Fälle

1. Verdacht auf Veruntreuung

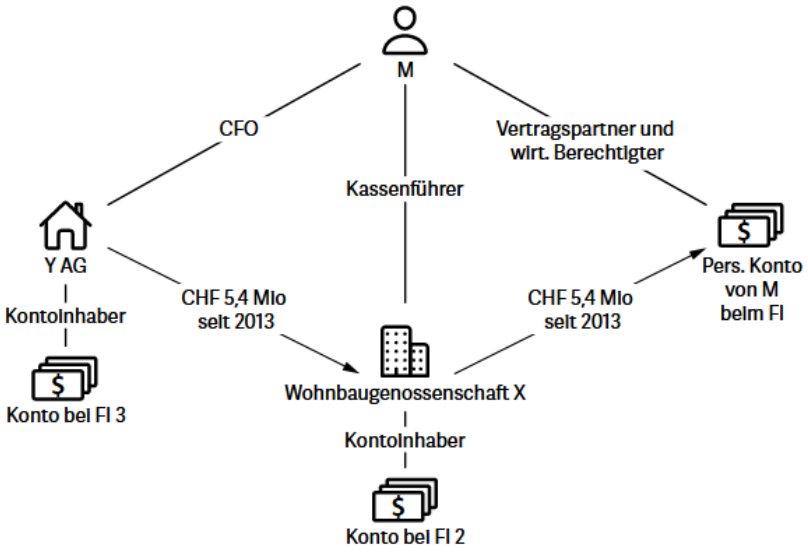
Sachverhalt

Der Kundenberater eines Finanzintermediärs (nachfolgend FI) stellt auf dem Privatkonto von M. unübliche eingehende Transaktionen fest, die auf die Wohnbaugenossenschaft X zurückgehen. Gemäss Kundenprofil des FI ist Kunde M. Kassenführer der Wohnbaugenossenschaft X und zudem CFO und Verwaltungsratsmitglied des Bauunternehmens Y AG.

Aus der Transaktionsanalyse des FI geht hervor, dass die auf M. lautende Geschäftsbeziehung primär durch Mittel der Wohnbaugenossenschaft X alimentiert worden ist. Die ungewöhnlich hohen Gutschriften lassen sich jedoch nicht durch Lohnzahlungen an den Kunden für seine Tätigkeit als Kassenführer erklären. Insgesamt wurden über CHF 5 Mio. von einem auf die Wohnbaugenossenschaft X lautenden Konto bei einem anderen Finanzintermediär auf das Privatkonto von M. überwiesen.

Der FI kontaktiert den Kunden, der zunächst erklärt, er erhalte Provisionen für Bauprojekte, die er auf eigene Rechnung führe. Der FI kann jedoch nicht klären, warum und für welche Projekte seinem Kunden in dieser Eigenschaft Gelder von der Wohnbaugenossenschaft X zufliessen. Aus der Dokumentation, die M. dem FI bei einem Treffen vorlegt, scheint hervorzugehen, dass die vom Konto der Wohnbaugenossenschaft X überwiesenen Gelder in Wirklichkeit von der Y AG stammen, bei der M. als CFO amtet. Die Gelder wurden über das Konto der Wohnbaugenossenschaft X transferiert. Der FI kann jedoch die Echtheit der vorgelegten Dokumentation nicht überprüfen, und das Treffen bringt auch keine Klarheit über die wirtschaftlichen Hintergründe der Transaktionen.

Das Transaktionsschema verstärkt vielmehr die Zweifel des FI. Die auf das Privatkonto des Kunden M. gutgeschriebenen Gelder könnten aus Veruntreuung stammen, die M. möglicherweise als Kassenführer bei der Wohnbaugenossenschaft X oder als CFO bei der Y AG begangen hat. Die Tatsache, dass der Verwaltungsrat des Bauunternehmens Y AG unmittelbar vor den ersten Transaktionen den Verzicht auf eine ordentliche oder eingeschränkte Revision beschlossen hatte, verstärken die Zweifel des FI. Er schliesst auf eine potenzielle Veruntreuung und meldet die Geschäftsbeziehung mit M. der MROS.



Lösung

Aufgrund der Identifizierung und Dokumentierung des mutmasslichen Transaktionsschemas konnte die MROS präzise Auskunftsbegehren nach Art. 11a Abs. 2 und 3 GwG formulieren und noch fehlende Informationen zu diesem Transaktionsschema einholen.

«Good Practices» des meldenden Finanzintermediärs

- **Der Kundenberater war aufmerksam und entdeckte die verdächtigten Transaktionen**, worauf die Compliance-Abteilung den Fall übernehmen und ergänzende Abklärungen einleiten konnte. Dies zeigt, wie wichtig die Funktion der Kundenberater als erste Verteidigungslinie bei der Geldwäschereibekämpfung auf Ebene der Finanzintermediäre ist. Verdächtige Aktivitäten auf den Geschäftsbeziehungen ihrer Kunden müssen rechtzeitig erkannt und abgeklärt werden, damit allenfalls nötige Massnahmen rasch in die Wege geleitet werden können.

- **Die MROS konnte dank der präzisen Dokumentation des IF gezielte Abklärungen vornehmen.** Auch wenn die MROS bei ihren Analysen oft neue Spuren entdeckt, stellen die Dokumentation und Einschätzung des Finanzintermediärs der Ausgangspunkt der MROS-Analyse dar. Sind die an die MROS übermittelten Informationen vollständig und präzise, erhöht sich auch die Effizienz der Meldestelle.

