

Casi

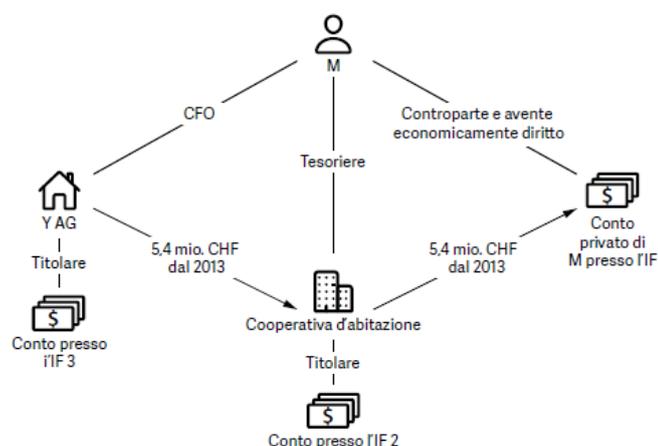
1. Sospetto di appropriazione indebita

Fattispecie

Il consulente alla clientela dell'intermediario finanziario (di seguito: «IF») constata bonifici anomali sul conto privato di M., effettuati dalla cooperativa d'abitazione X. Secondo le informazioni figuranti nel profilo cliente allestito dall'IF, M. sarebbe il tesoriere della cooperativa in questione. Inoltre, M. sarebbe anche responsabile delle finanze (CFO) e membro del consiglio d'amministrazione dell'impresa di costruzioni Y AG.

Dall'analisi delle transazioni effettuata dall'IF emerge che la relazione d'affari intestata a M. è stata alimentata principalmente da fondi provenienti dalla cooperativa d'abitazione X. I bonifici insolitamente elevati non possono costituire salari che il cliente avrebbe potuto percepire per la sua funzione di tesoriere. In totale, la cooperativa d'abitazione X. ha versato sul conto privato di M. un totale di oltre 5 milioni di franchi, provenienti da un conto ad essa intestato e aperto presso un altro intermediario finanziario.

L'IF contatta il cliente, che in un primo momento, dichiara di incassare provvigioni per progetti di costruzione che conduce per conto proprio. L'IF non riesce però ad accertare quale sia la causale di questi versamenti e per quali progetti il cliente M. dovrebbe ricevere a questo titolo fondi provenienti dalla cooperativa X. In base alla documentazione fornita da M. all'IF in occasione di un appuntamento, sembra che i fondi versati dai conti della cooperativa provengano in realtà dalla società Y AG, di cui M. è CFO. Questi fondi transitano attraverso il conto della cooperativa d'abitazione X. L'IF non riesce a verificare l'autenticità della documentazione prodotta e neanche il colloquio con M. consente di accertare i retroscena economici di queste transazioni. Lo schema delle transazioni corrobora i sospetti dell'IF. I fondi accreditati sul conto privato di M. potrebbero essere frutto di un'appropriazione indebita commessa dal cliente in veste di tesoriere della cooperativa d'abitazione X. o di CFO della società Y AG. Il fatto che la società di costruzioni Y AG abbia rinunciato a una revisione ordinaria e a una revisione limitata in seguito a una decisione del consiglio di amministrazione prima dell'inizio delle transazioni sospette, rafforza ulteriormente i sospetti dell'IF in merito alla potenziale presenza di un reato di appropriazione indebita; l'IF trasmette quindi a MROS una segnalazione relativa alle relazioni d'affari intrattenute con M.



Soluzione

L'identificazione e la documentazione da parte dell'IF delle transazioni ha permesso in seguito a MROS di formulare una serie di domande precise ai sensi dell'art. 11a cpv. 2 e 3 LRD e di acclarare rapidamente i fatti.

Buone pratiche dell'intermediario finanziario autore della segnalazione

- **Il consulente alla clientela è stato attento e ha individuato alcune transazioni sospette**, sicché il dipartimento Compliance ha proseguito gli accertamenti effettuando ulteriori verifiche. Questo esempio dimostra l'importanza del ruolo dei consulenti alla clientela i quali fungono da primo strumento di difesa del dispositivo antiriciclaggio a disposizione degli intermediari finanziari. I consulenti sono tenuti a individuare e a chiarire tempestivamente eventuali attività sospette nelle relazioni d'affari dei loro clienti al fine di poter adottare rapidamente le misure eventualmente necessarie.
- **Grazie alla documentazione precisa fornita dall'intermediario finanziario, MROS ha potuto effettuare accertamenti mirati.** Benché MROS individui spesso nuove piste nell'ambito delle sue analisi, la documentazione completa, precisa e la valutazione dell'intermediario finanziario costituiscono il punto di partenza di queste analisi. Una documentazione allestita in modo accurato può aumentare considerevolmente l'efficacia di MROS.

