FINANCIAL INTELLIGENCE UNIT
FÜRSTENTUM LIECHTENSTEIN

Fallsammlung 2022/1:
Risiken, Methoden, Typologien & Anhaltspunkte

Juli 2022

Einleitung

Die vorliegende dritte Ausgabe der Fallsammlung aus der Praxis der Stabsstelle FIU (SFIU) beinhaltet sowohl Geldwäscherei- als auch Terrorismusfinanzierungsfälle (Anti-Money-Laundering; AML und Terrorist Financing; TF).

Ziel dieser Ausgabe ist es, den Compliance-Verantwortlichen weitere Beispiele für Verdachtsmomente zur Verfügung zu stellen, indem auf Grundlage von Fällen aus der Praxis Musterfälle erstellt wurden. Diese wurden erforderlichenfalls ergänzt, geändert oder optimiert, um einen entsprechenden Praxisnutzen zu erzielen.

Zielpublikum

- Mitarbeitende der Compliance-Abteilungen
- Mitarbeitende an der unmittelbaren Kundenfront
- (für die Wahrnehmung der Sorgfaltspflichten verantwortliche) Mitglieder der Geschäftsleitungen

Publikation

Die Publikation erfolgt persönlich via goAML an die registrierten Sorgfaltspflichtigen sowie via Homepage der Stabstelle FIU für die interessierte Allgemeinheit.

Inhalt

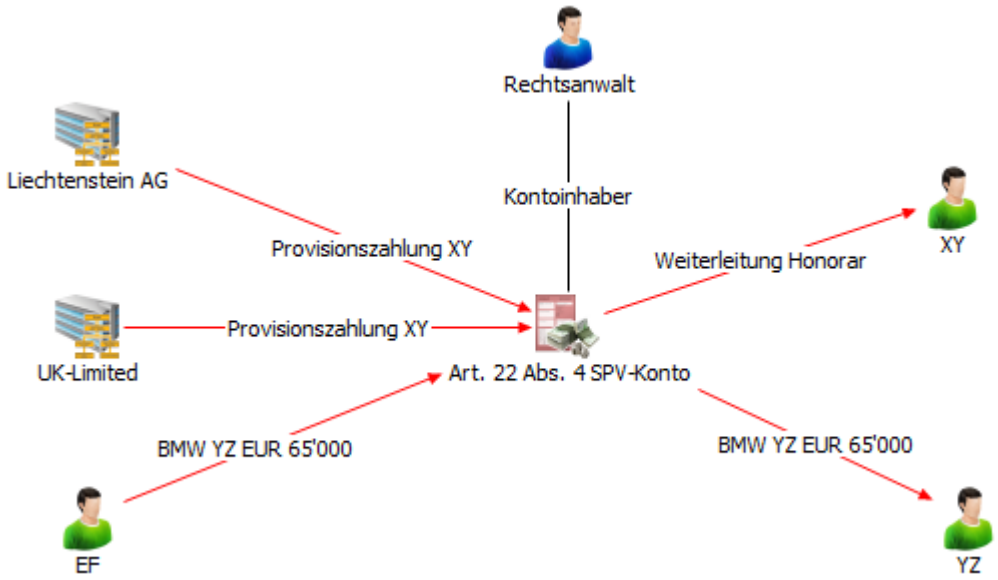
Transaktionen für Dritte – Rechtsanwaltskonten nach Art. 22b Abs. 4 SPV

Unter Rechtsanwaltskonten bzw. «forensische Konten» nach Art. 22b Abs. 4 SPV versteht man Bankkonten, welche Banken zu einem gewissen Grad von deren Sorgfaltspflichten befreien, vorausgesetzt, die Konten werden durch einen im Inland zugelassenen Rechtsanwalt für spezifische in der SPV abschliessend geregelte Vorgänge verwendet. Dies sind beispielsweise die Abwicklung und gegebenenfalls damit verbundene kurzfristige Anlage von Gerichtskostenvorschüssen oder Kautionen. Mittels vorliegender Sachverhaltsdarstellung soll dargelegt werden, wie eine missbräuchliche Verwendung solcher Bankkonten aussehen könnte.

