STABSSTELLE FINANCIAL INTELLIGENCE UNIT (FIU)
DES FÜRSTENTUMS LIECHTENSTEIN

FALLSAMMLUNG 2024/1

RISIKEN, METHODEN, TYPOLOGIEN & ANHALTSPUNKTE

April 2024

Herausgeber:
Stabsstelle Financial Intelligence Unit (SFIU)
des Fürstentums Liechtenstein
Äulestrasse 51
FL-9490 Vaduz
Telefon +423 236 61 25
E-Mail info.sfiu@llv.li
Website www.fiu.li

I. Einleitung

Die vorliegende sechste Ausgabe der Fallsammlung aus der Praxis der Stabsstelle FIU (SFIU) fokussiert sich auf Risiken, Methoden, Typologien und Anhaltspunkte aus dem Bereich der Geldwäschereibekämpfung sowie der Bekämpfung von Terrorismusfinanzierung.

Den Compliance-Verantwortlichen sollen weitere aktuelle und praxisrelevante Beispiele für Verdachtsmomente im Zusammenhang mit Geldwäscherei und Terrorismusfinanzierung mit dem Ziel, noch besser betreffend die vorgestellten Thematiken sensibilisiert zu werden, zur Verfügung gestellt werden. Hierfür wurden wie gewohnt auf Grundlage von Fällen aus der Praxis, Musterfälle erstellt, die teilweise ergänzt, geändert und/oder optimiert wurden, um einen grösstmöglichen 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 SFIU für die interessierte Allgemeinheit.

Inhaltsverzeichnis

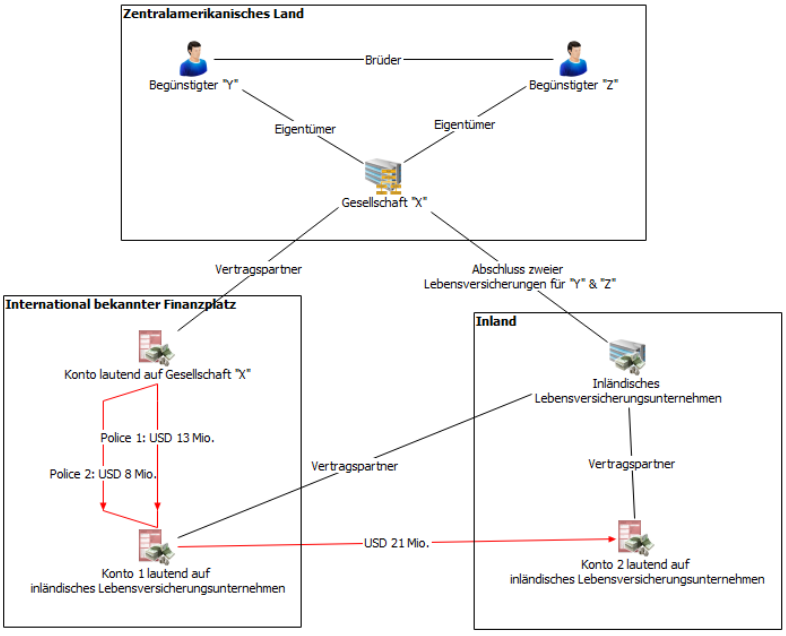
II. Fälle

1. Lebensversicherungspolicen

Ein inländisches Lebensversicherungsunternehmen schloss **zwei Lebensversicherungspolicen** mit derselben zentralamerikanischen Gesellschaft «X», welche Bestandteil einer komplexen Gesellschaftsstruktur war, ab. Vermittelt wurde die Geschäftsbeziehung über einen Versicherungsvermittler aus einem Drittstaat.

Bei den beiden versicherten Personen und Erlebensbegünstigten – «Y» und «Z» – handelte es sich um zwei Brüder, die beide Teileigentümer der Gesellschaft «X» waren. Sie stammten aus demselben zentralamerikanischen Land, welches zum Zeitpunkt der Aufnahme der Geschäftsbeziehung von der sog. **FATF Risikoländerliste**[1] erfasst und zudem gemäss **internationalem Korruptionsindex**[2] unter den Hochrisikoländern geführt war.

In «Police 1» wurden **USD 13 Mio.** und in «Police 2» **USD 8 Mio.** mittels Einmalprämie eingebracht. Der Transfer dieser Gelder erfolgte jedoch nicht unmittelbar von einem Konto der «X» aus dem zentralamerikanischen Staat, sondern ausgehend von einem weiteren Konto der Gesellschaft in einem Drittstaat, der für seine Funktion als internationaler Finanzplatz global bekannt ist. Die Gelder wurden dabei zunächst auf das Konto des Lebensversicherungsunternehmens in demselben bekannten Finanzplatz transferiert. Erst in einem zweiten Schritt erfolgte ein Weiterüberweisung dieser Gelder vom Konto der Lebensversicherung auf deren inländisches Konto, wobei als Zahlungsreferenz lediglich die Nummer der Police ohne weitere Angaben vermerkt wurde.



[1] https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-2023.html

[2] https://www.transparency.org/en/cpi/2022

Im Rahmen der Aufnahme der Geschäftsbeziehung wurden die erforderlichen Identifikationsdokumente eingeholt sowie ein Geschäftsprofil angelegt, welches jedoch nicht mit inhaltlich relevanten Informationen angereichert oder verifiziert wurde. Zudem wurden zum Zeitpunkt der Policen-Eröffnung **keine Hintergrundüberprüfungen** mittels *Open Source Intelligence* (OSINT) – weder zur Vertragspartnerin «X» noch zu den beiden versicherten Personen «Y» und «Z» – vorgenommen. Die Geschäftsbeziehung wurde als «**normales Risiko**» klassifiziert.

Gemäss Angaben im Geschäftsprofil sollten die eingebrachten Vermögenswerte aus der Geschäftstätigkeit der «X» in der **Baubranche** im zentralamerikanischen Risikoland sowie aus einem **Teilverkauf aus der komplexen Gesellschaftsstruktur** stammen.