2. Sospetta tratta di esseri umani / prostituzione forzata

Fattispecie

Sul conto di una cliente, la quale ha indicato di gestire un salone di bellezza, è stato identificato lo schema transazionale seguente: per un anno, il conto è stato alimentato con frequenti versamenti in contanti per un totale di oltre 70 000 franchi. Questi versamenti venivano effettuati dalla cliente stessa ma anche da diverse altre donne. Ciò che ha particolarmente colpito l'IF, è il fatto che questi importi venivano versati in parte in una città svizzera e nei giorni successivi venivano prelevati in un'altra città svizzera o altrove in Europa. Dall'analisi delle transazioni e dagli ulteriori accertamenti condotti è emerso che sia la cliente sia le altre donne avevano legami con ambienti a luci rosse. A seguito di una delle transazioni di passaggio verso un Paese terzo europeo, l'IF scopre, tramite le sue ricerche, che il destinatario era il presunto compagno della cliente. Nell'ambito di successivi accertamenti, l'IF trova su World Check che il destinatario del denaro, nonché presunto compagno della cliente, avrebbe dei legami con la criminalità organizzata e la tratta di esseri umani. L'IF ha inoltre notato pagamenti regolari e frequenti per pubblicità su piattaforme di intrattenimento per adulti. Data la frequenza delle spese per annunci pubblicitari, l'intermediario ha intuito che i pagamenti venivano effettuati per più di una persona. Inoltre, erano stati pagati canoni di locazione per diversi alloggi, fatto inconsueto dato il profilo della cliente. Infine, anche il comportamento e le dichiarazioni incoerenti e apparentemente poco plausibili della cliente hanno indotto l'IF a esaminare più da vicino la relazione d'affari. La cliente aveva dichiarato di gestire un salone di bellezza e che i suddetti versamenti effettuati da altre donne costituivano pagamenti per trattamenti di bellezza. A riprova di queste affermazioni, la cliente ha fornito le corrispondenti fatture. Tuttavia, da ricerche effettuate su fonti pubbliche l'IF non è riuscito a individuare un salone di bellezza che avesse il nome indicato o fosse in relazione con la cliente. Inoltre, l'IF dubitava anche dell'autenticità dei giustificativi da lei prodotti: per esempio una persona aveva ricevuto un insolito numero elevato di trattamenti; in quel periodo la cliente si trovava all'estero, dove diceva di aver effettuato i trattamenti; in altri giustificativi prodotti figuravano prezzi diversi per gli stessi trattamenti.

Soluzione

Buone pratiche dell'intermediario finanziario autore della segnalazione

- **L'intermediario finanziario ha immediatamente notato i movimenti sospetti, e, dopo aver proceduto agli opportuni accertamenti, ha trasmesso senza indugio una comunicazione di sospetto.** L'invio tempestivo di una comunicazione di sospetto è essenziale per l'efficienza dell'operato di MROS. Da un lato, aumenta le probabilità di rintracciare o addirittura bloccare gli averi in questione, e, dall'altro le informazioni possono rappresentare un importante complemento per procedimenti già in corso in Svizzera o all'estero.
- **L'intermediario finanziario ha effettuato ricerche approfondite nelle fonti pubbliche.** Queste ricerche hanno consentito in particolare di poter controllare le persone coinvolte e i loro presunti indirizzi e di scoprire che queste persone avevano legami con gli ambienti a luci rosse. Inoltre, per uno dei destinatari del denaro, il presunto compagno della cliente, la ricerca nella banca dati World Check ha fornito un riscontro rilevante.
- **Divieto di divulgazione («tipping off»): la cliente è stata interrogata con discrezione su tutte le transazioni sospette. Le sue dichiarazioni incoerenti, incomplete e sospette sono state documentate e spiegate in modo dettagliato;** le informazioni ricevute dai clienti (nella misura in cui ciò sia possibile senza che i clienti in questione si accorgano dei sospetti che l'intermediario finanziario ha nei loro confronti) sono un elemento importante delle informazioni trasmesse a MROS con una comunicazione di sospetto. MROS non è autorizzato a contattare direttamente i clienti degli intermediari finanziari. Quindi, sotto questo aspetto, deve basarsi sulle informazioni raccolte dall'intermediario finanziario. Il comportamento dei clienti, per esempio la coerenza o la correttezza delle loro affermazioni, possono fornire utili indizi a MROS per le sue analisi. Tuttavia, è importante che l'intermediario finanziario esamini tali informazioni e indizi con spirito critico, e che fornisca a MROS tutti gli elementi necessari per valutare ed eventualmente verificarne l'attendibilità. L'intermediario finanziario conosce meglio di chiunque altro i propri clienti e dovrebbe quindi sfruttare questo vantaggio durante le sue analisi.