Ein inländischer Rechtsanwalt empfing auf einem Rechtsanwaltskonto nach Art. 22b Abs. 4 SPV rund USD 800'000 von einer Liechtensteinischen AG und einer UK-Limited mit dem Buchungstext «Provisionszahlung XY». Diese Vermögenswerte wurden in kleineren Tranchen mit dem Buchungstext «Weiterleitung Honorar» an «XY» weitergeleitet.

Im Rahmen der Prüfung dieser nicht profilkonformen Transaktionen fiel der Bank auf, dass «XY» 2011 im Ausland wegen Geldwäscherei und gewerbsmässigem Betrug angeklagt wurde und 2021 wiederholt Privatinsolvenz angemeldet hatte.

Die daraufhin ausgedehnte Prüfung zeigte, dass auf das gleiche Konto im Jahr 2019 eine Zahlung über EUR 65'000 von «EF» mit dem Buchungstext «BMW YZ» einging. Diese Vermögenswerte wurden gleichentags an «YZ» weitergeleitet.



Auf einem anderen «Art. 22 Abs. 4-Konto» eines Rechtsanwalts gingen zwischen 2018 und 2020 ca. CHF 180’000 mit dem Buchungstext «legal Assistance» aufgeteilt auf 48 Transaktionen eines Absenders ein. Oft gingen diese separaten Transaktionen in engem zeitlichem Kontext, teilweise sogar gleichentags auf diesem Konto ein. Danach wurden die Vermögenswerte auf das Kanzlei-Konto des Rechtsanwalts übertragen. Bei der Absenderin der Vermögenswerte handelte es sich um eine Person, welche in öffentlichen Quellen im Zusammenhang mit Drogenhandel und kriminellen Organisationen in Osteuropa genannt wurde.

Diese Beispiele zeigen, dass obgleich im Falle von Rechtsanwaltskonten vereinfachte Sorgfaltspflichten ex lege angewendet werden dürfen, sichergestellt werden muss, dass solche Konti auch tatsächlich nur für die Zwecke verwendet werden, für welche die SPV

Ausnahmen vorsieht. Die Erkennung einer missbräuchlichen Verwendung von Rechtsanwaltskonten erfordert folglich eine entsprechende Überwachung der Transaktionen sowie des Verwendungszwecks.

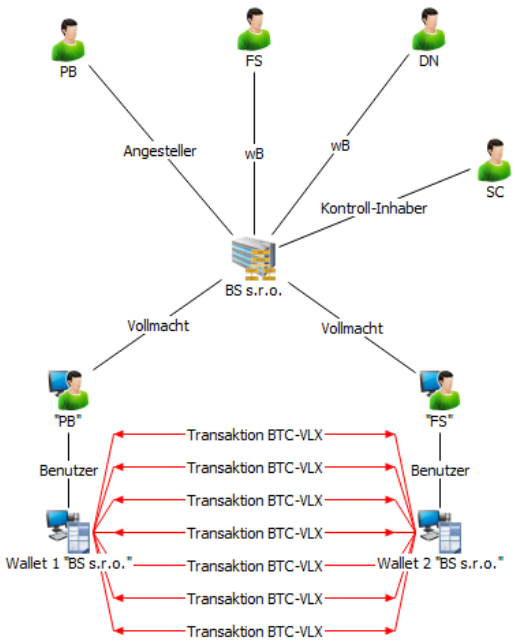
Die vorstehenden Beispiele veranschaulichen die Bedeutung der Transaktionsüberwachung im Rahmen der vereinfachten Sorgfaltspflichten. Auch wenn vereinfachte Sorgfaltspflichten ausschliesslich bei Geschäftsbeziehungen bzw. Transaktionen mit einem grundsätzlich geringen Risiko angewendet werden dürfen, kann nicht ausgeschlossen werden, dass auch diese missbräuchlich verwendet werden. Aus diesem Grund stellt die Anwendung vereinfachter Sorgfaltspflichten keine Ausnahme von den Sorgfaltspflichten, sondern lediglich eine risikoangemessene Erleichterung bei deren Anwendung dar[1].
Folglich ist die angemessene Überwachung von Transaktionen (insb. Verifizierung des Transaktionszwecks etc.) unerlässlich, um eine allfällig missbräuchliche Verwendung erkennen zu können.