2. Verdacht auf Menschenhandel / Zwangsprostitution

Sachverhalt

Auf dem Konto einer Kundin, die gemäss eigenen Angaben einen Beauty-Salon betreibt, beobachtet der Finanzintermediär (FI) folgendes verdächtiges Transaktionsverhalten: während eines Jahres wurde die Geschäftsbeziehung durch häufige Bareinzahlungen in Gesamthöhe von über CHF 70’000 alimentiert. Diese Einzahlungen wurden, nebst der Vertragspartnerin selbst, von verschiedenen weiblichen Drittpersonen getätigt. Auffallend ist, dass diese Gelder teilweise in einer Schweizer Stadt eingezahlt wurden und in den darauffolgenden Tagen in einer anderen Schweizer Stadt, oder teilweise auch in europäischen Drittländern, abgehoben wurden. Die Transaktionsanalyse und weiteren Abklärungen zeigen, dass sowohl die Vertragspartnerin als auch die weiblichen Drittpersonen Verbindungen zum Rotlichtmilieu aufweisen.

Bei einer der Durchlauftransaktionen an ein europäisches Drittland kann der FI bei seinen Nachforschungen eruieren, dass der Empfänger der angebliche Lebenspartner der Vertragspartnerin ist. Bei den weiteren Abklärungen zu dieser Person stösst der FI auf einen relevanten World-Check Treffer. Dieser bringt den Geldempfänger und angeblichen Lebenspartner der Vertragspartnerin mit organisierter Kriminalität und Menschenhandel in Verbindung.

Der FI bemerkt zudem regelmässige und häufige Zahlungen für Werbungen auf Adult Entertainment Plattformen. Die Häufigkeit der Werbekäufe lässt darauf schliessen, dass die Zahlungen für mehrere Personen getätigt werden. Zudem erfolgen Mietzahlungen für mehrere Mietobjekte, was in Anbetracht des Kundenprofils auffallend ist. Schliesslich geben auch das Verhalten und die inkohärent und nicht plausibel wirkenden Angaben der Vertragspartnerin dem FI Anlass, die Geschäftsbeziehung genauer unter die Lupe zu nehmen. Sie gibt an, einen Beauty-Salon zu betreiben und die eingangs erwähnten Zahlungen von weiblichen Drittpersonen entsprächen den Zahlungen für in Anspruch genommene Schönheitsbehandlungen. Dies belegt die Vertragspartnerin mit entsprechenden Rechnungen. Der FI kann jedoch anhand von Open Source Recherchen keinen Beauty-Salon mit dem angegebenen Namen und mit Verbindung zur Vertragspartnerin identifizieren. Ausserdem hat er Zweifel an der Authentizität der eingereichten Rechnungsbelege. So scheinen z. B. bei einer Person unüblich viele Behandlungen durchgeführt worden zu sein; die Vertragspartnerin weilte in der Zeit im Ausland, in welcher sie

angeblich die Behandlungen durchführte oder den mutmasslichen Kundinnen wurden für identische Behandlungen/Leistungen unterschiedliche Preise verrechnet.

Lösung

«Good practices» des meldenden Finanzintermediärs

- **Der Finanzintermediär hat die verdächtigen Bewegungen zeitnah bemerkt und nach seinen Abklärungen unverzüglich eine Meldung erstattet.** Eine zeitnahe Absetzung der Meldung ist für die effiziente Arbeit der Meldestelle essentiell. Einerseits erhöht es die Chancen einer Nachverfolgung oder gar Sperrung der Mittel, andererseits können die Informationen allenfalls für bereits laufende Verfahren in der Schweiz oder im Ausland eine nützliche Ergänzung darstellen.
- **Es wurden ausführliche Open Source Recherchen durchgeführt.** So wurden unter anderem die involvierten Personen sowie deren mutmassliche Adressen überprüft. Dabei wurden bei den verschiedenen involvierten Personen Verbindungen zum Rotlichtmilieu gefunden. Zudem erlaubte die World Check Suche dem Finanzintermediär wichtige Informationen über einen der Geldempfänger, den angeblichen Lebenspartner der Vertragspartnerin, zu sammeln.
- **Tipping off: Die Vertragspartnerin wurde diskret zu allen verdächtigen Transaktionen befragt. Inkohärente, inkomplette oder verdächtige Aussagen der Vertragspartnerin wurden dokumentiert und ausgeführt.** Befragungen von Vertragspartnerinnen und Vertragspartnern sind ein wichtiger Teilaspekt jener Informationen, die im Falle einer Meldung an die MROS übermittelt werden (sofern dies möglich ist, ohne die betroffenen Kunden zu alarmieren bezüglich des gegen sie erhobenen Verdachts). Die MROS hat nicht die Befugnis Vertragspartnerinnen und Vertragspartner direkt zu kontaktieren. Somit muss sich die Meldestelle hierfür auf die Informationen abstützen, die der Finanzintermediär einholen konnte. Oft liefert das Verhalten der Vertragspartnerinnen und Vertragspartner, wie z. B. die Kohärenz oder Wahrheit ihrer Aussagen, Indizien, die der MROS bei der Analyse einer Verdachtsmeldung hilfreich sein können. Dabei ist es aber wichtig, dass der Finanzintermediär diese Informationen und Indizien auch kritisch hinterfragt und der MROS alle verfügbaren Elemente liefert, um ihre Verlässlichkeit einschätzen und allenfalls überprüfen zu können. Der Finanzintermediär kennt seine Kundinnen und Kunden am besten und sollte diesen Vorteil in die Analyse einfliessen lassen.
- **Es wurde eine detaillierte Transaktionsanalyse durchgeführt und die wichtigen Bewegungen präzise zusammengefasst.** Unter anderem wurden Abklärungen zu den Gegenparteien getroffen und von der Vertragspartnerin eingereichte Rechnungen zur Begründung der auffälligen Zahlungen im Detail analysiert und die inhaltliche Plausibilität untersucht.
- **Die übermittelten Dokumente/ Beilagen waren komplett und jedes Verdachtsmoment war dokumentiert.** Es mussten keine fehlenden Dokumente eingefordert werden. Nachträgliche Einforderungen von Dokumenten i.S.v. Art. 11a Abs. 1 GwG sind zeitaufwändig, sowohl für MROS als auch für den meldenden Finanzintermediär. Gemäss Art. 3 Abs. 1 lit. H MGwV hat der meldende Finanzintermediär sicherzustellen, dass die Verdachtsmomente, auf die sich seine Meldung stützt, möglichst genau dargelegt, und alle sachdienlichen Unterlagen übermittelt werden.