L'intermediario finanziario ha effettuato un'analisi dettagliata delle transazioni e riassunto con precisione le principali transazioni. In particolare, l'intermediario finanziario ha condotto accertamenti in merito alle controparti e analizzato in dettaglio le fatture prodotte dalla cliente a giustificazione dei pagamenti insoliti e verificato la plausibilità del loro contenuto.

I documenti e gli allegati trasmessi erano completi e ogni elemento di sospetto era ben documentato. MROS non ha dovuto richiedere alcun documento mancante. Le richieste di documenti complementari effettuate ai sensi dell'art. 11a cpv. 1 LRD sono dispendiose, sia per MROS sia per l'intermediario finanziario segnalante. Secondo l'art. 3 cpv. 1 lett. h OUD, l'intermediario finanziario segnalante deve assicurarsi che gli elementi di sospetto su cui si basa la sua comunicazione siano descritti per quanto possibile in modo preciso, e che vengano trasmessi tutti i documenti utili.

Conclusione

La conoscenza delle varie caratteristiche e degli indicatori dei reati preliminari al riciclaggio di denaro costituisce un presupposto importante nell'ambito di una strategia di conformità efficiente. Vari indizi o combinazioni di indizi portano alla supposizione dell'esistenza di diversi reati preliminari. Nel caso della tratta di esseri umani, per esempio, si possono individuare indicatori diversi rispetto ai casi di corruzione o truffa. **Nella fattispecie, l'intermediario finanziario ha evidenziato indicatori importanti per l'individuazione del reato di tratta di esseri umani o di sfruttamento della prostituzione, e, in particolare i seguenti¹:**

- frequenti pagamenti in contanti;

¹ Per un'illustrazione più dettagliata degli indicatori e della casistica per l'identificazione di casi di tratta di esseri umani e reati preliminari affini, cfr. p. es. rapporto del GAFI *Financial Flows from Human Trafficking*, luglio 2018.

- versamenti sul conto in una città e corrispondenti prelievi in un'altra città (transazioni di passaggio);
- trasferimento di importi piuttosto esigui;
- versamenti effettuati da numerose persone o destinati a numerosi beneficiari;
- trasferimenti di denaro verso l'estero a persone e società localizzate in Paesi da cui proviene un'elevata percentuale di vittime della tratta di esseri umani;
- versamenti ricorrenti e frequenti per pubblicità su piattaforme di intrattenimento per adulti;
- spese frequenti per vari hotel o alloggi in affitto;
- spese non corrispondenti alla documentazione KYC («Know Your Customer») del cliente;
- legami con gli ambienti a luci rosse.

La relazione d'affari è stata segnalata sulla base di un approccio olistico a seguito della concomitanza di diversi elementi che, se considerati isolatamente, non bastano a fondare un sospetto; un legame con gli ambienti a luci rosse, per esempio, non è di per sé un motivo sufficiente per far nascere dei sospetti: se si rispettano determinate regole, in Svizzera la prostituzione è legale. Questi vari elementi, in combinazione con altri fattori sospetti come per esempio i riscontri forniti dalla ricerca effettuata nella banca dati World Check come nel caso di specie, possono però essere indicativi dell'esistenza di un reato preliminare. L'approccio olistico dell'intermediario finanziario segnalante ha permesso quindi di scoprire dei legami i quali non sarebbero emersi basandosi su un approccio più unilaterale (incentrato su elementi isolati della relazione d'affari, quali p. es. le transazioni o gli aspetti KYC).