Marktmanipulation durch sog. «wash-trading» im Krypto Bereich

«FS» und «PB» eröffneten 2020 jeweils ein Konto bei einem Krypto-Exchange-Service Provider in Liechtenstein. Beide verwendeten bei der Eröffnung eine Emailadresse, welche einen sehr ähnlichen Firmennamen beinhaltete («BS»). FS beantragte nach der Eröffnung die Umwandlung des Kontos in ein Firmenkonto für «BS s.r.o.,», Schweiz. Bei der «BS s.r.o.», Schweiz, handelt es sich um eine Zweigniederlassung eines Tschechischen Unternehmens und wurde als Serviceanbieter für Krypto Asset Manager im Gross- und Einzelhandel beschrieben. Als wirtschaftlich Berechtigte von «BS s.r.o.» wurden «FS» und «DN» und als kontrollierende Person wurde zusätzlich «SC» festgestellt.

Zwischen Mai und Juni 2022 wurden 1'160'040 Trades zwischen den beiden Konten/Wallets von «BS s.r.o.» ausgeführt, was ca. 96% des gesamten Handelsvolumens in diesem Markt ausmachte.

Dieses Handelsverhalten wird «wash trading» genannt und dient unter anderem der künstlichen Steigerung des Handelsvolumens, wodurch der Eindruck entsteht, dass es sich um ein begehrtes Finanzinstrument handelt.



Wirtschaftlich betrachtet macht dieses Handelsverhalten keinen Sinn, da jede Transaktion mit Gebühren verbunden ist. Die handelnden Parteien nehmen die Gebühren in Kauf, um den Anschein eines begehrten Finanzinstruments zu erwecken, mit dem Zweck eine Kurssteigerung zu erwirken oder Dritten den Eindruck eines wertvollen Tokens zu vermitteln.

In der Krypto-Welt kommt «wash-trading» häufig im Zusammenhang mit sog. NFTs (non-fungible Token) beim Verkauf von bspw. «Kunstwerken» vor. So berichten

[1] vgl. Kapitel 5.1 der FMA-Richtlinie 2013/1 zum risikobasierten Ansatz im Sinne des SPG: Link

kommerzielle Dienstleister aus dem Krypto-Analysebereich, dass die Nutzung dieser «wash trades» ein bekanntes Vorgehen zur Manipulation der Bewertung darstellt.

Verwirklichte Anhaltspunkte (gem. Anhang 3, III, E SPV):

4. Durchführung mehrerer Transaktionen innerhalb eines kurzen Zeitraums.
8. Durchführung von mehreren Hin-und-her-Transaktionen unter Einbezug derselben VT-Identifikatoren.

Beim «wash-trading» handelt es sich somit um Abläufe, bei denen dieselben Personen sowohl als Verkäufer als auch al Käufer agieren, um Wert und Liquidität eines Vermögenswerts künstlich zu erhöhen. Er verkauft sich demnach bspw. NFT selbst, indem er zwei Wallets benutzt. Für Außenstehende scheint es, als würde jemand tatsächlich Betrag X für einen NFT bezahlen, und somit bekommt dieser NFT plötzlich ein Preisschild. Erkannt werden kann dieses Verhalten unter Umständen daran, dass die meisten Vorkommnisse bei Coins mit geringer Marktkapitalisierung stattfinden und insbesondere Coins mit geringer Liquidität sich hierfür eignen. Ein besonderes Augenmerk kann auch eine plötzliche intensive Präsenz des Coins in sozialen Medien sein.

