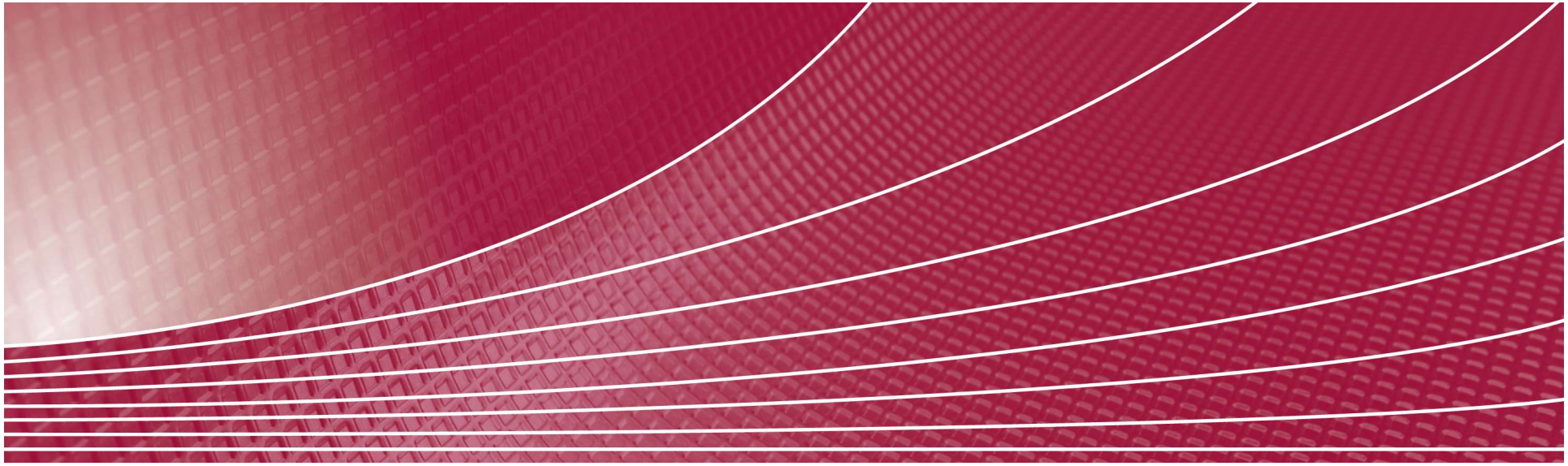
FMA

Finanzmarktaufsicht
Liechtenstein

Feedbackschreiben Sorgfaltspflichten Vor-Ort-Prüfungen 2023 «CASP-Sektor»

Finanzmarktaufsicht Liechtenstein, Vaduz, 05. April 2024



Inhalt

FMA
Finanzmarktaufsicht
Liechtenstein

A. Einführung
B. Feststellung und Überprüfung der Identität des VP/WB
C. Risikobewertung
D. Geschäftsprofile (SoF/ SoW)
E. Risikoadäquate Überwachung der Geschäftsbeziehung
F. Travel Rule
G. Fazit

A. Einführung

FMA
Finanzmarktaufsicht
Liechtenstein

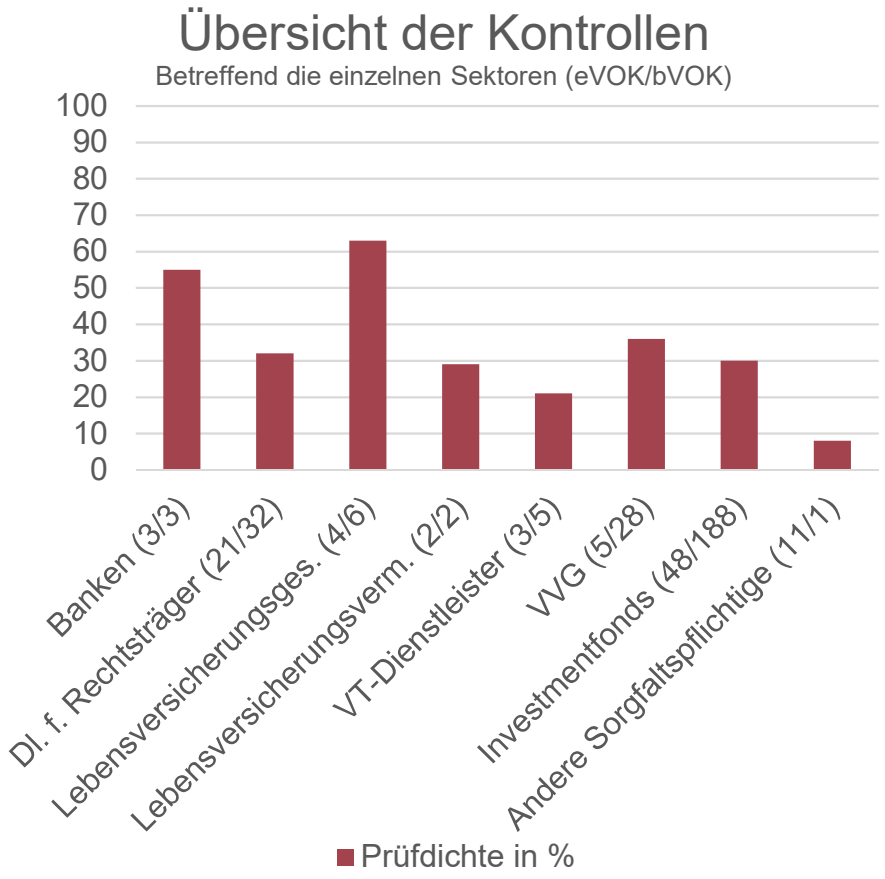
Das Feedbackschreiben soll einen Überblick über die letztjährige Prüfrunde betreffend die Wahrnehmung der Sorgfaltspflichten geben. Gesamthaft wurden 97 Sorgfaltspflichtige einer eigenständigen Vor-Ort-Kontrolle der FMA unterzogen und bei 263 Finanzintermediären wurde eine Prüfung durch einen Wirtschaftsprüfer beauftragt.