3. Sospetto riciclaggio di denaro per mestiere

Fattispecie

Un IF controlla il conto privato di un avvocato che da diversi anni non è più iscritto all'ordine e con il quale intrattiene una relazione d'affari. L'IF constata l'esistenza di numerosi mittenti di fondi i quali versamenti sono rapidamente trasferiti su altri conti in Svizzera e all'estero. Il conto è dunque stato utilizzato come conto di passaggio e l'avvocato ha avuto un ruolo di agente escrow. L'intermediario chiede quindi spiegazioni al proprio cliente. Constata che il cliente si presenta a terzi come avvocato iscritto all'ordine nonostante da anni non lo sia più. L'avvocato spiega che, pur non patrocinando più, ha conservato una clientela che segue come consulente legale. In particolare, ha messo il proprio conto a disposizione dei clienti. A suo dire, uno dei suoi clienti non potrebbe effettuare talune transazioni a causa del dispositivo di prevenzione antiriciclaggio. L'avvocato produce diversi atti giuridici a conferma delle dichiarazioni da lui rilasciate all'IF. Da parte sua, quest'ultimo effettua alcune ricerche sulle controparti clienti dell'avvocato e trova articoli di giornale e altri riscontri negativi. Uno dei clienti risulta essere oggetto di un procedimento penale all'estero. Non potendo fugare il dubbio che l'avvocato abbia riciclato denaro per i propri clienti, l'IF segnala il conto personale del proprio cliente a MROS.

Soluzione

Buone pratiche dell'intermediario finanziario autore della segnalazione

- **L'intermediario finanziario ha orientato le proprie ricerche e i propri accertamenti in base al profilo del cliente.** L'analisi delle transazioni gli ha permesso di constatare l'esistenza di diversi bonifici provenienti da diverse controparti e l'utilizzo del conto come conto di passaggio.
- **L'intermediario finanziario ha dunque svolto ricerche approfondite sulle controparti** trovando informazioni negative che ha provveduto a documentare correttamente.

4. Sospetta sottrazione di virtual asset

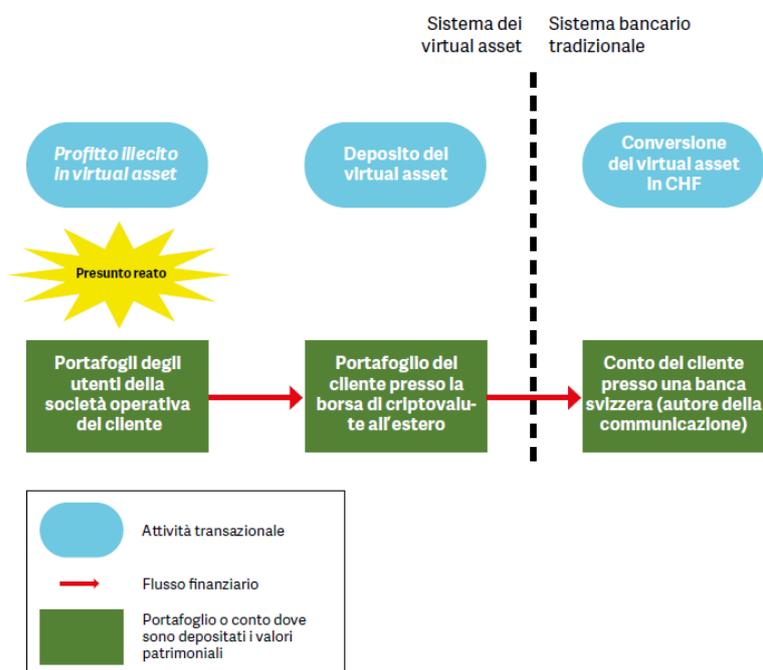
Fattispecie

Alcuni clienti di un IF del settore bancario sembrerebbero operare nel settore dei virtual asset, in particolare attraverso una delle loro società operative. Il loro patrimonio proverrebbe essenzialmente da