Fazit

Kenntnisse der verschiedenen Charakteristiken und Indikatoren von Geldwäscherei-Vortaten sind eine wichtige Voraussetzung für eine effiziente Compliance Strategie. Verschiedene Anzeichen bzw. Kombinationen von Anzeichen deuten auf unterschiedliche Vortaten hin. So können z.B. bei Menschenhandel andere Indikatoren identifiziert werden als bei Korruptions- oder Betrugsfällen.

Im vorliegenden Fall hat der Finanzintermediär wichtige Indikatoren zur Erkennung von Menschenhandel oder Zwangsprostitution hervorgehoben, unter anderem die folgenden[1]:

- Häufige Bareinzahlungen – Alimentierungen des Kontos in Stadt x mit korrespondierenden Barabhebungen in Stadt y (Durchlauftransaktionen)
- Transfers von relativ niedrigen Geldbeträgen
- Vielzahl von Personen, die Einzahlungen vornehmen oder Auszahlungen erhalten
- Ausgehende internationale Geldtransfers an Personen und Firmen in Ländern aus denen überproportional viele Opfer von Menschenhandel stammen
- Wiederkehrende und häufige Zahlungen für Werbungen auf Adult Entertainment Plattformen
- Häufige Ausgaben für unterschiedliche Hotels/Mietobjekte
- Ausgaben, die sich nicht mit dem KYC der Kundin/ des Kunden decken
- Verbindungen zum Rotlichtmilieu

Die Vertragsbeziehung wurde basierend auf einem holistischen Ansatz gemeldet. Die verschiedenen Elemente sind isoliert betrachtet noch nicht unbedingt verdächtig; eine Verbindung zum Rotlichtmilieu ist zum Beispiel an sich noch kein ausreichender Verdachtsgrund – Sexarbeit ist in der Schweiz unter Einhaltung gewisser Regeln legal. In Kombination mit anderen verdächtigen Faktoren, wie im vorliegenden Fall dem World Check Treffer, können diese verschiedenen Elemente aber indikativ für eine zugrundeliegende Vortat sein. Durch den holistischen Ansatz des meldenden Finanzintermediärs konnten Verbindungen hergestellt werden, die bei einem einseitigen Ansatz (Fokus auf isolierte Teilgebiete der Geschäftsbeziehung wie z.B. auf die Transaktionen oder die KYC Aspekte) unentdeckt geblieben wären.

3. Verdacht auf berufsmässige Geldwäscherei

Sachverhalt

Ein Finanzintermediär (FI) überwacht das Privatkonto eines Anwalts, der schon seit einigen Jahren nicht mehr im Anwaltsregister eingetragen ist. Er stellt eine Vielzahl von Auftraggebern fest, deren Überweisungen rasch auf andere Konten in der Schweiz oder im Ausland transferiert werden. Das Konto wurde demnach als Durchlaufkonto verwendet, und der Anwalt spielte die Rolle eines «Escrow Agent». An diesem Punkt bittet der FI seinen Kunden um Erklärungen zu diesen Aktivitäten. Er stellt fest, dass der Kunde Dritten gegenüber als zugelassener Anwalt auftritt, was er seit mehreren Jahren nicht mehr ist. Der Anwalt erklärt, er vertrete zwar keine Mandanten mehr vor Gericht, leiste aber weiterhin Rechtsberatung für seine Klienten. Insbesondere stellte er den Kunden auch sein Konto zur Verfügung. Nach Darstellung des ehemaligen Anwalts könne einer seiner Klienten bestimmte Transaktionen aufgrund von Geldwäscherei-Präventionsmassnahmen nicht mehr vornehmen. Der Anwalt legt dem FI verschiedene Rechtsakten vor, die seine Darstellung stützen. Der FI stellt seinerseits Nachforschungen über die Gegenparteien der Transaktionen auf dem Konto des Anwalts an und stösst dabei auf negative Presseberichte und andere nachteilige Informationen. Gegen einen der Klienten des Anwalts läuft offenbar ein Strafverfahren im Ausland.
Da sich die Zweifel nicht ausräumen lassen, dass der Anwalt für einen Klienten Geld gewaschen hat, meldet der FI das Privatkonto des Anwalts an die MROS.