Abweichungen vom Geschäftsprofil, nicht hinterfragte Annahme von hohen Vermögenswerten

Mitte 2021 eröffnete eine Bank eine Geschäftsbeziehung mit «Kunde A». Im ursprünglichen Geschäftsprofil wurde festgehalten, dass sich das Gesamtvermögen des Kunden auf mehrere Millionen USD belaufe. Insgesamt sollten davon etwa USD 5 Mio. für Investmentzwecke auf das Konto bei der Bank eingehen und wurde ein Transaktionsvolumen von rund USD 10 Mio. pro Jahr im Profil erfasst. Der Kunde gab an ein «selfmade» Millionär zu sein, der durch den Verkauf seiner Gesellschaft in Amerika per Ende 2009 rund USD 1.9 Mio. eingenommen habe. Den erzielten Verkaufserlös habe er Mitte 2010 bis Ende 2012 in Wertpapiere (B-Aktien) und diverse Immobilien investiert und auf Grund seines «guten Händchens» habe er von enormen Kurssteigerungen profitiert.

Die Geschäftsbeziehung wurde als solche mit regulären Sorgfaltspflichten eingestuft. Ein Adverse Media Check sowie eine Prüfung kommerzieller Datenbanken ergab keine relevanten Ergebnisse.

Nach Ansicht des zuständigen Kundenberaters der Bank sei die vom Kunden beschriebene Performance vor dem Hintergrund der zeitlichen Abfolge nicht unrealistisch, um das entsprechende Wertpapiervermögen angehäuft zu haben.

Zwecks Prüfung der Hintergrundinformationen betreffend die Immobilien sowie es ursprünglichen Verkaufs der Gesellschaft wurden Kaufverträge eingefordert. Ebenso erfolgte eine Abklärung zum Käufer des Unternehmens, welche jedoch ergebnislos verlief.

Mit der ersten Transaktion (einer Wertschrifteneinlieferung) wurden über USD 12.5 Mio. übertragen, womit die Angaben im Geschäftsprofil zum erwarteten Transaktionsvolumen) bereits in einem Vorgang überschritten wurden. Zudem wurden weitere Wertschriftenlieferungen in Höhe von mehr als USD 50 Mio. auf das Konto transferiert und damit die Angaben hinsichtlich der zu erwartenden Vermögenseingänge gemäss Geschäftsprofil deutlich überschritten. Die Wertschrifteneinlieferungen erfolgten jeweils über eine Gesellschaft mit Sitz in den Cayman Islands.

Im Zeitraum von 10 Monaten erfolgten Transaktionen mit einem Gesamtvolumen von mehr als USD 400 Mio., was dem 40-fachen Volumen des im Geschäftsprofil angegebenen Transaktionsvolumens entspricht.

Festzuhalten ist, dass einfache Abklärungen im Laufe der Geschäftsbeziehung und ab

November 2021 besonders unter dem Druck der Compliance erfolgten. Diese Abklärungen waren jedoch unvollständig und mangelhaft. So wurde im Hinblick auf die Wertpapiertransaktionen lediglich festgestellt, dass diese von einer Cayman Island-Gesellschaft übertragen wurden und der Vertragspartner diesbezüglich Depotinhaber war. Zum konkreten wirtschaftlichen Hintergrund dieser eingebrachten Vermögenswerte beinhalteten die einfachen Abklärungen jedoch keine Angaben sowie keine weitergehende Dokumentation.

Die Risikoeinstufung zum Zeitpunkt der Eröffnung der Geschäftsbeziehung wurde mit «regulär» vorgenommen. In der Folge wurde diese Einstufung wiederholt korrigiert bis schlussendlich eine Einstufung als «hohes Risiko» erfolgte - u.a. aufgrund des exorbitant hohen Transaktionsvolumens.

Mangels befriedigender Antworten bzw. Übermittlung entsprechender Informationen und Belege des Kunden wurde Anfang 2022 seitens der Compliance ein Antrag auf Saldierung der Geschäftsbeziehung gestellt.