Das Feedbackschreiben beinhaltet insbesondere Erkenntnisse betreffend dir Aufbau- und Ablauforganisation, dir Risikobewertungen, der Anwendung der Sorgfaltspflichten, insbesondere der Umsetzung bei Kunden, welche einem erhöhten Risiko zugeordnet sind, den Prozessen betreffend Verdachtsmitteilungen und der Überprüfungshandlungen und Meldepflichten im Zusammenhang mit restriktiven Massnahmen. Sofern aus Sicht der FMA notwendig werden «good and bad practices» mittels Fallbeispielen näher erläutert, sodass die Erwartungshaltung der FMA und gute Marktstandards besser nachvollzogen werden können.

Neue Finanzintermediäre wurden einer Vollprüfung unterzogen, während bereits in den Vorjahren geprüft Finanzintermediäre einer Schwerpunktprüfung unterzogen wurden. Schwerpunkte im CASP-Sektor lagen auf der Risikobewertung, dem Geschäftsprofil und der Feststellung und Überprüfung der wirtschaftlich berechtigten Person. Bei der Durchführung eigenständiger Vor-Ort-Kontrollen wurde darüber hinaus unter anderem die risikoadäquate Überwachung inkl. Transaktionsüberwachung der Geschäftsbeziehung als weiterer individueller Schwerpunkt in der Prüfung gesetzt.

Bei sämtlichen Prüfungen wurde die effektive Wahrnehmung mittels mehrerer Stichprobenprüfungen untersucht.

Überblick der geprüften Finanzintermediäre im Jahr 2023



B. Feststellung und Überprüfung der Identität des VP/WB

Im CASP-Sektor erfolgt die Feststellung und Überprüfung der Identität des Vertragspartners bzw. der wirtschaftlich berechtigten Person fast ausschliesslich ohne persönlichen Kontakt. Unter Berücksichtigung diverser Sicherungsmassnahmen erfolgt demzufolge das Onboarding in der Regel mittels Video- oder Remoteidentifikation.

Zu den anzuwendenden Sicherungsmassnahmen gehören gemäss FMA-Wegleitung 2019/7 neben der Prüfung der verwendeten Identifikationsdokumente und den in Art. 6 Abs. 1 SPV genannten Daten zur Überprüfung der Identität des Vertragspartners, die Dokumentation der im Rahmen der Identifikation erstellten Dokumente und Aufzeichnungen sowie die Einholung von Informationen welche für die Anwendung von weiteren Sorgfaltspflichten (Geschäftsprofil, Risikobewertung risikoadäquate Überwachung) benötigt werden.

Grundlegend werden für die Video- und Remoteidentifikation Anwendungen von marktbekannten Service Providern genutzt. Diese erfüllen in der Regel die Anforderungen der genannten FMA-Wegleitung. In einem Einzelfall konnte jedoch nach wie vor ein Onboarding mittels gefälschtem Ausweis in der Kontrolle festgestellt werden.

Im Hinblick auf die Vorgaben der FMA-Wegleitung 2019/7 darf zudem auf die kürzlich veröffentlichte Änderungen (Inkrafttreten am 6. Mai 2024) hingewiesen werden.

Good Practice

Noch vor einigen Jahren wurden im Rahmen von Sorgfaltspflichtkontrollen die Aufnahme der Geschäftsbeziehung ohne persönlichen Kontakt mittels nicht erlaubter Identifikationsdokumente festgestellt. Diese Thematik wurde von den Sorgfaltspflichtigen aufgegriffen, indem die Einstellungen der einzelnen Identifikationstools individuell an den Risikoappetit der Sorgfaltspflichtigen und die vor allem an die sorgfaltspflichtrechtlichen Anforderungen angepasst wurde..