Im Rahmen eines sog. «**File Reviews**» wurden schrittweise sämtliche Policen aufgearbeitet und überprüft. Diese Aufarbeitung umfasste u.a. entsprechende OSINT-Abfragen und Verifizierungshandlungen mit Fokus auf dem Hintergrund und der Herkunft der Vermögenswerte.

Bei den gegenständlichen Policen trat dabei zutage, dass sowohl die Vertragspartnerin «X» als auch die beiden versicherten Personen bereits seit 2017 Gegenstand von Strafverfahren im zentralamerikanischen sowie einem weiteren Staat waren und u.a. wegen **Korruption** und **Betrug** angeklagt wurden. «Y» und «Z» standen zudem in unmittelbarer und öffentlich bekannter Verbindung zu ehemals hochrangigen Politikern dieses Landes. Des Weiteren wurde zwischenzeitlich bereits ein **internationaler Haftbefehl** gegen «Y» und «Z» erlassen, was ebenfalls über öffentliche Quellen nachvollzogen werden konnte. Diese Feststellungen führten mit **deutlicher Verspätung** zu einer Verdachtsmitteilungserstattung.

Dieser Sachverhalt zeigt einmal mehr die Schwächen bei der Sorgfaltspflichterfüllung durch Sorgfaltspflichtige – sowohl bereits bei der Aufnahme der Geschäftsbeziehung selbst als auch im Rahmen der laufenden Überwachung – auf. Zudem wird veranschaulicht, wie essentiell zeitnahe und umfassende Verdachtsmitteilungen für die Arbeit der SFIU sind. Darüber hinaus werden Risiken im Lebensversicherungsbereich beleuchtet, da insbesondere Lebensversicherungspolicen mit **hohen Einmalprämien** ein entsprechendes Risiko bergen – insbesondere, wenn die Hintergründe nicht mit der erforderlichen Sorgfalt aufgearbeitet werden.

Seitens der Sorgfaltspflichtigen wurden **diverse Risikoindikatoren** wie bspw. die Involvierung von Risikoländern (FATF/Korruptionsindex) und von (Ex-)PEPs sowie Durchlauftransaktionen, Bestandteile einer komplexen Struktur und hohe Einmalprämien nicht angemessen berücksichtigt und adressiert. Des Weiteren wurden auch die Umstände, weshalb eine zentralamerikanische Gesellschaft eine Police mit einer inländischen Versicherung abschliesst, dabei jedoch der Transfer der Vermögenswerte über ein Drittstaatenkonto der Vertragspartnerin sowie ein weiteres ausländisches Konto der Versicherung selbst veranlasst wird, nicht kritisch hinterfragt und abgeklärt. Dieser Transfer der Einmalprämien ausgehend vom Konto des Versicherungsunternehmen auf ihr inländisches Konto, verbunden mit einer reinen Zweckangabe der Nummer der Police, verunmöglichte eine Überwachung und Überprüfung durch die kontoführende inländische Bank.

Stichworte:

- Produkt Lebensversicherung
- Hohe Einmalprämien
- Herkunft der eingebrachten Vermögenswerte
- Durchlauftransaktionen u.a. über Konten der Versicherung selbst
- Involvierung FATF-Risikoland
- Involvierung Risikoland gemäss internationalem Korruptionsindex
- Treffer in kommerziellen Datenbanken und öffentlichen Quellen
- Offensichtlich erhöhtes Diskretionsbedürfnis der Kunden
- Verbindung zu PEP oder Ex-PEP

2. Verdachtsmitteilungsschwelle

Treuhandgesellschaft «X» eröffnete 2011 eine Geschäftsbeziehung für einen EU-Bürger «Z» und errichtete sodann eine **diskretionär ausgestaltete liechtensteinische Stiftung** «S» mit dem ausschliesslichen Zweck der Leistung von Zuwendungen an den Begünstigten «Z» gemäss Beistatut. Parallel dazu wurde bei einer inländischen Bank ein Konto für die Stiftung «S» eröffnet.

Die Stiftung «S» wurde von einer weiteren Gesellschaft des «Z», der «T AG», zu 100% gehalten. Gemäss Geschäftsprofil handelte es sich bei der «T AG» um eine operativ tätige Gesellschaft aus einem **osteuropäischen Land**, welche im Bereich von Immobiliengeschäften sowie der Logistik tätig sei und Zielmärkte in Osteuropa bediene.

Die Herkunft der Vermögenswerte wurde im Rahmen der Aufnahme der Geschäftsbeziehung mit der Stiftung «S» mit Gewinnen der «T AG» angegeben und **nicht weitergehend verifiziert**. Hintergründe zum Kunden «Z» selbst wurden **nicht vertieft abgeklärt**.

2023 fielen im Rahmen eines Profilupdates diverse negative Presseberichte im Zusammenhang mit dem Kunden «Z» auf. Gemäss *Open Source Intelligence* (OSINT) wurde «Z» bereits seit 2015 **gewerbsmässiger Betrug** vorgeworfen. Zudem sei «Z» im europäischen Ausland zu einer **langjährigen Haftstrafe verurteilt** worden, das Urteil sei jedoch noch nicht in Rechtskraft erwachsen.

Einer der beiden inländischen Sorgfaltspflichtigen erstattete daraufhin umgehend Verdachtsmitteilung an die SFIU. Zwar konnte im Rahmen der durch die OSINT-Treffer veranlassten besonderen Abklärungen keine Auffälligkeiten im Transaktionsverhalten festgestellt werden, jedoch konnte ein unmittelbarer Zusammenhang mit den bekannten Vorwürfen auch **nicht ausgeschlossen** werden.

Der zweite Sorgfaltspflichtige reagierte erst auf ein Auskunftsersuchen der SFIU. Er veranlasste entsprechende Abklärungen und erstattete eine Verdachtsmitteilung. Jedoch wurde die Verdachtsmitteilung unter Darlegung erstattet, weshalb aus Sicht des

Sorgfaltspflichtigen eben gerade **kein Verdacht vorliege**. Eine unmittelbare Verbindung sowohl der Stiftung «S» als auch des Kunden zum Sachverhalt hätte aus Sicht des Sorgfaltspflichtigen trotz der diversen Berichte in den öffentlichen Quellen nicht festgestellt werden können. Insbesondere sei das im Ausland ergangene Urteil noch nicht in Rechtskraft erwachsen, weshalb die Unschuldsvermutung gelte.