questa società e da investimenti in criptovalute effettuati quando questa tecnologia era ancora agli albori. In seguito a un'insolita richiesta urgente presentata dai suoi clienti, l'IF ha seguito con particolare attenzione il gruppo di relazioni d'affari in questione, coinvolgendo anche il dipartimento compliance, è stato inoltre notato un comportamento insolito nelle transazioni effettuate. In un breve lasso di tempo, sui conti dei clienti in questione sono stati effettuati diversi versamenti per un totale di centinaia di migliaia di franchi. Gli importi depositati provenivano in larga parte da borse di cripto valute molto note e registrate in varie giurisdizioni. Parte di questi depositi proveniva dunque verosimilmente dalla conversione o dalla vendita di monete virtuali. A seguito di queste transazioni sospette, l'IF ha provveduto dunque a effettuare una serie di accertamenti, al termine dei quali è sorto il dubbio che queste transazioni avessero potuto costituire una sottrazione di fondi di clienti e utenti delle borse in questione. Altre transazioni sospette effettuate in un secondo tempo hanno rafforzato tale sospetto. L'IF ha prontamente definito un campo d'indagine riguardante l'origine dei fondi in cripto valute e la loro conformità fiscale. Gli accertamenti condotti si sono presto concentrati su aspetti tecnici quali l'ottenimento di schermate dei conti dei clienti dell'IF sulle borse di criptovalute e la raccolta delle prove relative alla provenienza delle criptovalute depositate su tali piattaforme al fine di poter infine risalire alla traccia cartacea (paper trail). L'IF ha anche cercato di raccogliere le prove dell'esistenza dei valori patrimoniali detenuti in criptovalute dei suoi clienti e depositati presso una borsa di criptovalute o in portafogli non ospitati (private / self-hosted / unhosted / non-custodial wallet).

Il campo d'indagine definito dall'IF comprendeva anche la questione della legittimità della società operante nel settore dei virtual asset, appartenente ai suoi clienti. Gli accertamenti condotti includevano per esempio la questione delle eventuali autorizzazioni richieste per tale attività nelle varie giurisdizioni interessate e i dubbi sulle informazioni pubblicate nel sito Internet della suddetta società.

Al termine dei suoi accertamenti, l'IF ha ipotizzato l'esistenza di una possibile sottrazione di fondi dei clienti, o utenti della società, e ha segnalato a MROS le relazioni d'affari detenute con il gruppo di persone in questione



Soluzione

Buone pratiche dell'intermediario finanziario autore della segnalazione

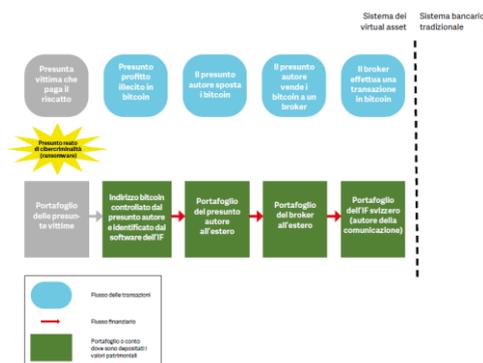
- **L'intermediario finanziario definito «tradizionale» ha dato prova di un'eccellente capacità di comprensione dei rischi che caratterizzano l'universo delle crypto valute.** Pur non essendo riuscito a ottenere tutti i chiarimenti richiesti, ha raccolto e documentato elementi pertinenti e preziosi per l'analisi di MROS sull'origine dei fondi e sull'attività della società del cliente. Tali chiarimenti hanno permesso a MROS in particolare di inviare tre richieste d'informazione a FIU estere e di ottenere informazioni riguardanti per esempio l'origine dei valori patrimoniali in crypto valute su una delle piattaforme o la legittimità della suddetta società.

5. Sospetta contaminazione indiretta

Fattispecie

L'IF opera nel settore delle crypto valute e può essere classificato come fornitore di servizi finanziari in relazione ai valori patrimoniali virtuali (virtual asset service provider, VASP). Nell'ambito di un controllo periodico delle transazioni, uno dei software di analisi blockchain dell'IF, identifica un livello di rischio elevato su transazioni in bitcoin effettuate per conto dei clienti. L'allarme generato dallo strumento di analisi sembra indicare l'esistenza di un nesso indiretto tra queste transazioni e attività cybercriminali di tipo ransomware². L'IF scopre che le transazioni sospette sono state effettuate nell'ambito dell'acquisto di alcune decine di bitcoin presso un partner commerciale all'estero. I bitcoin in questione sono stati acquistati per conto di un cliente dell'IF. Questo partner commerciale è una società di brokaggio «over the counter» (OTC broker) e quindi un VASP, assoggettato a obblighi di diligenza e registrato presso un'autorità di vigilanza.