Bad Practice

Nicht in allen Fällen konnte im Rahmen der Kontrolle die Dokumentation der im Rahmen der Identifikation erstellten Dokumente und Aufzeichnungen mit allen Sicherungsmassnahmen vorgezeigt werden. Diesbezüglich sollte sichergestellt werden, dass die Service Provider entsprechende Bestätigungen ausstellen und diese auch im Einzelfall bei der Dokumentation des Kunden abgegriffen und verfügbar gemacht werden können.

C. Risikobewertung

FMA
Finanzmarktaufsicht
Liechtenstein

Mit dem Business Risk Assessment haben die Sorgfaltspflichtigen die für sie bestehenden Risiken in Bezug auf Geldwäscherei und Terrorismusfinanzierung zu ermitteln und zu bewerten.

Mit der Risikobewertung auf Kundenebene soll jede Geschäftsbeziehung einem Risiko zugeordnet werden. Im CASP-Sektor ist diesbezüglich zu beachten, dass grundsätzlich keine vereinfachten Sorgfaltspflichten zur Anwendung gelangen.

Die Risikoklassifizierung im CASP-Sektor erfolgt in der Praxis je nach Sorgfaltspflichtigen auf andere Art und Weise. Einige haben die Risikobewertung im Onboarding Tool integriert und andere dafür ein separates Template erstellt.

Grundlegend kann jedoch festgehalten werden, dass die Vorgaben der FMA-Wegleitung 2018/7 in Ziff. 4 des Kapitel II VT-Dienstleister und weitere Sorgfaltspflichtige mit Bezug zu VT-Dienstleistungen weitestgehend umgesetzt sind.

Die durchgeführten Kontrollen zeigten auf, dass grundsätzlich jede Geschäftsbeziehung einem Risiko zugeordnet wurde. In wenigen Ausnahmefällen wurde die Geschäftsbeziehung einem falschen Risiko zugeordnet.

Zudem wurde im Rahmen einer Kontrolle festgestellt, dass die Geschäftsbeziehungen wohl einem Risiko zugeordnet wurden, jedoch die Risikobewertung selbst nicht dokumentiert war bzw. nicht nachzuvollziehen war.

Good Practice

Alle kontrollierten CASPs verfügten über ein Business Risk Assessment. Nur bei einem Einzelfall musste das Business Risk Assessment angepasst werden, da es die bestehenden Risiken in Bezug auf Geldwäscherei und Terrorismusfinanzierung nicht adäquat adressierte.

Bad Practice

Der Risikobewertung auf Kundenebene sind oftmals Länderlisten hinterlegt. Bei einigen Kontrollen wurde festgestellt, dass diese nicht unmittelbar aktualisiert wurden bzw. die Risikobewertungen anschliessend nicht angepasst wurden.

Einige Sorgfaltspflichtige haben jede Geschäftsbeziehung wohl einem Risiko zugeordnet, allerdings war nicht in allen Fällen dokumentiert, wie diese Risikobewertung zu Stande kam.

D. Geschäftsprofile (SoF/ SoW)

FMA
Finanzmarktaufsicht Liechtenstein

Das Geschäftsprofil hat grundsätzlich folgendes zu enthalten:

Vertragspartner und wirtschaftlich berechtigte Person; Bevollmächtigte und Organe, die gegenüber dem Sorgfaltspflichtigen handeln; Herkunft der eingebrachten Vermögenswerte, wirtschaftlicher Hintergrund des Gesamtvermögens, einschliesslich Beruf und Geschäftstätigkeit des effektiven Einbringers der Vermögenswerte sowie den Verwendungszweck der Vermögenswerte.

Im CASP-Sektor hat das Geschäftsprofil zudem den VT-Identifikator (Public Key) zu enthalten.

Da im CASP-Sektor das Onboarding fast ausschliesslich ohne persönliche Kontakt erfolgt, stammen auch die meisten Informationen zum Geschäftsprofil direkt vom Kunden. Deshalb ist es für den Sorgfaltspflichtigen unverzichtbar die diesbezüglich gemachten Angaben des Kunden zu plausibilisieren (Sind diese Grundsätzlich stimmig?).

Bei manchen Geschäftsprofilen konnte festgestellt werden, dass diese nicht anlassbezogen aktualisiert wurden. In dem Zusammenhang war besonders auffällig, dass im Rahmen der Überprüfungshandlungen des Kundenverhaltens oder von Transaktionen (einfache Abklärungen) neue Kenntnisse gewonnen wurden, welche schlussendlich nicht in einer Aktualisierung des Geschäftsprofils mündeten.