Von der Bank wurde es verabsäumt, durch entsprechende Abklärungen und Nachforschungen den vermeintlichen wirtschaftlichen Hintergrund der Geschäftsbeziehung zu plausibilisieren. Mangelhaft abgeklärt wurde insbesondere, ob die Zahlung des Kaufpreises von USD 1.9 Mio. tatsächlich geleistet wurde, der Kaufpreis insgesamt objektiv plausibel gewesen wäre, die Gesellschaft im Handelsregister eingetragen war und, ob die Generierung des Vermögens von über USD 50 Mio. mittels Belegen nachweisbar ist. Weiters wäre zu plausibilisieren gewesen, ob die Vermehrung des Wertpapiervermögens auf mehr als USD 50 Mio. innerhalb von 11 Jahren in diesem Ausmass tatsächlich hätte erfolgen können.

Im Rahmen der Analyse stellte sich heraus, dass «Kunde A» im Ausland bereits wegen Steuerhinterziehung und Zuwiderhandlungen gegen das Wertpapiergesetz («pump and dump») bekannt und infolgedessen Gegenstand von Strafverfahren war und verurteilt wurde.

Verwirklichte Anhaltspunkte (gem. Anhang 3 II SPV):

10. Kunde erteilt vorsätzlich falsche oder irreführende Auskünfte oder verweigert die für die Geschäftsbeziehung notwendigen und für die betreffende Tätigkeit üblichen Auskünfte und Unterlagen.
25. Hinweise auf gerichtlich strafbare Handlungen des Kunden im In- oder Ausland.

Verwirklichte Anhaltspunkte (gem. Anhang 3 V SPV):

1. Nicht nachvollziehbare, substantielle und nicht dem Geschäftsprofil entsprechende Transaktionen im Zusammenhang mit der Geschäftstätigkeit des Kunden.

Die Schwierigkeit bei diesem Sachverhalt liegt darin, überhaupt zu erkennen, dass «vorsätzlich falsche oder irreführende Auskünfte» erteilt werden.

Dieses Beispiel zeigt einmal mehr, wie wichtig bei der gesamtheitlichen Betrachtung und Beurteilung von Sachverhalten die Erfahrung von Compliance-Mitarbeitern ist. Das Basieren auf rein formalistischen Abklärungen («Check the box») kann bewusst von Kriminellen ausgenutzt werden, wenn diese genügend mit den gängigen Sorgfaltspflichten vertraut sind, was regelmässig der Fall ist.

Terrorismusfinanzierung über Krypto Service-Dienstleister

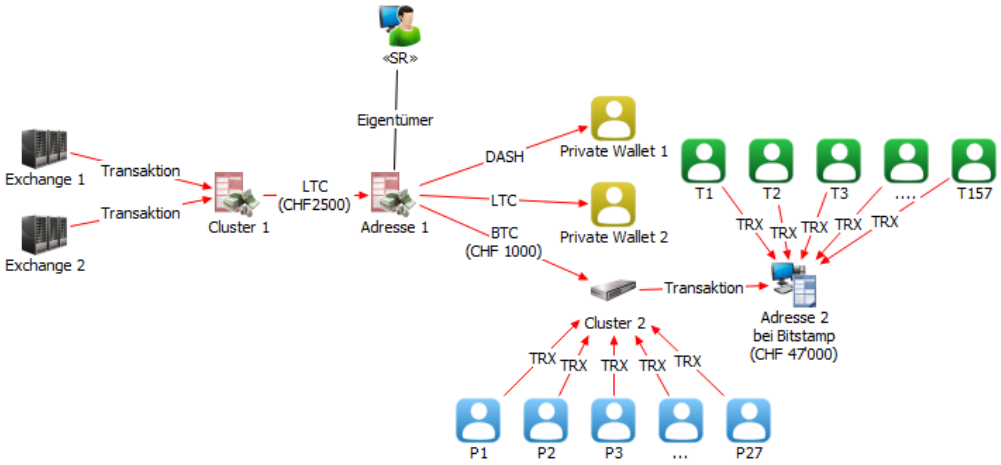
Anfang Mai 2022 erhielt ein Krypto Service-Dienstleister eine Vorladung des Select Committee des US-Amerikanischen Repräsentantenhauses welches den Angriff auf das Capitol vom 6. Januar 2021 untersucht.