Lösung

«Good Practices» des meldenden Finanzintermediärs

- **Der Finanzintermediär richtete seine Nachforschungen und Abklärungen bezüglich seines Kunden nach dessen Kundenprofil aus**, nachdem er bei der Transaktionsanalyse

[1] Vgl. z. B. den GAFI Report Financial Flows from Human Trafficking, Juli 2018, für detailliertere Ausführungen zu Indikatoren und Fallstudien zur Erkennung von Menschenhandel und verwandten Vortaten.

feststellte, dass verschiedene Eingänge von Dritten stattfanden und das Konto als Durchlaufkonto verwendet wurde.

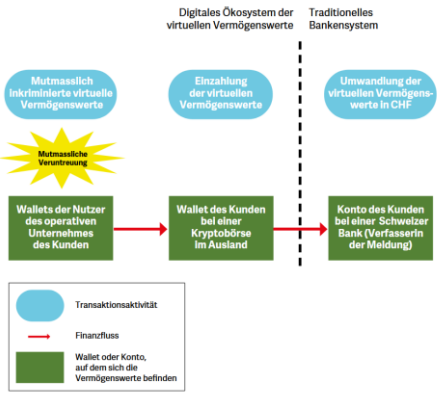
– **Der Finanzintermediäre stellte vertiefte Nachforschungen zu den Gegenparteien an** und stiess auf negative Informationen, welche er präzise dokumentierte.

4. Verdacht auf Veruntreuung von virtuellen Vermögenswerten

Sachverhalt

Mehrere Kunden eines Finanzintermediärs aus dem Bankensektor (nachfolgend FI) sind offenbar im Bereich der virtuellen Vermögenswerte aktiv, namentlich über eines ihrer operativen Unternehmen, wobei es sich um eine Handels- und Investitionsplattform für Kryptowährungen handle. Ihr Vermögen hatten sie anscheinend mehrheitlich mit diesem Unternehmen und frühzeitigen Investitionen in Kryptowährungen erwirtschaftet. Im Zuge einer dringenden Anfrage einer dieser Kunden, die dem FI ungewöhnlich erscheint, richtet der FI ein besonderes Augenmerk auf diese Geschäftsbeziehungen und bezieht die Compliance-Abteilung mit ein. Parallel dazu fällt dem FI auf den Konten dieser Kunden ein unübliches Transaktionsverhalten jüngeren Datums auf. In kurzer Zeit wurden einige Hunderttausend Franken in mehreren Überweisungen auf die fraglichen Kundenkonten überwiesen. Die Gelder stammten zum grossen Teil von bekannten Kryptobörsen (Exchanges), die in diversen Ländern registriert sind. Ein Teil der Einlagen ging also offenbar auf den Umtausch oder Verkauf von virtuellen Vermögenswerten zurück. Im vorliegenden Kontext erscheinen diese Transaktionen dem FI gleichwohl verdächtig und er nimmt weitere Abklärungen vor. Der FI vermutet, dass es sich bei diesen Transaktionen um eine mögliche Veruntreuung von Geldern von Kunden bzw. Nutzern der Plattform der Kunden des FI handle. Im weiteren Verlauf fallen dem FI weitere verdächtige Transaktionen auf, die seinen Verdacht verstärken.

Bei seinen Abklärungen grenzt der FI seine Nachforschungen rasch ein und konzentrierte sich auf die Herkunft der Vermögenswerte in Kryptowährungen und deren Steuerkonformität. Die durchgeführten Abklärungen konzentrieren sich relativ schnell auf technische Aspekte wie das Erlangen von Screenshots der Konten seiner Kunden bei den Exchanges und von Nachweisen der Herkunft der Kryptowährungen auf diesen Exchanges, um letztendlich den „paper trail“ nachvollziehen zu können. Ausserdem versucht der FI, Beweise für die Existenz des Vermögens in Kryptowährungen seiner Kunden zu finden, unabhängig davon, ob dieses bei einer Kryptobörse oder über private Wallets (private / self-hosted / unhosted / non-custodial wallet) gehalten wird. Auch die Frage nach der Legitimität des Unternehmens seiner Kunden, welches im Sektor der virtuellen Vermögenswerte tätig ist, ist Teil der Nachforschungen. Die Abklärungen umfassen zum Beispiel die Bewilligungen, die für diese Tätigkeit je nach Land erforderlich sind, sowie die Infragestellung der auf der Website des Unternehmens veröffentlichten Informationen. Nach seinen Abklärungen kommt der FI zum Schluss, dass möglicherweise Gelder von Kunden oder Benutzern der Plattform seiner Kunden veruntreut wurden, und meldet die Geschäftsbeziehungen mit diesen Personen der MROS.