Aufgrund der ersten Verdachtsmitteilung konnte der erforderliche Analyseprozess der SFIU eingeleitet und nach weitergehenden Abklärungen ein Analysebericht erstellt und **Massnahmen gegenüber den Sorgfaltspflichtigen** initiiert werden.

Aus Sicht der SFIU wurden von beiden Sorgfaltspflichtigen **die Überwachungspflichten gemäss SPG nicht ordnungsgemäss** erfüllt, da die bereits seit einigen Jahren öffentlich bekannten Vorwürfe nicht festgestellt wurden.

Darüber hinaus konnte bei einem der beiden Sorgfaltspflichtigen ein **mangelndes Verständnis von der Verdachtsmitteilungspflicht sowie der Verdachtsmitteilungsschwelle** gemäss Art. 17 SPG und der Rolle der SFIU festgestellt werden. Sinn und Zweck von Verdachtsmitteilungen ist, dass die SFIU durch diese in die Lage versetzt wird, einen bestehenden Verdacht weitergehend abzuklären und diesen entweder auszuräumen oder zu erhärten. Der SFIU stehen hierfür diverse Instrumente – insbesondere der Austausch mit Partnerbehörden – zur Verfügung, die deutlich über das Mögliche von Sorgfaltspflichtigen hinausgehen. Eine solche Analyse setzt jedoch eine **funktionierende Überwachung von Geschäftsbeziehungen** sowie eine **umgehende Erstattung von Verdachtsmitteilungen** durch die Sorgfaltspflichtigen voraus.

Bei der SFIU handelt es sich gerade nicht um einen Teil der Strafverfolgungsbehörden und die Analyse findet vorgelagert zu allfälligen strafrechtlichen Ermittlungen und Verfahren statt. Für die Einleitung einer Analyse genügt der SFIU bereits ein **einfacher Verdacht** oder **Hinweis** auf ein **Vorgehen**, welches sich **potentiell als Vortat** herausstellen könnte. Insbesondere spielt es für die Erreichung der Verdachtsmitteilungsschwelle keine Rolle, ob ein strafrechtlich relevantes Verfahren noch nicht eingeleitet wurde oder ein gerichtlicher Entscheid ergangen, jedoch noch nicht rechtskräftig ist. Andernfalls würde das System der Verdachtsmitteilungserstattung sowie der damit verbundenen Analysetätigkeiten der SFIU ad absurdum getrieben.

Gemäss Ausführungen im Unterkapitel 2 «Voraussetzungen für die Erstattung einer Verdachtsmitteilung» des Kapitels C «Erläuterungen zur Mitteilungserstattung» der FIU-Wegleitung[3] reicht für die Bejahung der Mitteilungspflicht aus, wenn ein **objektiver Grund zur Annahme eines Verdachts** besteht, selbst wenn der Sorgfaltspflichtige subjektiv der Meinung ist, sein Vertragspartner habe sich nichts zuschulden kommen lassen.

[3] https://archiv.llv.li/files/sfiu/fiu-wegleitung_de.pdf

Stichworte:

- Mangelhafte laufende Überwachung
- Tiefe Frequenz betreffend Profil-Updates und Neubeurteilung des Risikos der Geschäftsbeziehung
- OSINT-Treffer
- Hinweise auf ausländische Strafverfahren
- Hinweise auf strafrechtliche Verurteilung im Ausland
- Mangelhaftes Verständnis betreffend die Verdachtsmitteilungsschwelle sowie die Rolle der SFIU

3. Risikoevaluierung von Kunden

Im Jahr 2021 eröffnete die inländische Bank «B» eine Geschäftsbeziehung für den Geschäftsmann «X», mit der Nationalität eines Drittstaates. Als Grund für die Eröffnung der Geschäftsbeziehung wurde vom Kunden das Verwalten seines Vermögens, das sich auf rund **CHF 35 Mio.** belief, angegeben. «X» verfolgte eine Laufbahn als Berater im Rohstoffbereich, einem Sektor, welcher für seine **hohe Korruptionsanfälligkeit** bekannt ist.

Die inländische Bank «B» stufte «X» im Zuge des Onboarding-Prozesses als «**tiefes Risiko**» ein. Dies obwohl seine diversen Tätigkeiten für Firmen, die in Hochrisiko-Sektoren und -Ländern aktiv waren, bekannt waren. Auch musste aufgrund des Vermögens von «X» angenommen werden, dass er **Schlüsselpositionen innerhalb dieser Gesellschaften** innegehabt haben musste.

Kurz nach Eröffnung der Geschäftsbeziehung bei der inländischen Bank «B» gingen **CHF 2 Mio.** auf das neu eröffnete Konto ein. Die Gelder wurden von einem ausländischen Konto lautend auf den Namen einer Firma, welche auf das Verwalten von Vermögen spezialisiert war, überwiesen.

Ein Jahr nach Eröffnung der Geschäftsbeziehung erlangte die inländische Bank «B» Kenntnis davon, dass Korruptionsermittlungen gegen einen früheren Arbeitgeber von Geschäftsmann «X» liefen. Konkret ging es um mögliche Verstrickungen in Bestechungsfälle. Aufgrund dieser Information fand die inländische Bank «B» heraus, dass bereits eine andere Gesellschaft, bei der «X» im Laufe seiner Karriere tätig war, noch vor der Eröffnung der Geschäftsbeziehung im Jahr 2021 wegen **Bestechung von ausländischen Amtsträgern**, um Zugang zu diversen Rohstoffen zu erhalten, verurteilt worden war.