Die Vorladung beinhaltete eine Anfrage zu einer Transaktion in Bitcoin (ca. CHF 1'000) vom Februar 2021, welche an die Adresse «Adresse 1»gesendet wurde. Diese Transaktion wurde von «SR» in Auftrag gegeben. «SR» war langjähriger Kunde des Krypto Service-Dienstleisters. In den Jahren zuvor fanden auf dessen Wallet ausser der Ersteinlage keine Transaktionen statt. Im Januar 2021 erhielt «SR» CHF 2'500 in LTC. Diese Transaktion kam von einem Cluster mit der „Root Adresse" «Cluster 1». Die Vermögenswerte schienen von zwei anderen Exchanges zu kommen und wurden vor dem Übertrag auf die Wallet von «SR» auf der „Root Adresse" «Cluster 1» konsolidiert.

Zwischen Januar und März 2021 initiierte «SR» 5 Zahlungen in DASH, BTC und LTC. Die BTC-Zahlung ist jene, die in der Vorladung des Select Committee des US-Amerikanischen Repräsentantenhauses untersucht wurde. Diese Zahlung scheint an einen Cluster mit der „Root Adresse" «Cluster 2»transferiert worden zu sein. Dieser Cluster hatte im gleichen Zeitraum auch noch 27 andere Zahlungen in unterschiedlicher Höhe erhalten. Von dort wurden die Vermögenswerte in einer Zahlung an die Adresse «Adresse 2» gesendet.

Diese Adresse «Adresse 2»hat zwischen Ende 2020 und Anfang 2021 157 Zahlungen in der Gesamthöhe von BTC 1 bekommen, was darauf hindeutet, dass diese Adresse für Fundraising verwendet wurde

Verschiedene Strafverfolgungsbehörden wurden entsprechend notifiziert und diese ermitteln in Zusammenarbeit mit dem Select Committee des US-Amerikanischen Repräsentantenhauses.



Der vorstehende Fall zeigt, wie einfach und effektiv terroristische Einheiten in der Praxis agieren können. Der Sachverhalt dient daher der Veranschaulichung, auf welche Weise sich terroristische Gruppen organisieren und finanzieren können. Folglich liegt die Möglichkeit des Erkennens solcher Aktivitäten insbesondere auf Hinweisen zu sog. Fundraising-Tätigkeiten, in denen es auf einem Konto/Wallet entgegen der plausibilisierten Profilangaben zu diversen Vermögenseingängen von verschiedenen Adressaten kommt. Im Bereich der Erkennung der Terrorismusfinanzierung kommt erschwerend hinzu, dass grundsätzlich kein betragsmässiger Schwellenwert gesetzt werden kann, da vor allem auch Kleinbeträge zu diesen Zwecken genutzt werden.
Hinweise auf Fundraising-Aktivitäten ohne entsprechend plausibilisierte Grundlagen im Geschäftsprofil sind insbesondere auch im Bereich tiefer Transaktionshöhen mit grösster Sorgfalt abzuklären. Gerade im Bereich der Finanzierung von extremistischen Aktivitäten sind oftmals kleine Vermögenswerte bei der Zielerreichung von entscheidender Relevanz.

Identitätsdiebstahl im Krypto-Bereich

Ein Fall, der die SFIU bereits seit 2020 beschäftigt, ist der eines Identitätsbetrügers, der mittlerweile bei einem Krypto Service-Dienstleister über 80 Wallets mit unterschiedlichen Identitäten eröffnen konnte.

Dabei verwendete er – in den, der SFIU bekannten Fällen – nur ca. 6 verschiedene Adressen, in jeweils leicht abgeänderter Form.

Zudem hat die Person bei jeder Eröffnung Selfies der gleichen Person (möglicherweise von sich selbst) verwendet. Dabei ist auffällig, dass ca. 90% der Selfies alle den selben, bzw. sehr ähnlichen Hintergrund haben (bspw. Tapete) und die Person überwiegend mit nacktem Oberkörper abgelichtet wurde. Die unbekannte Täterschaft hat offensichtlich aufgrund der gemachten Erfahrungen keine Notwendigkeit gesehen, einen grösseren Aufwand zu betreiben.

