche Faktoren grundsätzlich Elemente einer risikoorientierten Kundenüberwachung sein können, reichen sie in ihrer isolierten Form in der Regel nicht aus, um den gesetzlichen Schwellenwert für eine Verdachtsmeldung nach Art. 9 GwG zu erfüllen. Die MROS stellt fest, dass viele dieser Meldungen im narrativen Teil vage bleiben und sich auf allgemeine Einschätzungen beschränken – ohne nachvollziehbaren Bezug zu einer konkreten strafbaren Vortat im Sinne von Art. 305bis StGB (z. B. Betrug, Veruntreuung, Korruption, qualifizierte Steuerdelikte).

Ein begründeter Verdacht im Sinne des GwG erfordert mehr als eine risikoorientierte Bewertung. Er setzt objektiv nachvollziehbare Anhaltspunkte voraus, die einen Zusammenhang zu mutmasslich deliktisch erlangten Vermögenswerten erkennen lassen.

[2] Schweizerisches Strafgesetzbuch, SR 311.0.

3.3 Typologie 3 – «Die Drittinformationen»

Die MROS erhält regelmässig Verdachtsmeldungen, welche auf Drittinformationen beruhen, zum Beispiel im Zusammenhang mit Medienberichten oder Editions- sowie Beschlagnahmeverfügungen von in- oder ausländischen Strafverfolgungsbehörden. Diese Informationen können für Finanzintermediäre Anlass für weiterführende Abklärungen darstellen. Für eine Verdachtsmeldung im Sinne von Art. 9 GwG ist entscheidend, dass der Finanzintermediär im Rahmen seiner geldwäschereirelevanten Abklärungen einen Bezug dieser Informationen zu seinen eigenen Geschäftsbeziehungen herstellt und nicht ausschliesslich Drittinformationen weiterleitet. Als spezifische Typologien können nachfolgende Beispiele aufgeführt werden:

3.3.1 Typologie 3.1 – «Die Editionsverfügung»

Die blosse Zustellung einer Editions- oder Beschlagnahmeverfügung durch eine Strafverfolgungsbehörde stellt für sich allein keinen meldepflichtigen Sachverhalt dar. Diese strafprozessualen Massnahmen dienen der Beweissicherung im Rahmen laufender Ermittlungen oder Strafverfahren und betreffen häufig spezifische Kundenbeziehungen, Kontobewegungen oder Transaktionsverläufe.

Erhält ein Finanzintermediär eine solche Verfügung, ist zu prüfen, ob über deren Inhalt hinaus zusätzliche, eigene Erkenntnisse vorliegen, die einen begründeten Verdacht auf Geldwäscherei, deren Vortaten, organisierte Kriminalität oder Terrorismusfinanzierung stützen könnten (Art. 9 Abs. 1 GwG i.V.m. Art. 6 GwG).

3.3.2 Typologie 3.2 – «Das TWINT-Konto»

Eine weitere Typologie von Verdachtsmeldungen ergibt sich im Zusammenhang mit der Bezahl-App TWINT. Diese Meldungen beruhen häufig auf Informationen, wonach ein TWINT-Konto in ein polizeiliches Ermittlungsverfahren involviert sei – beispielsweise infolge einer Mitteilung durch eine Strafverfolgungsbehörde, eines behördlichen Auskunftsersuchens oder eines informellen Hinweises. In einer Vielzahl dieser Fälle wird jedoch keine konkrete Verdachtslage geschildert, sondern lediglich auf die angebliche «Involvierung» hingewiesen – ohne weitere Angaben zu den Hintergründen, zum Deliktskontext oder zur betroffenen Person. Solche pauschalen Hinweise begründen für sich allein noch keinen meldepflichtigen Verdacht im Sinne von Art. 9 Abs. 1 GwG. Vielmehr bedarf es zusätzlicher, durch den Finanzintermediär selbst gewonnener Erkenntnisse, welche einen Bezug zu Geldwäscherei, deren Vortaten, organisierter Kriminalität oder Terrorismusfinanzierung erkennen lassen.