Lösung

«Good Practices» des meldenden Finanzintermediärs

- **Der sogenannt «traditionelle» Finanzintermediär hat ein hervorragendes Verständnis für die Risiken im Bereich der Kryptowährungen bewiesen.** Auch wenn er nicht in der Lage war, alle Abklärungen vorzunehmen, sammelte und dokumentierte er relevante und für die Analyse der MROS wertvolle Informationen über die Herkunft der Gelder und die Geschäftstätigkeit des Unternehmens der Kunden. Die MROS konnte aufgrund dieser Abklärungen drei Auskunftsersuchen an ausländische FIUs stellen. So erhielt die Meldestelle zum Beispiel Informationen zum Ursprung der Guthaben der Kunden des Finanzintermediärs in Kryptowährungen bei einer der im Ausland angesiedelten Kryptobörsen oder auch zur Legitimität des vorgenannten Unternehmens.

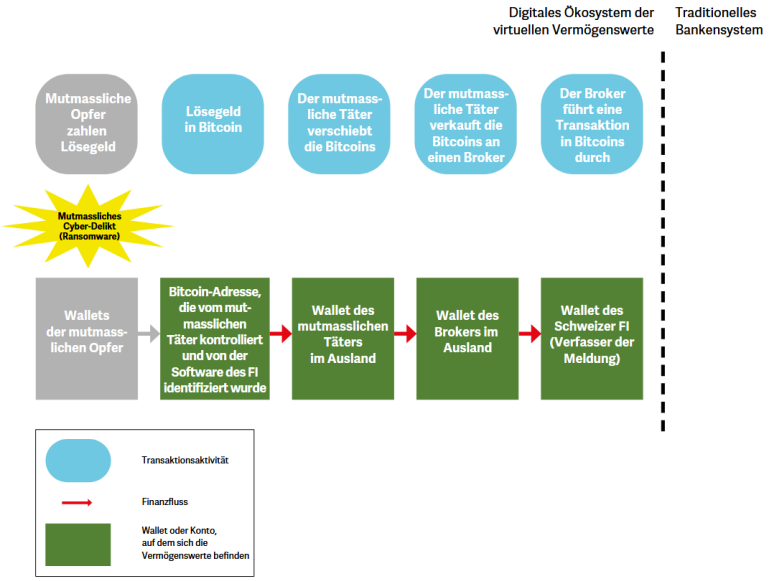
5. Mögliche indirekte Kontamination

Sachverhalt

Der Finanzintermediär (FI) ist in der Vermittlung von Kryptowährungen tätig und kann als Virtual Asset Service Provider (nachfolgend VASP) qualifiziert werden. Im Rahmen der periodischen Überprüfung der Transaktionen zeigt das Blockchain-Analyseprogramm des FI ein erhöhtes Risiko bei Bitcoin-Transaktionen an, die auf Rechnung von Kunden durchgeführt worden waren. Die Warnung des Analyseprogramms schien auf eine indirekte Verbindung zwischen diesen Transaktionen und Straftaten im Bereich der Cyberkriminalität mit Ransomware[2] zurückzugehen.

Die verdächtigen Transaktionen waren im Rahmen des Kaufs von mehreren Dutzend Bitcoins bei einem Geschäftspartner im Ausland durchgeführt worden. Die fraglichen Bitcoins wurden auf Rechnung eines Kunden des FI gekauft. Beim Geschäftspartner handelt es ich um einen OTC-Broker und somit ebenfalls um einen Finanzintermediär des Typs VASP, welcher bestimmten Sorgfaltspflichten unterworfen und bei einer Aufsichtsbehörde registriert ist. Der FI setzt ein Untersuchungsprotokoll in Gang. Die Nachforschungen werden unter anderem auf zwei Ziele ausgerichtet. Erstens versucht der FI, die Situation beim Broker abzuklären, um in Erfahrung zu bringen, ob dieser bereits selbst Abklärungen vorgenommen hatte und zu welchem Resultat er gekommen war. Zweitens führt der FI eine kritische Analyse durch, um zu verstehen, warum das IT-Programm ein hohes Risiko anzeigt und ob dieses Resultat allein Grund genug für eine Meldung an die MROS ist. Dafür wird eine vertiefte Analyse mit Bezug auf die vom Blockchain-Analyse-Programm genutzten Quellen durchgeführt. Es geht darum herauszufinden, ob tatsächlich eine Straftat stattgefunden hat. Für diese Analyse werden unter anderem verschiedene Blockchain-Analyse-Programme einbezogen, um die Transaktionen nachzuverfolgen und die Resultate zu vergleichen. Aufgrund der Analyse des Transaktionsverlaufs sowie der weiteren durchgeführten Abklärungen kommt der FI zum Schluss, dass möglicherweise tatsächlich ein Verbrechen begangen worden war und diesbezüglich eine Verbindung zu einem Kunden seines Geschäftspartners im Ausland besteht. Am Ende des Untersuchungsprotokolls beschliesst der FI, den Fall an die MROS zu melden.

[2] Bei Ransomware handelt es sich um eine Schadsoftware (Malware), die sich auf dem Computer installiert, Daten verschlüsselt und/ oder den Computer blockiert. In den meisten Fällen handelt es sich um eine sogenannte Drive-by-Infection (Infektion durch unbeabsichtigtes Herunterladen). Es reicht dabei, dass das Opfer von einem unzureichend geschützten Computer eine manipulierte Seite aufruft, damit sich die Schadsoftware auf dem Computer installieren kann. Die Täter fordern dann ein Lösegeld, damit die Daten entschlüsselt oder der Computer entsperrt werden kann. Manchmal sendet die Malware auch eine scheinbar offizielle Benachrichtigung, die je nach Land unterschiedliche Polizeilogos verwendet und das Opfer zur Zahlung einer Geldstrafe auffordert.