Auch die verwendeten Pässe zeigten immer die gleiche Person. Bei den dem Krypto Service-Dienstleister und in der Folge der SFIU übermittelten Pässen handelte es sich allesamt um Fälschungen von sehr guter Qualität.

Der Täter arbeitete jeweils mit gestohlenen Identitäten und Kreditkartendaten. So wurden in jedem Fall Einzahlungen über Kreditkarten auf das eröffnete Wallet gemacht, in Bitcoin gewechselt und umgehend an eine externe, private Adresse transferiert. Die einzelnen Beträge lagen zwischen weniger als hundert Euro bis zu mehreren tausend Euro.

Mittlerweile sind Strafvollzugsbehörden in mehreren Ländern mit diesem Fall befasst.

Aus Sich der SFIU ist es folglich unerlässlich, dass sowohl verwendete Adressen, also auch Selfies mit grösserer Sorgfalt abgeglichen werden, um solche Fälle effizient erkennen und verhindern zu können.

Zu denken ist insbesondere an die Verwendung von Gesichtserkennungssoftware oder adäquaten Identifikationsverfahren im Rahmen des Kundenannahmeprozesses. Vergleiche hierzu die Wegleitung 2019/7 der Finanzmarktaufsicht zu den im Sinne von Art. 14 Abs. 1 SPV anwendbaren Sicherungsmassnahmen bei Geschäftsbeziehungen und Transaktionen ohne persönliche Kontakte (Wegleitung zu den Sicherungsmassnahmen nach Art. 14 SPV)[2].

[2] https://www.fma-li.li/files/list/fma-wl-2019-7-sicherungsmassnahmen.pdf

Veruntreuung durch einen Mitarbeiter

Aus einer Verdachtsmitteilung ergab sich, dass bei einem Treuhandunternehmen festgestellt wurde, dass ein zeichnungsberechtigter Mitarbeiter («XY») vom firmeneigenen Konto bei einer inländischen Bank einen fünfstelligen CHF-Betrag auf sein privates Konto bei einer ausländischen Bank überwiesen hat. Ein schlüssiger Rechtsgrund für diese Überweisung konnte bis zum Mitteilungszeitpunkt nicht festgestellt werden. Insbesondere konnten salär-, spesen- oder andere vergütungsbezogene Gründe ausgeschlossen werden. Eine Durchsicht der unmittelbar verfügbaren Bankbelege des Kontos bei der betroffenen Bank ergab, dass zwischen 2020 und 2021 neun Transaktionen vom firmeneigenen Konto auf das Konto von «XY» bei der ausländischen Bank mit Beträgen von ca. CHF 10'000 bis CHF 50'000 stattgefunden hatten. Insgesamt handelte es sich um Überweisungen mit einem Gesamtbetrag von über CHF 260'000.

In der weiteren Analyse der Zahlungen stellte sich heraus, dass die Transaktionen, die «XY» auf sein Konto bei einer ausländischen Bank getätigt hatte, in «Sammelzahlungen» des Treuhandunternehmens eingliedert und daher objektive betrachtet nicht leicht erkennbar waren.

Ferner wurde durch vertiefte Abklärungen offensichtlich, dass «XY» bereits im Jahre 2002 begonnen hatte, sukzessive Zahlungen auf ausländische Konten im Ausland, welche in seinem Namen bzw. dem Namen seiner/s Ehepartners und seiner Nachkommen geführt wurden, zu veranlassen. Ebenso erfolgten diverse Bareinzahlungen auf ausländische Konten, welche der Höhe nach nicht im Einklang mit seinem Verdienst standen. In Summe wurde so mehr als eine halbe Million CHF über einen Zeitraum von 20 Jahren vom Konto des Treuhandunternehmen abgezogen.