Die blosse pauschale Nennung eines TWINT-Kontos im Rahmen polizeilicher Abklärungen genügt nicht, um die erforderliche Schwelle eines «begründeten Verdachts» zu erreichen. Finanzintermediäre sollten bei TWINT-bezogenen Sachverhalten sorgfältig prüfen, ob eigene Beobachtungen oder interne Analysen zusätzliche verdachtsbegründende Elemente liefern (Art. 6 GwG), welche die Voraussetzungen für die Erstattung einer Verdachtsmeldung nach Art. 9 GwG erfüllen.

3.3.3 Typologie 3.3 – «Medienberichte»

Auch Medienberichte über Kunden eines Finanzintermediärs oder deren mutmassliches Fehlverhalten reichen allein nicht aus, um eine Meldung nach Art. 9 GwG zu begründen. Der Finanzintermediär muss die Informationen in den Medienberichten in einen konkreten Bezug zu seinen Geschäftsbeziehungen oder zu ungewöhnlichen Transaktionen setzen und die Erkenntnisse, die er im Rahmen seiner Abklärungen (Art. 6 GwG) gewonnen hat, in der Meldung darstellen.

3.4 Typologie 4 – «Die Nutzung von Kryptobörsen»

Die MROS verzeichnet eine zunehmende Anzahl von Verdachtsmeldungen, bei denen ausschliesslich die Nutzung von Kryptowährungen oder die Inanspruchnahme von Krypto-Dienstleistungen als verdachtsbegründendes Element angeführt wird. Solche Meldungen stützen sich in der Regel ausschliesslich auf den Umstand, dass Kunden z.B. Fiatgeld in Kryptowährungen tauschen (bzw. umgekehrt), Kryptowährungen auf Konten einzahlen, die bei Kryptobörsen geführt werden oder Zahlungen (etwa Löhne, Honorare oder Dienstleistungen) in Kryptowährungen empfangen.

Die MROS stellt in diesen Fällen regelmässig fest, dass die Darstellung des Sachverhalts sehr vage bleibt und sich auf die blosse Nennung des Kryp-

to-Bezugs beschränkt. Es fehlen häufig substanzielle Angaben zu effektiv getätigten Transaktionen, zur wirtschaftlichen Berechtigung, zur Herkunft der Mittel oder zu einem möglichen Deliktskontext. Der alleinige Verweis auf die Verwendung von Kryptowährungen oder die Beteiligung eines Krypto-Dienstleisters genügt jedoch nicht, um einen «begründeten Verdacht» im Sinne von Art. 9 GwG darzustellen.

Die Nutzung von Kryptowährungen ist per se nicht verdächtig. Sie stellt – analog zur Nutzung ausländischer Bankverbindungen, Barzahlungen oder Treuhandkonstruktionen – ein potenzielles Risikoelement dar, das einer differenzierten risikoorientierten Abklärung unterzogen werden muss. Eine Verdachtsmeldung an die MROS ist nur dann gerechtfertigt, wenn über die Risikoeinschätzung hinaus konkrete Tatsachen vorliegen, die auf eine mögliche Geldwäschereihandlung oder eine strafbare Vortat hindeuten.

3.5 Typologie 5 – «Opferkonten»

«Opferkonten» stellen aus Sicht der MROS eine besondere Kategorie von Verdachtsmeldungen dar. Es handelt sich in der Regel um Konstellationen, in denen Kundinnen und Kunden zwar über rechtmässig erworbene Mittel verfügen, diese jedoch infolge von Betrug oder durch den Verlust von Zahlungsmitteln unverschuldet in einen deliktischen Zusammenhang geraten.

3.5.1 Typologie 5.1 – «Der Kunde als Opfer»

Die MROS erhält regelmässig Verdachtsmeldungen, bei welchen über die Mittelherkunft keine Zweifel bestehen und die Inhaber der Mittel Opfer von betrügerischen Handlungen wurden. In der Praxis handelt es sich dabei häufig um sogenannte «Opferkonten», über welche redliche Kundinnen und Kunden – beispielsweise im Rahmen von Love Scams oder Anlagebetrug– Vermögenswerte an Täterschaften (in der Regel mit Sitz im Ausland) transferieren.