Aufgrund dieser Informationen konnte die Bank eine potenziell strafbare Herkunft der eingebrachten Vermögenswerte nicht mehr ausschliessen und erstattete der SFIU umgehend Mitteilung. Um sicherzustellen, dass «X» sein Vermögen bei der inländischen Bank «B» nicht ins Ausland transferieren konnte und die SFIU mehr Zeit für die Aufbereitung des Analyseberichtes erhielt, machte sie von **Art. 18 Abs. 3 SPG und der damit verbundenen kurzfristigen Transaktionssperre** Gebrauch. Diese Bestimmung ermöglicht es der SFIU anzuordnen, dass Sorgfaltspflichtige Transaktionen in Bezug auf eine konkrete Geschäftsbeziehung für eine Frist von höchstens zwei Arbeitstagen nicht durchführen dürfen.

Die SFIU erhielt im Zuge des Analyseprozesses relevante **Informationen von ausländischen Partnerbehörden**. Dabei wurde bekannt, dass mittlerweile auch gegen den Geschäftsmann «X» selbst ein Strafverfahren eröffnet wurde. Im Rahmen der eingeleiteten inländischen strafrechtlichen Untersuchung konnten in der Folge vermögenssichernde Massnahmen ergriffen werden.

Bei diesem Fall stellt sich die Frage, ob die inländische Bank «B» den Kunden «X» in eine aufgrund der zum Zeitpunkt verfügbaren Informationen angemessene Risikokategorie einstufte. Obwohl einer der früheren Arbeitgeber von «X» zum Zeitpunkt des Onboardings bereits **verurteilt wegen Bestechung von ausländischen Amtsträgern** war und der Kunde zudem seine gesamte Karriere hindurch in für **Korruption anfälligen Sektoren und Ländern** tätig gewesen war, erfolgte eine Einstufung als «tiefes Risiko». Die Informationen zur Verurteilung seines früheren Arbeitgebers waren in öffentlichen Quellen mittels einfacher Suche ohne grossen Aufwand auffindbar.

Darüber hinaus ist der Fall hinsichtlich der «Mitteilungsgründe» zu beleuchten. Wie u.a. im Jahresbericht 2022[4] erläutert, werden nach wie vor die meisten Verdachtsmitteilungen letztendlich (mittelbar) durch **externe Faktoren**, wie beispielsweise Rechtshilfeersuchen, (ausländische) Strafverfahren, Medienberichte oder Treffer in kommerziellen Datenbanken ausgelöst. Auch im gegenständlichen Fall meldete die sorgfaltspflichtige Bank ihren Verdacht aufgrund einer **externen Information**. Auch wenn die Information, dass gegen den Geschäftsmann «X» zum Zeitpunkt der Eröffnung der Geschäftsbeziehung bei der inländischen Bank «B» ein Strafverfahren im Ausland lief, noch nicht in öffentlich zugänglichen Quellen auffindbar war, war doch einer der früheren Arbeitgeber von «X» bereits rechtskräftig verurteilt worden. Zudem hatte der Kunde «X» sowohl beim aktuellen als auch beim früheren Arbeitgeber jeweils eine Schlüsselposition inne. Die Sorgfaltspflichtige hätte folglich bereits vor dem Erhalt der externen Information **vertiefte Abklärungen vornehmen und detailliertere Angaben beim Kunden selbst** einholen müssen.

[4] https://www.llv.li/serviceportal2/amtsstellen/stabstelle-financial-intelligence-unit/fiu_jahresbericht_2022_de.pdf

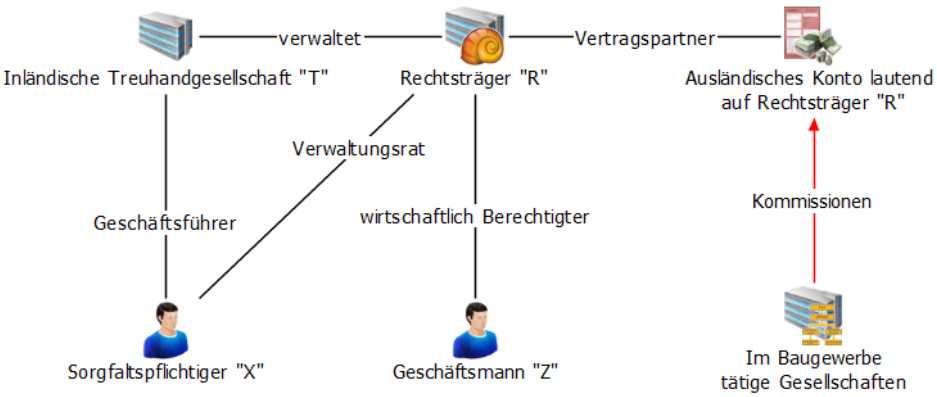
Einmal mehr zeigt sich, wie zentral die Berücksichtigung von **Informationen aus öffentlichen Quellen** ist. *Open Source Intelligence* (OSINT) bezeichnet in diesem Kontext die Nutzung frei verfügbarer, offener Quellen wie Printmedien, TV oder Internet zur Sammlung von Informationen zwecks Erkenntnisgewinnung.

Stichworte:

- Bestechung von ausländischen Amtsträgern
- Risikoevaluierung des Kunden entspricht nicht dem objektiven Risiko
- Verdachtsmitteilung an SFIU aufgrund externer Information
- Hochrisiko-Sektoren & -Länder
- Transaktionssperre durch SFIU
- Austausch von Informationen mit ausländischen Partnerbehörden

4. Verletzung der Mitteilungspflicht

Seit 2010 verwaltete die inländische Treuhandgesellschaft «T» den Rechtsträger «R». Der Geschäftsführer «X» von «T» fungierte als Verwaltungsrat von «R», wodurch «X» gemäss Art. 3 Abs. 1 Bst. k SPG **sorgfaltspflichtig** war. Beim Gründer und wirtschaftlich Berechtigten des Rechtsträgers «R» handelte es sich um einen aus einem afrikanischen Land stammenden Geschäftsmann «Z». Dieser trat als Vermittler von Aufträgen für diverse internationale Gesellschaften, die überwiegend im **Baugewerbe** tätig waren, auf. Die in den Rechtsträger «R» einfliessenden Vermögenswerte stammten aus **Kommissionen**, die «Z» für seine Vermittlungstätigkeiten erhielt. Im Schnitt betrug eine solche Kommissionszahlung CHF 50'000, wobei diese in unregelmässigen Abständen auf ein ausländisches Bankkonto transferiert wurden.