Bild: iStockphoto

Dieser Fall zeigt, wie geschickt und dreist Täter vorgehen und bewusst Vertrauensverhältnisse über Jahre ausnützen. Dieser Sachverhalt soll zudem veranschaulichen, dass es sich nicht zwingend um externe Täter handeln muss, sondern diese ebenfalls aus dem unmittelbaren Umfeld stammen können.

Solide Kontrollmechanismen wie zum Beispiel das Vier-Augen-Prinzip zerstören nicht Vertrauen, sondern sie fördern dieses vielmehr.

Aus der Glücksspiel-Praxis

Ein Glücksspielanbieter berichtete in einer Verdachtsmitteilung was folgt:

Bei Herrn «A» handelte es sich um einen Stammgast. Aufgrund der regelmässigen Besuche und der hohen Spieleinsätze gehörte dieser Gast zu den sog. «High Rollern».

Bereits im Jahr 2020 hatte «A» die interne Umsatz-Schwellenwertgrenze überschritten und wurde infolgedessen bezüglich der Herkunft der Vermögenswerte bzw. der als Spieleinsatz verwendeten Gelder befragt. Zusätzlich wurde seine Risikokategorisierung erhöht. Die von «A» gemachten Angaben wurden mittels Recherche überprüft und plausibilisiert. «A» wurde auf mindestens halbjährlicher Basis neuerlich überprüft und die Transaktionsumsätze überwacht und mittels der getätigten Angaben plausibilisiert.

«A» spielte ausschliesslich an Automaten.

Aus Sicht des Spielers werden – unabhängig von dessen Einsatz – alle ihm ausbezahlten Werte kumuliert als «total out» bezeichnet. Aus Optik des Glücksspielanbieters wesentlich ist der Bruttospielertrag. Dieser entspricht dem Betrag, um den sämtliche getätigten Spieleinsätze der Besucher deren Gewinne übersteigen. Die Auszahlungsquote wiederum entspricht dem durchschnittlichen Anteil der Gewinnauszahlungen an den Einsätzen. Wenn bspw. eine 96%-ige Auszahlquote als Berechnungsgrundlage verwendet wird, kann so der Bruttospielertrag ermittelt werden. Zusammengefasst: in diesem Beispiel verbleiben im rechnerischen Durchschnitt 4% aller von den Spielern ins Casino gebrachten Gelder beim Casino.

Im Dezember 2021 wurde «A» erneut bezüglich seiner Transaktionen überprüft. Gemäss seinen Angaben verwendete er ausschliesslich sein Gehalt zum Spielen. Demzufolge wurde dieses als Grundlage herangezogen, um die Höhe der Einsätze zu plausibilisieren. Es wurden sohin die eingebrachten Werte mit dem Gehalt gegengerechnet, um zu eruieren, wieviel Prozent des Gehaltes im gesamten Zeitraum für das Spiel aufgewendet wurde.
Demnach hat «A» 44% seines Gehaltes für das Spiel in diesem Casino verwendet. Da 44% des Gehaltes einen auffällig hohen Prozentsatz darstellt, wurden von ihm weitergehende Finanzunterlagen eingefordert. Da der Kunde nach der ersten Aufforderung keinerlei Unterlagen eingebracht hatte, wurde ihm Anfang 2022 erneut ein Ansuchen zur Beibringung der Unterlagen ausgehändigt. Seit diesem Zeitpunkt hat er den Glückspielanbieter nicht mehr besucht.

Insbesondere im Glücksspielbereich ist das Verhältnis von eingesetztem Geld zur wirtschaftlichen Leistungsfähigkeit des Kunden unter Berücksichtigung dessen Gesamtsituation von entscheidender Bedeutung, um die Plausibilität des an den Tag gelegten Verhaltens beurteilen zu können.

In Anbetracht sowohl der Geldwäschereirisiken sowie eines nicht zu vernachlässigenden Suchtpotenzials und der damit verbundenen gravierenden gesellschaftlichen Folgen, ist die Überwachung sowie das konsequente Hinterfragen gemachter Angaben essentiell, um kriminelles Verhalten erkennen zu können.