Lösung

«Good Practices» des meldenden Finanzintermediärs

- **Der Finanzintermediär hat die Abklärungen beim Broker im Ausland und die Blockchain Analyse (mit graphischen Darstellungen) ausgezeichnet dokumentiert, aber auch die Quellen eines der Analyseprogramme kritisch unter die Lupe genommen und hinterfragt.** Die MROS konnte auf dieser Basis ergänzende Analysen vornehmen und die Weiterleitung der Informationen an eine ausländische FIU prüfen.

6. Ausgesuchte Erkenntnisse aus zugestellten Urteilen nach Art. 29a Abs. 1 GwG

Menschenhandel und Förderung der Prostitution

2021 wurden der MROS mehrere, nicht zusammenhängende Urteile im Zusammenhang mit Menschenhandel und der Förderung der Prostitution zugestellt. Zusammengefasst kamen die Opfer, wobei es sich in diesen Fällen ausschliesslich um Frauen und Transpersonen handelte, aus zwei Regionen: Osteuropa und Thailand. Täterschaft und Opfer kamen in beiden Fällen aus demselben Land. Bei den Organisationen, die Menschenhandel betreiben, zeigten sich bei den Fällen mit osteuropäischen und thailändischen Opfern gewisse Gemeinsamkeiten, jedoch auch deutliche Unterschiede in Bezug auf die Organisation und Vorgehensweise der Täterschaft.

Die folgenden Ausführungen beziehen sich auf die Merkmale in Bezug auf thailändische Opfer von Menschenhandel:

Die im Zuge der Verfahren aufgedeckten Organisationsstrukturen wiesen auf zwei «Organisationen» hin, eine in Thailand und eine in der Schweiz. Sowohl in Thailand als auch in der Schweiz war die Täterschaft vorwiegend weiblich. Weibliche Vermittlerinnen rekrutierten die Opfer in Thailand. Die Opfer aus Thailand wussten zwar, dass sie der Prostitution nachgehen werden, waren allerdings über den finanziellen Teil und die Abarbeitungsmodalitäten ihrer Schulden (Vermittlungs-, Reise- und Lebenshaltungskosten) nur rudimentär informiert worden. Die Einreise in die Schweiz erfolgte mittels von den Vermittlerinnen vorgängig organisierten Visen. Oftmals wurden die Opfer als Scheininhaber/-innen von Firmen registriert, was der Beantragung eines Touristenvisums für den Schengen Raum diente. Teilweise wurden mit Hilfe der Schweizer «Organisation» auch gefälschte EU-Reisepässe organisiert, um in der Schweiz eine L-Aufenthaltsbewilligungen erwirken zu können.

In der Schweiz angekommen, wurden die Opfer von Mittelsfrauen abgeholt und in die zugewiesenen Bordelle begleitet. Ab dem Zeitpunkt der Ankunft in der Schweiz waren die Opfer immer begleitet, bzw. unter Beobachtung und somit sozial isoliert. Im Falle von Einreisen mittels gefälschter Reisepässe wurden die Opfer auch bei Behördengängen (Beantragung Visa etc.) begleitet, wobei die Täterschaft teilweise vor der Örtlichkeit der Behörde wartete.

Für die Vermittlung und die Reise mussten die Opfer Schulden in Höhe von ca. CHF 40'000 – 60'000 an die Vermittlerinnen zurückzahlen. Darüber hinaus kamen laufend neue Kosten für Kost und Logis hinzu. Aus den Urteilen war ersichtlich, dass die von den Opfern erzielten Umsätze im Verhältnis 50:50 aufgeteilt wurden, wobei 50% der Umsätze für die Rückzahlung der Vermittlungs- und Reisekosten und 50% als Anteil an die Bordellbetreiberin abzuführen waren. Entsprechend wurden den Opfern jeweils sämtliche Umsätze abgenommen. Transaktionen wurden jeweils von den Bordellbetreiberinnen bzw. Mittelsfrauen ausgeführt. Den Opfern wurde bald klar, dass, wenn überhaupt, nur ein sehr kleiner Teil der erzielten Umsätze in deren Herkunftsland zur Unterstützung der Familie gesendet werden würde.

Wesentlich für die Möglichkeit der Kontrolle der Opfer trotz der schlechten Bedingungen war neben Einschüchterungen die Tatsache, dass die Ansprechpersonen für die Opfer oft ältere Frauen waren. Gemäss den Ausführungen in den Urteilen führte der in Thailand tief verankerte Respekt vor älteren Personen im Folgenden zu einem strikten Gehorsam der Opfer.

Im Hinblick auf die Analyse des erfolgten Transaktionsverhaltens über Geschäftsbeziehungen bei Schweizer Finanzintermediären wurde zur Gänze auf die zugestellten Urteile abgestellt, da in keinem der analysierten Fälle eine Verdachtsmeldung an die MROS erstattet wurde.