Die Treuhandgesellschaft «T» notierte bei der Aufnahme der Geschäftsbeziehung mit dem Rechtsträger «R» in dessen Profil, dass **keine schriftlichen Verträge**, welche die auf den Rechtsträger «R» eingehenden Zahlungen plausibilisieren könnten, vorhanden seien. Diese Angaben wurden in den darauffolgenden Jahren im Profil des Rechtsträgers «R» durch die Treuhandgesellschaft «T» jeweils bestätigt. Es wurden zu **keinem Zeitpunkt schriftliche Dokumente**, die die Herkunft der Vermögenswerte verifiziert hätten, eingeholt.

Der wirtschaftlich Berechtigte der «R», Geschäftsmann «Z», wurde gemäss öffentlich

zugänglichen Informationen im Jahr 2021 wegen **Verdachts auf Betrug und Veruntreuung** in seinem Heimatland inhaftiert und ein Jahr später zu einer vierjährigen **Haftstrafe** verurteilt. Diese Tatsache wurde im Profil über «R» und «Z» durch die inländische Treuhandgesellschaft «T» zwar erwähnt, ohne jedoch weitere Schritte zu unternehmen. Es wurde lediglich vermerkt, dass aufgrund der Inhaftierung von «Z» keine Möglichkeit zur Kontaktaufnahme bestand. Die dabei nötigen Abklärungen zur Sorgfaltspflicht bezüglich möglicher Geldwäschereitatbeständen wurden nicht vorgenommen.

Es gilt zu erwähnen, dass ein Jahr vor der Inhaftierung von «Z», im Jahr 2020, der autokratisch herrschende Präsident des Herkunftslandes von «Z» durch einen Putsch abgesetzt wurde. Geschäftsmann «Z» war öffentlichen Berichten zufolge eng mit dem ehemaligen **Präsidenten verbunden**. Darüber wurde jedoch im Profil, welches durch die Treuhandgesellschaft «T» über «R» und «Z» angelegt wurde – trotz der offensichtlichen Relevanz – nichts vermerkt. Die Möglichkeit, dass der Geschäftsmann «Z» durch seine enge Verbindung zum Ex-Präsidenten des Landes ein **hohes Risiko** dahingehend aufwies, dass dieser sich im «Dunstkreis» des mächtigen Politikers **bereichern** könnte, wurde offensichtlich ausgeblendet.

Erst aufgrund äusserer Einflüsse (Revision) erstattete die Treuhandgesellschaft «T» der SFIU 2023 – mehr als **zwei Jahre nach Bekanntwerden der Verhaftung** von «Z» – schliesslich Mitteilung. Basierend auf dieser Verdachtsmitteilung waren zwei unterschiedliche Sachverhalte zu prüfen: Einerseits bestand der **Verdacht auf geldwäschereirelevante Tatbestände** durch den Rechtsträger «T» sowie den Geschäftsmann «Z». Andererseits war zu prüfen, ob im gegenständlichen Fall eine **Verletzung der Mitteilungspflicht** gemäss Art. 17 Abs. 1 i. V. m. Art. 30 Abs. 1 Bst. a SPG durch den Geschäftsführer «X» vorlag.

Gemäss **Art. 17 Abs. 1 SPG** haben Sorgfaltspflichtige nach Art. 3 SPG der SFIU **umgehend schriftlich Mitteilung** zu erstatten, wenn der Verdacht auf Geldwäscherei, eine Vortat zur Geldwäscherei, organisierte Kriminalität oder Terrorismusfinanzierung besteht.

Es ist festzuhalten, dass jedenfalls spätestens ab dem Zeitpunkt der Publikation der öffentlichen Berichte, dass der Geschäftsmann «Z» wegen Verdachts auf Betrug und Veruntreuung in seinem Heimatland inhaftiert worden war – also im Jahr 2021 – ein Verdacht i. S. d. Art. 17 Abs. 1 SPG bestand. Dem Geschäftsführer «X» war bekannt, dass Anschuldigungen gegen «Z» im Raum standen, da eine entsprechende Aktualisierung des Geschäftsprofils aufgrund der Inhaftierung vorgenommen wurde. Spätestens ab diesem Zeitpunkt konnte **nicht mehr ausgeschlossen** werden, dass **Vermögenswerte** des Rechtsträgers «R» in Verbindung mit **potenziell kriminellen Tätigkeiten** standen.

Die **Mitteilung** an die SFIU erfolgte jedoch erst mehr als **zwei Jahre später**, wobei der aus der Revision resultierende Druck der Auslöser für diese Mitteilung war. Dies entspricht nicht den Vorgaben des Art. 17 Abs. 1 SPG, wonach ein Verdacht auf Geldwäscherei, eine Vortat der Geldwäscherei, organisierte Kriminalität oder Terrorismusfinanzierung «umgehend» der SFIU mitgeteilt werden muss. Folglich handelte es sich hier um eine **Verletzung der Mitteilungspflicht**.