L'IF attua dunque un protocollo che prevede una serie di accertamenti che hanno principalmente due obiettivi: in un primo momento, l'IF cerca di chiarire la situazione presso il broker, anche per capire se avesse già effettuato accertamenti da parte sua e quali fossero stati i risultati. Successivamente, l'IF effettua un'analisi indipendente e accurata per capire il motivo per cui il software di analisi blockchain abbia segnalato un livello di rischio importante e se tale risultato possa giustificare di per sé una comunicazione a MROS. A tal fine, effettua un'analisi approfondita della fonte utilizzata dal software di analisi. Si tratta dunque di cercare di scoprire se sia stato effettivamente commesso un reato. La ricerca condotta comprendeva anche l'impiego di vari software di analisi blockchain per ricostruire il flusso delle transazioni e paragonare i risultati. Alla luce dell'analisi dei flussi delle transazioni e degli accertamenti condotti, l'IF ha ipotizzato che se fosse stato effettivamente commesso un reato, esisterebbe dunque un legame tra tale reato e un cliente del proprio partner commerciale all'estero. Alla fine degli accertamenti previsti dal protocollo, l'IF ha pertanto deciso di segnalare il caso a MROS.



² Per «ransomware» si intende un tipo di malware, ossia un programma informatico che si installa su un computer e lo blocca o cripta i dati in esso contenuti. Nella maggior parte dei casi il computer viene infettato con il metodo detto drive by download (ossia per caricamento involontario). Affinché il malware si installi basta che la vittima visiti un sito Internet manipolato tramite un computer non sufficientemente protetto. In seguito i criminali chiedono il pagamento di un riscatto per decodificare i dati o sbloccare il computer. Talvolta il malware invia un messaggio apparentemente ufficiale avvalendosi dei loghi della polizia a seconda del Paese e chiedendo alla vittima di pagare una multa.

Soluzione

Buone pratiche dell'intermediario finanziario autore della segnalazione

L'intermediario finanziario ha svolto un eccellente lavoro di documentazione de- gli accertamenti condotti presso un altro intermediario finanziario (broker all'estero), dell'analisi blockchain (consegna di grafici), e dell'esame critico delle fonti utilizzate da uno dei suoi software di analisi. Su questa base MROS ha proceduto in particolare ad analisi complementari al fine di valutare l'opportunità di trasmettere informazioni a una FIU.

6. Riscontri tratti da alcune sentenze tra- smesse in virtù dell'art. 29a cpv. 1 LRD

Tratta di esseri umani e favoreggiamento della prostituzione

Nel 2021, MROS ha ricevuto diverse sentenze non collegate tra loro e riguardanti la tratta di esseri umani e il favoreggiamento della prostituzione. In questi casi, le vittime, esclusivamente donne e persone transgenere, provenivano sostanzialmente da due regioni: l'Europa orientale e la Thailandia. In entrambi i casi, gli autori e le vittime provenivano dallo stesso Paese. A livello delle organizzazioni che esercitano la tratta di esseri umani, i casi riguardanti le vittime dell'Europa orientale e le vittime thailandesi presentavano alcuni punti in comune, ma anche notevoli differenze nell'organizzazione e nel metodo seguito dagli autori.

Le seguenti considerazioni si riferiscono alle caratteristiche relative alle vittime della tratta di esseri umani provenienti dalla Thailandia:

Le strutture organizzative scoperte nel corso dei procedimenti facevano riferimento a due «organizzazioni», la prima in Thailandia e la seconda in Svizzera. Tanto in Thailandia quanto in Svizzera, gli autori erano soprattutto di sesso femminile. Alcune intermediarie reclutavano le vittime in Thailandia. Queste ultime sapevano che avrebbero dovuto lavorare come prostitute, ma erano state informate soltanto sommariamente in merito agli aspetti finanziari e alle modalità di rimborso dei debiti (spese di intermediazione, viaggio e sussistenza). Le vittime sono entrate in Svizzera con i visti procurati loro anticipatamente dalle intermediarie. Spesso venivano registrate come titolari prestante di una ditta per facilitare l'ottenimento di un visto turistico per lo spazio Schengen. In parte, tramite l'«organizzazione» svizzera, sono stati procurati loro anche passaporti falsificati dell'Unione europea, per consentire loro di ottenere un permesso L per dimoranti temporanei in Svizzera.