Die Meldepflicht gemäss GwG bezweckt die Unterbindung von Geldwäscherei im Zusammenhang mit deliktisch erlangten Vermögenswerten . Bei reinen Opferkonten ist dieser Zusammenhang in der Regel nicht gegeben, da es sich um legitime Vermögenswerte handelt, die erst nach dem Abfluss kriminellen Akteuren zugeführt werden. Der Transfer selbst mag zwar strafrechtlich relevant sein – die relevanten strafprozessualen Massnahmen richten sich jedoch primär gegen die Empfänger der Gelder und nicht gegen den Geschädigten, der seine Gelder legal erwirtschaftet hat und dies dokumentieren kann.

3.5.2 Typologie 5.2 – «Die gestohlene Debit-/Kreditkarte»

Die MROS erhält regelmässig Verdachtsmeldungen im Zusammenhang mit gestohlenen oder verlorenen Kredit- bzw. Debitkarten. Diese Meldungen erfolgen häufig unmittelbar nach der Verlustmeldung durch die betroffene Kundin oder den betroffenen Kunden, ohne dass deliktische Transaktionen stattgefunden haben. In diesen Konstellationen handelt es sich um den klassischen Fall der Meldung eines Opferkontos, bei dem die betroffene Person unverschuldet einen Vermögensgegenstand (in diesem Fall eine Zahlungskarte) verliert oder gestohlen wird.

Meldungen, die sich allein auf den Kartenverlust ohne jegliche Folgehandlung oder Kontextinformation stützen, entfalten für die MROS keinerlei verwertbaren Analysewert. Eine Weiterbearbeitung ist in solchen Fällen nicht möglich, da weder das Objekt der Meldung (die Zahlungskarte) noch deren Nutzung kriminalitätsrelevante Merkmale aufweist. Die blosse Tatsache, dass eine Zahlungskarte abhandengekommen ist, genügt nicht für die Annahme eines begründenden Verdachts auf Geldwäscherei, deren Vortaten, organisierte Kriminalität oder Terrorismusfinanzierung. Erst wenn der Finanzintermediär aufgrund der Durchführung der besonderen Sorgfaltspflichten nach Art. 6 GwG zu weiteren geldwäschereirelevanten Informationen gelangt, kann sich ein relevanter Anfangsverdacht ergeben. Solange die Kartennutzung nicht erfolgt oder keine missbräuchliche Verwendung feststellbar ist, liegt kein Bezug zu deliktisch erlangten Vermögenswerten vor – und damit auch kein begründeter Verdacht für eine Verdachtsmeldung im Sinne von Art. 9 GwG.

3.6 Typologie 6 – «Der Finanzintermediär als Betrugsopfer»

Die MROS erhält regelmässig Meldungen von Finanzintermediären, deren Institut selbst Opfer von

betrügerischen Handlungen wurde. Solche Konstellationen betreffen in der Praxis häufig Cyberangriffe oder Social-Engineering-Fälle (z. B. CEO-Fraud) oder interne Fehlleitungen infolge manipulierten Zahlungsverkehrs.

In diesen Konstellationen werden Vermögenswerte des Finanzintermediärs selbst – etwa aus betriebseigenen Konten – an Täterschaften, die oft im Ausland operieren, transferiert. Der Finanzintermediär erleidet dadurch einen unmittelbaren finanziellen Schaden. Dabei handelt es sich jedoch um Vermögenswerte legitimer Herkunft, ohne Hinweis auf einen Zusammenhang mit strafbaren Vortaten Dritter oder geldwäschereirelevanten Vorgängen.

Die Meldepflicht gemäss Art. 9 GwG setzt einen begründeten Verdacht auf deliktisch erlangte Vermögenswerte voraus. Wenn jedoch das meldende Institut selbst geschädigt ist und seine eigenen Mittel irrtümlich oder betrugsbedingt an eine Täterschaft weiterleitet, fehlt in der Regel jeglicher Bezug zu einer Vortat zur Geldwäscherei im Sinne des Gesetzes. Solche Konstellationen sind daher nicht Gegenstand der Meldepflicht an die MROS.