Stichworte:

- Kommissionen aus Vermittlungstätigkeiten
- Involvierung Risikoland
- Verbindung zu (Ex-)PEP
- Mangelhafte Überwachung
- Fehlen von schriftlichen Verträgen/fehlende Verifizierung
- Verurteilung wegen Betruges und Veruntreuung
- Mitteilung nicht unmittelbar nach Bekanntwerden der Verdachtsfälle erstattet
- Verletzung der Mitteilungspflicht gemäss Art. 17 Abs. 1 i. V. m. Art. 30 Abs. 1 Bst. a SPG

5. Herausforderungen bei der Erkennung von Finanzierung von Rechtsterrorismus

Die SFIU erhielt eine Information einer europäischen Partnerbehörde, wonach ein «Herr X» wegen **Verdachts auf Vorbereitungshandlungen für einen terroristischen Anschlag** festgenommen worden sei. Die ausländische FIU teilte der SFIU ausserdem mit, dass «Herr X» seit Monaten vom nationalen Nachrichtendienst beobachtet wurde. Im Internet verbreitete der Verdächtige in einschlägigen Foren **rechtsextremes Gedankengut** und veröffentlichte Bilder, auf denen er mit Waffen posierte. In den sozialen Medien rief er zudem aktiv dazu auf, ihn bzw. seine Firma «Z» finanziell zu unterstützen, damit «*endlich einmal ein Zeichen gesetzt werde*», wie er schrieb. In diesem Zusammenhang konnten im Ausland auch Transaktionen mit einer Verbindung zu Liechtenstein festgestellt werden. Spätere Ermittlungen ergaben, dass «Herr X» geplant hatte, eine **lokale Moschee** während des Freitagsgebets zu stürmen und möglichst viele **Gläubige zu töten**.

Gemäss eingehender Informationen wurden von fünf inländischen Konten, Vermögenswerte in der Höhe von durchschnittlich CHF 500 – der geringste Wert betrug CHF 100, wobei sich der Maximalbetrag auf CHF 1'000 belief – auf ein ausländisches Bankkonto lautend auf «Herrn X» transferiert.

Die Informationen, welche die SFIU von den inländischen Banken zu den fünf Kontoinhabern erhielt, zeichnete ein **einheitliches Kundenbild** mit folgenden Merkmalen:

- Kunden ohne nennenswerte Vermögenswerte;
- Kunden aus dem Retail-Segment;
- Berufliche Tätigkeiten in Bereichen ohne inhärentes Geldwäscherei-/ Terrorismusfinanzierungs-Risiko;
- Nationalität, Geburtsort und Domizilland der Kunden als Länder mit tiefem Risiko gekennzeichnet;
- Kunden von Finanzinstituten in tiefste Risikoklasse eingestuft;
- Transfer von geringen Geldbeträgen (max. CHF 1'000);
- Überweisungen an «Herrn X» mit Schlagwörtern wie «Schenkung», «Unterstützung» oder «Zuwendung» kommentiert.

Zusätzlich zu den oben genannten Merkmalen der Kunden der inländischen Banken, war «Herr X» in den von den Finanzinstituten üblicherweise verwendeten kommerziellen Datenbanken nicht verzeichnet, wodurch auch die Gegenpartei der Geldtransfers («Herr X») **keine Treffer generierte**. Darüber hinaus war das Domizilland des Geldempfängers kein Risikoland. In dieser Konstellation zeigen sich folglich die **Grenzen des risikobasierten Ansatzes**.

Im gegenständlichen Fall handelte es sich um eine spezifische Form des Terrorismus – den sogenannten **Rechtsterrorismus**. Die Egmont Gruppe[5] definiert Rechtsterrorismus in ihrem Bericht «*FIU Capabilities and Involvement in the Fight against the Financing of Extreme Right-Wing Terrorism: State of Play and Perspectives*[6]» als Anwendung terroristischer Gewalt durch rechtsextreme Gruppen wie Neonazis, Neofaschisten und ultranationalistische Gruppierungen. Dabei ist ein zentrales Konzept des Rechtsextremismus die Vorstellung, dass eine bestimmte Gruppe von Menschen mit einem gemeinsamen Element (z.B. Nation, Rasse oder Kultur) allen anderen überlegen ist.

Es wird ersichtlich, dass sich in Fällen von potenzieller (Rechts-)Terrorismusfinanzierung das Erkennen von verdächtigen Geldflüssen durch die Finanzinstitute als äusserst herausfordernd gestaltet. So schreibt die Financial Action Task Force (FATF)[7] in ihrem Bericht «*Ethnically or Racially Motivated Terrorism Financing*[8]», dass aufgrund der Tatsache, dass die meisten rechtsextremistisch-motivierten Attacken von einzelnen Akteuren durchgeführt werden, es nur **begrenzt Informationen** darüber gibt, wie sich die Geldflüsse gestalten. Da die **Kosten** für diese Art von Terrorismus relativ **gering** sind, erscheinen die **Transaktionen** der Täter nur **selten als verdächtig**.

Dieser Sachverhalt verdeutlicht die Herausforderung, mögliche Terrorismusfinanzierungen durch Sorgfaltspflichtige zu entdecken. Der dargestellte Sachverhalt soll jedenfalls einige potenzielle Anhaltspunkte aufzeigen.

Es ist festzuhalten, dass die Sorgfaltspflichtigen grundsätzlich nicht die erforderlichen Möglichkeiten haben, abschliessend festzustellen, ob der Tatbestand der Terrorismusfinanzierung gemäss Art. 278d StGB erfüllt ist. Dies ist jedoch nicht erforderlich, da bereits der **reine Verdacht ausreichend** für eine Verdachtsmitteilung an die SFIU ist.

---

[5] https://egmontgroup.org/

[6] https://egmontgroup.org/wp-content/uploads/2022/01/IEWG-ERWTF-public-bulletin2.pdf

[7] https://www.fatf-gafi.org/en/home.html

[8] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Ethnically-or-racially-motivated-terrorism-financing.pdf.coredownload.inline.pdf

Bei dieser Gelegenheit wird ergänzend auf die Ausführungen im Unterkapitel 2 «Voraussetzungen für die Erstattung einer Verdachtsmitteilung» des Kapitels C «Erläuterungen zur Mitteilungserstattung» der FIU-Wegleitung[9] verwiesen, wonach die Sorgfaltspflichtigen **im Zweifel eine Mitteilung** machen sollen. Können nach Vornahme der Abklärungen nach Art. 9 SPG die **Verdachtsmomente nicht beseitigt** werden, ist die **Mitteilungspflicht zu bejahen**. Besondere Voraussetzungen (zum Beispiel im Sinne eines «begründeten Verdachts») sind nicht gefordert.