Una volta giunte in Svizzera, le vittime venivano accolte da altre intermediarie di sesso femminile e portate nei postriboli assegnati. Dall'arrivo in Svizzera, le vittime erano costantemente accompagnate o sorvegliate, e quindi isolate socialmente. Le vittime che entravano con un passaporto falsificato venivano accompagnate anche durante il disbrigo delle formalità burocratiche (richiesta del visto ecc.), e, talvolta, le autrici le attendevano davanti agli uffici delle autorità.

Per le spese di intermediazione e di viaggio le vittime dovevano rimborsare alle intermediarie una somma compresa tra 40 000 e 60 000 franchi. A questo debito venivano man mano ad aggiungersi nuove spese di vitto e alloggio. Dalle sentenze emerge che i profitti realizzati dalle vittime venivano divisi a metà: il 50 per cento veniva destinato al rimborso delle spese di intermediazione e di viaggio, mentre l'altro 50 per cento era la partecipazione versata alla donna che gestiva il postribolo. Le vittime venivano dunque depredate di tutti i profitti. Le transazioni venivano effettuate dalle donne che gestivano i postriboli o dalle intermediarie. Le vittime capivano ben presto che semmai fosse stato versato qualcosa per sostenere le loro famiglie in patria sarebbe stato soltanto una minima parte dei loro profitti. Nonostante le cattive condizioni, il controllo sulle vittime era essenzialmente esercitato, oltre che con intimidazioni, anche per via del fatto che le loro interlocutrici erano spesso donne più anziane. Secondo le considerazioni espresse nelle sentenze, il rispetto per gli anziani, profondamente radicato nella cultura thailandese, spingeva le vittime all'assoluta obbedienza nei confronti di queste donne.

Per l'analisi del comportamento assunto nelle transazioni tramite relazioni d'affari con intermediari finanziari svizzeri ci si è basati esclusivamente sulle sentenze trasmesse, poiché nei casi analizzati, MROS non aveva ricevuto alcuna comunicazione di sospetto.

Dalle sentenze analizzate emergono gli elementi seguenti:

- le vittime non disponevano di conti propri presso le banche; le relazioni d'affari erano intestate alle autrici;
- secondo la documentazione KYC, le autrici non operavano negli ambienti a luci rosse;
- in genere le autrici che effettuavano i versamenti erano molto più anziane delle vittime;
- le somme versate sui conti intestati alle autrici erano comprese tra 60 000 e 140 000 franchi annui;
- i versamenti su questi conti erano effettuati da terzi;
- il denaro versato veniva trasferito in Thailandia a vari intermediari per il pagamento delle spese di intermediazione;
- da questi conti venivano in parte versati mediante trasferimento bancario anche importi modesti a familiari delle vittime;
- altre transazioni, destinate sia agli intermediari sia ai familiari delle vittime, venivano effettuate tramite fornitori di servizi di pagamento anziché tramite bonifici bancari

7. Abklärungspflichten (KYC)

Fattispecie

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

Fattispecie

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

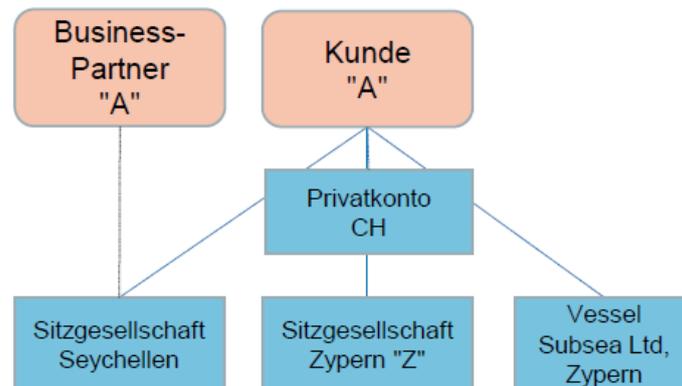
9. Umgang mit komplexen Strukturen

Fattispecie

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 "Steuroptimierung" 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)

Fattispecie

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