3.7 Typologie 7 – «Schwarze Kassen»

Die MROS erhält regelmässig Verdachtsmeldungen im Zusammenhang mit sogenannten «Schwarzen Kassen», d. h. mit Vermögenswerten, die gemäss Einschätzung des meldenden Finanzintermediärs potenziell dazu bestimmt sein könnten, zukünftig als Bestechungsgelder eingesetzt zu werden. Diese Meldungen erfolgen häufig im Kontext internationaler Geschäftsbeziehungen, insbesondere bei erhöhten Korruptionsrisiken (z. B. im Rohstoffhandel, Bauwesen, Energieversorgung oder bei grenzüberschreitenden Staatsaufträgen).

Die Annahme, dass bestimmte Gelder zukünftig für eine unzulässige Einflussnahme eingesetzt werden könnten, genügt für sich allein nicht, um die gesetzlichen Voraussetzungen für eine Verdachtsmeldung gemäss Art. 9 Abs. 1 GwG zu erfüllen. Solange die betroffenen Vermögenswerte aus einer legalen Quelle stammen – etwa aus dem ordentlichen Geschäftsbetrieb – und (allenfalls hypothetisch) für eine künftig begangene strafbare Handlung vorgesehen sind, fehlt es an der im Geldwäschereigesetz vorausgesetzten deliktischen Herkunft. Entscheidend ist, dass die Geldwäschereitatbestände gemäss Art. 305bis StGB zwingend eine bereits begangene Vortat voraussetzen, welche zu deliktisch erlangtem Vermögen geführt hat (z. B. durch Bestechung, ungetreue Geschäftsbesorgung oder Betrug). Erst wenn die Bestechungshandlung tatsächlich stattgefunden hat – insbesondere, wenn ein Zahlungseingang auf dem Konto des mutmasslich bestochenen Amtsträgers oder Funktionsträgers erfolgt – kann der Tatbestand einer Vortat erfüllt sein. In solchen Fällen kann beim kontoführenden Finanzintermediär ein begründeter Verdacht entstehen, dass Vermögenswerte deliktischer Herkunft vorliegen, wodurch die Meldepflicht ausgelöst wird.

3.8 Typologie 8 – «Das Börsendelikt ohne in der Schweiz kotierte Titel»

In der Praxis erhält die MROS regelmässig Verdachtsmeldungen im Zusammenhang mit mutmasslichen Börsendelikten gemäss Art. 142 (Insiderhandel) und Art. 143 FinfraG[3] (Marktmanipulation). Beide Deliktstypen gelten unter bestimmten Voraussetzungen als qualifizierte Vortaten zur Geldwäscherei im Sinne von Art. 305bis StGB.

Gemäss Art. 154 Abs. 2 und Art. 155 Abs. 2 FinfraG qualifizieren Insiderhandel und Marktmanipulation erst ab einem durch die strafbare Handlung erzielten Vermögensvorteil von mehr als einer Million Franken als Verbrechen im Sinne des Strafgesetzbuches. Nur dann liegt eine Vortat zur Geldwäscherei vor, welche eine Meldung nach Art. 9 GwG rechtfertigen kann – vorausgesetzt, es bestehen begründete Verdachtsmomente hinsichtlich der deliktischen Herkunft der Vermögenswerte.

Für die Meldepflicht ist zu beachten, dass die Strafnormen der Artikel 142 und 143 FinfraG nur dann zur Anwendung kommen, wenn sich die mutmasslich missbräuchlichen Handelsaktivitäten auf Effekten beziehen, die an einem in der Schweiz domizilierten Handelsplatz oder DLT-Handelssystem zum Handel zugelassen sind. Sofern diese Voraussetzungen nicht erfüllt sind und insbesondere keine An-

[3] Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel (Finanzmarktinfrastrukturgesetz, FinfraG), SR 958.1.

haltspunkte für eine inkriminierte Herkunft der Vermögenswerte bestehen, schafft das Absetzen einer Verdachtsmeldung an die MROS keinen Mehrwert für die Bekämpfung der Geldwäscherei.