Stichworte:

- Rechtsterrorismus als spezifische Form des Terrorismus
- Herausforderungen bei der Erkennung von TF-Transaktionen
- Unauffällige Kundschaft
- Grenzen des risikobasierten Ansatzes
- Grosse Bedeutung von OSINT & sozialer Medien
- Im Zweifel eine Verdachtsmitteilung erstatten

6. Terrorismusfinanzierung und besonders vulnerable Sektoren

Nebst dem Bankensektor, der, wie im vorhergehenden Fall geschildert, anfällig dafür ist, für die Finanzierung von Terrorismus missbraucht zu werden, gibt es **weitere Sektoren**, die ein erhöhtes Terrorismusfinanzierungs-Risiko aufweisen.

Insbesondere **Zahlungsinstitute** sowie **VT-Dienstleister** und **Betreiber von Handelsplattformen für nicht-fungible Token** sind mit Blick auf die angebotenen Dienstleistungen vulnerabel, um zum Zwecke der Terrorismusfinanzierung missbraucht zu werden. Das nachfolgende Beispiel steht stellvertretend für eine bekannte Vorgehensweise von Terrorismusunterstützern.

Zwischen Mai 2020 und August 2022 tätigte «Frau X» insgesamt **zehn Transaktionen** im Gesamtwert von rund **CHF 3'200**, wobei sie jeweils dasselbe inländische Zahlungsinstitut an verschiedenen Orten im Land benutzte. Die Geldüberweisungen in Fiatwährung gingen an insgesamt drei Individuen mit Wohnsitz in zwei verschiedenen **Ländern im Südosteuropa**. «Frau X» brauchte dabei Verwendungszwecke wie «Schenkung», «Unterstützung» oder «Spende».

Im Januar 2023 – also rund fünf Monate nach der letzten Überweisung – wurde ein Artikel in einer osteuropäischen Zeitung veröffentlicht, wonach mehrere Personen in einem südosteuropäischen Land wegen des **Verdachts zur Aufforderung zur Begehung von terroristischen Straftaten** angeklagt worden seien. Eine dieser war namensidentisch mit «Herrn Z», der als einer der drei Geldempfänger der Überweisungen von «Frau X» mittels zwei Transfers einen **Geldbetrag in Höhe von insgesamt CHF 750** erhalten hatte. Das inländische Zahlungsinstitut erstattete umgehend eine Verdachtsmitteilung an die SFIU wegen **Verdachts auf Terrorismusfinanzierung**. Dabei war es dem inländischen Zahlungsinstitut nicht möglich, das Verhältnis von «Frau X» zu den drei Individuen, die Gelder erhielten, und insbesondere zu «Herrn Z»,

[9] https://archiv.llv.li/files/sfiu/fiu-wegleitung_de.pdf

festzustellen. Auch war nicht abschliessend bestimmbar, ob es sich beim Individuum, welches im Zeitungsartikel erwähnt wurde, tatsächlich um den Geldempfänger handelte oder ob die beiden Personen lediglich namensidentisch waren. Da **nicht ausgeschlossen werden konnte**, dass es sich um dasselbe Individuum handelte, erfolgte korrekterweise die Verdachtsmitteilung des Sorgfaltspflichtigen.

Im vorliegenden Fall waren zudem die **folgenden Indikatoren** für den Verdacht der Terrorismusfinanzierung relevant:

- Einzelperson («Frau X»), welche Gelder an mehrere Personen in unterschiedlichen Ländern sendete, ohne dass jeweils eine offensichtliche (verwandtschaftliche o.ä.) Beziehung zueinander bestand;
- Geldüberweisungen in Länder, welche ein erhöhtes Risiko für Terrorismusfinanzierung aufwiesen;
- Als Zahlungszweck wurden Schlagwörter in Verbindung mit Wohltätigkeits- und Hilfszahlungen angegeben.

Im Zuge ihrer Analyse stellte die SFIU fest, dass ein auf «Frau X» lautendes Konto bei einer inländischen Bank geführt wurde. Nachforschungen ergaben, dass keine verdächtigen Transaktionen über dieses Konto ausgeführt wurden. Jedoch hob «Frau X» wiederholt **Barbeträge an Geldautomaten** im Wohnsitzland von «Herrn Z» in **Südosteuropa** ab. Im Rahmen ihrer Analyse fand die SFIU ausserdem heraus, dass «Herr Z» wegen des Verdachts zur Aufforderung zur Begehung von terroristischen Straftaten angeklagt wurde und es sich um dieselbe Person wie den Transaktionsempfänger handelte. Dies zeigte, dass vermeintlich unauffällige Beträge von einem inländischen Zahlungsinstitut mit dem **mutmasslichen Ziel** versendet wurden, **terroristische Aktivtäten zu unterstützen**.

Zusätzlich zu den im vorherigen und diesem Sachverhalt erwähnten Dienstleister (Bank- & Zahlungsinstitute), die ein besonderes Risiko aufweisen, für Terrorismusfinanzierung missbraucht zu werden, gilt es den **Krypto-Sektor** hervorzuheben. Aufmerksame Leser der früheren SFIU-Fallsammlungen werden festgestellt haben, dass Fälle von Terrorismusfinanzierung oftmals eine Verbindung zu Kryptowährungen aufweisen. Dabei mache gemäss «*The 2024 Crypto Crime Report*[10]» die Verwendung von Kryptowährungen durch terroristische Organisationen nur einen kleinen Teil der illegalen Transaktionen im Kryptowährungs-Universum aus, wobei dies dennoch ein allgegenwärtiges Problem sei.

Analog zum traditionellen Finanzsystem ist es im Rahmen von Krypto-Transaktionen möglich, bestimmte **verdächtige Verhaltensweisen zu erkennen** und an die SFIU mitzuteilen. Die Kombination der durch die **Indikatoren** angezeigten Transaktionen mit anderen Informationen, die im Rahmen der Analyse des Kunden gewonnen wurden (insbesondere **KYC-Informationen**), hilft bei der Feststellung, ob hinreichende Gründe für eine Verdachtsmitteilung vorliegen.