Folgende Typologien wurden in den analysierten Urteilen erkennbar:

- Die Opfer verfügten über keine eigenen Geschäftsbeziehungen bei Banken. Die Geschäftsbeziehungen lauteten auf die Täterschaft.
- Die Täterschaft war gemäss den Unterlagen im KYC nicht im Rotlichtmilieu tätig.
- Die einzahlende Täterschaft war in der Regel deutlich älter als die Opfer.
- Die Einnahmen der Täterschaft auf den auf ihren Namen lautenden Geschäftsbeziehungen betrugen ca. CHF 60'000 bis CHF 140'000 jährlich.
- Einzahlungen auf diese Geschäftsbeziehungen der Täterschaft wurden durch Dritte getätigt.
- Die einbezahlten Gelder wurden jeweils nach Thailand an verschiedene Vermittler zur Abzahlung der Vermittlungsgebühren überwiesen.
- Teilweise wurden von den Geschäftsbeziehungen auch kleinere Beträge mittels Banküberweisungen an Familienangehörige der wechselnden Opfer transferiert.
- Weitere Transaktionen erfolgten anstelle von Banküberweisungen via Zahlungsdienstleister an die Vermittler als auch an Familienangehörige der Opfer.

7. Abklärungspflichten (KYC)

Sachverhalt

Vertragspartner: A AG mit Sitz BVI. WiBe hat Nationalität Indien und Wohnsitz in Singapur. Gemäss Banksystem führt der WiBe drei weitere Geschäftsbeziehungen mit der Bank (zwei Stiftungen, bei denen er Errichter und Begünstigter ist, plus eine weitere Sitzgesellschaft mit Sitz in Frankreich).

Assets under Management (AuM): 30 Mio.

Geschätztes Vermögen: unbekannt

KYC: "Servicegesellschaft –keine operative Tätigkeit. Gemäss WiBe (telefonische Auskunft) ist der Grund für die vier Gesellschaften die klare Trennung des Vermögens. WiBe (Nationalität Indien) ist pensioniert, war Juwelier. Vermögen kommt aus Investments."

Wie beurteilen Sie dieses KYC?

Lösung

- Keine Abklärung der Gründe der Verwendung der Sitzgesellschaft ("klare Trennung des Vermögens")
- Zu wenig Informationen und keine Plausibilisierung des Ursprungs des Vermögens ("stammt das Vermögen aus der Juweliertätigkeit oder ist es anderen Ursprungs -"Investments"?")
- Falls "Investments": Angabe zu pauschal und zu knapp
- Mittel der Abklärungen: ungenügend (telefonische Auskunft)

Erwartungen FINMA

- Detaillierte Begründung und Plausibilisierung des Setups
- Informationen zu Source of Wealth und Source of Funds sind immer zu formalisieren und zu plausibilisieren
- Mündliche Auskünfte der Vertragspartei allein genügen nicht

8. Überwachung der Kundenbeziehung

Sachverhalt

Die Privatbank X eröffnet fünf Kundenbeziehungen für den argentinischen Kunden C (Kunde C hat ein Privatkonto) und seine im Bereich Sportvermarktung (Verkauf von Fernsehrechten etc.) tätigen Gesellschaften D, E, F und G. Zweck des Privatkontos: "Vermögensanlage", erwartete Vermögenswerte: CHF 15 Mio.

1. Der Kunde wickelt über alle Kundenbeziehungen C bis G kommerzielle Transaktionen ab (rund 5'000 in 10 Jahren). G verzeichnet nur Ein- und Ausgänge mit Stichwort "Consulting".
2. Für Transaktionen mit erhöhten Risiken liefert der Kunde auf Nachfrage jeweils 100 bis 200-seitige Vertragsdokumente.
3. Für die jährliche Überprüfung der Kundenbeziehungen kopiert der Kundenberater jeweils die Informationen aus dem KYC in das Formular und unterzeichnet dieses.
4. Nach zwei Jahren weist das Privatkonto einen Saldo von CHF 70 Mio. auf.
5. Nach fünf Jahren wird die Bank auf Presseberichte aufmerksam, welche den Kunden mit Korruptionsvorgängen in Verbindung bringen. Der Kunde bezeichnet dies als "Lügenkampagne von Konkurrenten".

Welche Fragen stellen Sie aus Sicht Compliance zu den einzelnen Punkten?

Lösung

1. Privatkonto: Zweck der Geschäftsbeziehung? "Consulting": Erhöhtes Risiko von Korruptionszahlungen
2. Knowhow (und Kapazität) von Front und Compliance, die Geschäftsbeziehungen zu überwachen?
3. Das Vorgehen zur Überprüfung der Kundenbeziehung / Aktualisierung des KYC-Files ist ungenügend
4. Hohe Abweichung zu erwarteten Vermögenswerten sollte erklärt werden
5. Überwachung von Negative News: Notwendig, u.U. Externe beiziehen

Erwartungen FINMA

- Bank muss Geschäft ihrer Kunden verstehen und das notwendige Front- / Compliance-Knowhow haben

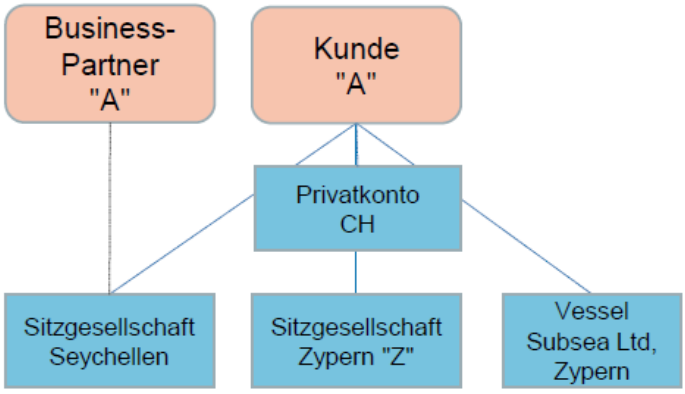
- KYC-Informationen sind nicht statisch, Bank muss Beziehungen mit erhöhten Risiken fortlaufend überwachen
- Verbindungen zwischen Transaktionen und KYC-Informationen herstellen
- Mittel der Abklärungen je nach Risiko