Für die Thematik der Terrorismusfinanzierung mittels Kryptowährungen sei auf den Anhang 3, III, E der SPV für Anhaltspunkte in Bezug auf VT-Dienstleistungen sowie Anhang 3, IV der SPV für Anhaltspunkte für

[10] Der Bericht muss mittels Angabe persönlicher Informationen heruntergeladen werden. Dies kann unter diesem Link gemacht werden.

Terrorismusfinanzierung verwiesen. Zusätzlich erwähnt der im Juni 2023 veröffentliche Bericht «*Report on Abuse of Virtual Assets for Terrorist Financing Purposes*[11]» der Egmont Gruppe eine ganze **Reihe von nützlichen Indikatoren**, um die potenzielle Nutzung von Kryptowährungen für den Zweck der Terrorismusfinanzierung zu erkennen. Sie finden diese Indikatoren im Anhang aufgelistet.

[11] Der offizielle Bericht der Egmont Gruppe ist nicht zur Veröffentlichung bestimmt (die Indikatoren dürfen selbstverständlich geteilt werden). Die öffentliche Version des Berichts kann hier gefunden werden.

III. Anhang: Indikatoren bzgl. potenzieller Nutzung von Kryptowährungen für den Zweck der Terrorismusfinanzierung

Red Flag Indicators Related to Transactions

The below list of red flag indicators contributed by participating FIUs may be useful to indicate potential utilization of VAs for TF purposes.

- Use of VASPs to transfer funds to wallets linked to cluster/wallet of known terrorist organisations or any organisations linked to violent extremism or radicalization.
- VA transactions are linked to extortion and ransomware.
- VA transactions with no link between the stated activity and the recipient.
- "Money mules" using VA ATMs to make deposits at different times and locations into the same address.
- Use of vouchers to purchase VAs.
- Purchase or sale of VAs in cash, irrespective of the amount.
- Cryptocurrency transfers to bank accounts where the VA is linked to:
  - Fake virtual currency exchanges.
  - The advertising of an unknown cryptocurrency on social networks where users identify the advertising as a scam in their comments.
  - Computer games, such as Minecraft.
  - The creation of own cryptocurrency in an attempt to legitimise proceeds of crime.
- Multiple transfers from fiat to VAs and vice versa on the same day.
- High volume and frequency of transfers between different types of VAs.
- The VA flows through a large number of intermediate addresses in a very short period of time prior to withdrawal or being added to a client's wallet.
- Incoming small transfers from many unrelated wallets with subsequent transfers to another wallet.
- The use of multiple VASPs, addresses, and wallets in several jurisdictions.

Related to Anonymity

- Use of the dark web, mixer/tumbler transactions or Coinjoin services in the case of virtual currencies.
- The VA passes through mixers/tumblers and is transferred to multiple wallets before being exchanged for fiat currency.
- Customer transactions involving more than one type of cryptocurrency or "chain-hopping" (trading one cryptocurrency for another), particularly to privacy coins (Monero, Dash, or Zcash).
- Portfolios that only consist of privacy coins or have a high value in privacy coins.
- Transfers of cryptocurrencies in micro-payments or large volumes in exchange for privacy coins.
- Virtual currency funds or privacy coins (Monero, Dash or Zcash) originating from an over-the-counter trade broker that advertises its services as privacy-oriented or anonymous.
- Client provides an anonymous email address obtained through an encrypted email service.
- Use of virtual wallets registered to a third party.

Related to Senders or Recipients

- The creation of a client relationship and/or initial transaction references a connection with a high-risk country (e.g., place of birth, address, telephone number, email address, IP address).
- New client relationship established with suspicious identity document, or the identity document is not legible.
- A non-profit organisation, foundation, or other association uses complex combined transaction chains (cash, payment institutions, virtual currencies, etc.) when executing payments.
- The wallet is held by individuals known to be connected to a TF scheme (sometimes via publicly available information) or has sending exposure to terror group fundraising activities.
- Client's wallet address has links or hops to or from a wallet address that has appeared on online platforms indicating support for violent extremism or radicalization (including social media, ads on fundraising sites, sites on Tor or messaging sites).
- Client's wallet or address is linked to fraudulent activity in media reports and/or cyber security bulletins.
- RE matches or has links to entities named in open-source law enforcement lists or the Office of Foreign Assets Control (OFAC).
- Many clients register with the exchange within a short period using a shared address, mobile device, phone number, IP address, and other common identity indicators.
- A broker charges abnormally high commission fees compared to the industry standard.
- Funds from or to a high-risk cryptocurrency exchange platform.

Related to Source of Funds or Wealth

- Client refuses or is unable to present CDD documents or information (including concerning the origin of property).
- Client is unwilling or unable to provide information about the source of privacy coins they once held or currently have.
- A series of complicated transfers of funds or VAs to multiple addresses or wallets that seems to be an attempt to hide the source and/or intended use of the funds or VAs.
- Funds or VAs are added or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (such as ransomware) and/or theft reports.

Related to Source of Funds or Wealth

- Client refuses or is unable to present CDD documents or information (including concerning the origin of property).
- Client is unwilling or unable to provide information about the source of privacy coins they once held or currently have.
- A series of complicated transfers of funds or VAs to multiple addresses or wallets that seems to be an attempt to hide the source and/or intended use of the funds or VAs.
- Funds or VAs are added or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (such as ransomware) and/or theft reports.

Related to Geographical Risks

- The VA transaction, or planned transaction, is linked to a VASP located in or received from a high-risk country.
- Forwarding VAs to or from a non-profit organisation, foundation, or other association/organisation that operates in a high-risk country or offers assistance or services to persons associated with a high-risk country.
- Use of IP addresses located in a conflict zone or sensitive area.
- VA transactions originating from FATF's non-cooperative countries and territories.

Geographical risks associated with exchange transactions usually take place via VA exchanges or brokers. The choice of digital asset exchanges and brokers for an exchange transaction should not be underestimated.