9. Umgang mit komplexen Strukturen

Sachverhalt

Bank X unterhält Geschäftsbeziehungen zu "A". "A" ist Norweger mit Domizil in Monaco. Er ist Unternehmer im Bereich "Shipping". Ihm gehört die operative Gesellschaft "Vessel Subsea Ltd." mit Sitz in Zypern. Das Gesamtvermögen von "A" beträgt ca. USD 100 Mio. jährliches Einkommen: USD 3 Mio.

- Die Bank X führt insgesamt 4 Kunden-beziehungen mit "A" und stuft alle 4 Kundenbeziehungen als "normales Risiko" ein.
- "A" ist bei weiteren drei Sitzgesellschaften als BO involviert. Diese Konten sind nicht bei der Bank X gebucht.
- Letzte Transaktion: Eingang von USD 15 Mio. auf Konto "Z". Begründung: "Brokerage Fee zwischen "Vessel Subsea Ltd." und der Sitzgesellschaft auf den Seychellen".



Welche Fragen sollte sich die Bank zur Geschäftsbeziehung A und seinem Setup stellen?

Lösung

- Big Picture über Geschäftsbeziehung A vorhanden?
  - Bank hat Beziehungsgeflecht und Gesamtübersicht über die Geschäftsbeziehung zu A vollständig abgeklärt und nachvollziehbar dokumentiert
  - Ergebnisse im Organigramm (inkl. involvierte Parteien und Geldflüsse) abgebildet

- Haben wir es mit einer komplexen Struktur zu tun?
  - Ja, da mehrere Sitzgesellschaften vorhanden, welche von fiduziarischen Aktionären geführt werden. Bank hat klare Hinweise, dass die bei der Bank X gebuchten zwei Sitzgesellschaften Teil eines grösseren Strukturkomplexes von "A" sind. Zahlungsstrom zwischen Sitzgesellschaften

- −Was ist das Risiko der Geschäftsbeziehung zu A?
  - Risikoeinstufung der Bank X ist zu hinterfragen
  - Komplexität der Struktur erfordert die Klassifizierung als Geschäftsbeziehungen mit erhöhtem Risiko (GmeR)

Erwartungen FINMA

- **Pauschalen Aussagen** wie "Asset Protection" oder "Steueroptimierung" zur Begründung des Einsatzes von Sitzgesellschaften sind zu **vermeiden**
- **Komplexen Strukturen** sind als Geschäftsbeziehung mit erhöhtem Risiko **(GmeR) zu klassifizieren** (andernfalls zwingend begründen, weshalb keine GmeR) **=> Vertiefte Abklärungen** erforderlich!
- Bank prüft **zweckmässige Risikoparameter** in Bezug auf **Verwendung von Sitzgesellschaften**

10. Abklärungspflichten (KYT)

Sachverhalt

1. Die mittlere Regionalbank Z hat den Unternehmer B aus Brasilien als Kunden. Eingang von USD 150 Mio., gemäss Kunde aus einem Vergleich mit der staatlichen Erdölgesellschaft.

2. Der Kunde möchte USD 100 Mio. gleich weiter an eine Genfer Privatbank transferieren.

3. Die Bank erhält ein 30-seitiges Dokument in portugiesischer Sprache, welches die Beilegung einer Streitigkeit im Bereich Charterverträge von Öltankern dokumentiert. Die Bank hält intern "Entschädigung für eine Verstaatlichung" als Rechtsgrund für die Zahlungen fest.

4. Zudem: Eingang von EUR 10 Mio., gemäss Kunde "Rückzahlung eines privaten Darlehens". Darlehensvertrag: Undatiert unterschrieben, Laufzeit von 28 Tagen, zinsfrei, ohne Angabe des Verwendungszwecks.

Welche Fragen stellen Sie aus Sicht Compliance zu den einzelnen Punkten?

Lösung

1. Sog. "**Vergleiche**" sind öfters **vorgeschoben**, um einen anderen Zahlungszweck zu verschleiern

2. Offensichtliche **Durchlauftransaktion**1, Risiko: Bank hat kein Gesamtbild (z.B. Zahlungsausgänge an Funktionäre der staatlichen Ölgesellschaft)

3. Bank hat offenbar Probleme, die eingereichten Belege inhaltlich und sprachlich zu verstehen. Frage: **Passt der Kunde überhaupt zur Bank?**

4. Bank sieht nur die Rückzahlung des angeblichen Darlehens - **keine Möglichkeit zur Kontrolle**, ob überhaupt eine Auszahlung stattfand. Zudem: Vertrag enthält mehrere verdächtige Elemente

Erwartungen FINMA

- Die Bank muss ihre Kunden verstehen und das **notwendige Front- / Compliance-Knowhow** haben

- **Transaktionsüberwachung**: Genügend kritisches Hinterfragen, Anfordern von Belegen, seriöse Abklärungen treffen und allenfalls Melderecht / -pflicht prüfen