Good Practice

Bei allen durchgeführten Kontrollen wurde zu jeder Geschäftsbeziehung ein Geschäftsprofil erstellt, welches in den meisten Fällen über den Mindestinhalt verfügte. Darüber hinaus war bei einigen Intermediären feststellbar, dass die Angaben im Geschäftsprofil im hohen und erhöhten Risiko durchgehend mittels Drittbelegen überprüft und plausibilisiert wurden. Auch in Fällen, in welchen keine verstärkten Sorgfaltspflichten angewendet wurden, erfolgten Überprüfungshandlungen der getätigten Kundenangaben mittels Drittbelegen.

Bad Practice

Bei einigen Geschäftsprofilen waren die Angaben im Geschäftsprofil in sich nicht stimmig. Wären diese zuvor vom Sorgfaltspflichtigen plausibilisiert worden, wäre dies aufgefallen.

In einzelnen Fällen von Geschäftsbeziehungen mit verstärkten Sorgfaltspflichten waren die Angaben im Geschäftsprofil zu generisch.

E. Risikoadäquate Überwachung der Geschäftsbeziehung

Die risikoadäquate Überwachung der Geschäftsbeziehung umfasst im CASP-Sektor unter anderem die Nutzung eines Blockchainanalysetools, den Abgleich der Transaktionen mit dem Geschäftsprofil des Kunden, die Nutzung eines Transaktionanalysesystems sowie die Durchführung von regelmässigen PEP-, Sanktions- und Medienchecks .

Mit der Nutzung eines Blockchainanalysetools können die CASPs vorab eingehende Token überprüfen. Es kann diesbezüglich festgehalten werden, dass bei allen im 2023 kontrollierten CASPs ein entsprechendes Tool zur Anwendung gelangt.

Durch den Abgleich von Transaktionen mit dem Geschäftsprofil, soll sichergestellt werden, dass keine Transaktionen getätigt werden, welche den im Geschäftsprofil enthaltenen Angaben widersprechen oder nicht plausibel sind. Dieser Abgleich erfolgt oftmals erst ab einem gewissen Schwellenwert.

Viele CASPs verwenden zudem ein Transaktionsanalysesystem welches sogenannte «Red flags» zu ungewöhnlichen Transaktionen hinsichtlich Geldwäscherei oder Terrorismusfinanzierung etc., hinterlegt hat. Wird eine der hinterlegten «Red flags» verletzt, wird eine Meldung generiert.

Technische Screeningmassnahmen im Zusammenhang mit Transaktionsszenarien und Transaktionsattributen konnten im Rahmen der Prüfungen darüber hinaus nicht nachgewiesen werden.

Die PEP-, Sanktions- und Medienchecks erfolgen grundsätzlich mittels entsprechender elektronischer Tools. Im CASP-Sektor werden die PEP-Checks und Medienrecherchen in der Regel häufiger als vorgeschrieben durchgeführt. Bezüglich der Überprüfung von internationalen Sanktionen ist festzuhalten, dass diese jeweils unmittelbar nach Erlass oder Änderung einer Zwangsmassnahme zu erfolgen hat.

Good Practice

Jeder kontrollierte CASP verwendet sowohl ein Blockchainanalyse-tool als auch ein System zur Identifikation von politisch exponierten Personen. PEP-Checks werden fast ausnahmslos rechtzeitig über den gesamten Kundenstamm durchgeführt und sind dokumentiert.

Positiv zu werten ist, dass bei einem Grossteil der Intermediäre zu den eingegangenen Token Blockchainanalysen mit entsprechender Bewertung vorliegen.

Das Transaktionsanalysesystem ermöglicht es aus der grossen Anzahl von Transaktionen diejenigen Transaktionen, welche verdächtig erscheinen, durch einen Compliance Mitarbeiter prüfen zu lassen.

Bad Practice

Grössere Mängel wurden hinsichtlich des Abgleichs von Transaktionen mit dem Geschäftsprofil festgestellt. Der Abgleich wurde oftmals nicht entsprechend dokumentiert bzw. erfolgte nicht in adäquater Art und Weise.

Der Abgleich kann sowohl automatisiert oder auch händisch erfolgen, ist aber in jedem Fall zu dokumentieren. In Fällen in denen die Transaktion nicht dem Geschäftsprofil entspricht, sind entsprechende Abklärungen vorzunehmen.

F. Travel Rule

Im Rahmen der eigenständigen Vor-Ort-Kontrollen wurden in den Prüfrunden 2022 und 2023 auch die Implementierung der Travel Rule überprüft. Die Travel Rule für Kryptodienstleistungen sieht den Informationsaustausch mit der Gegenpartei des Kryptowertetransfer betreffend den Auftraggeber- und Begünstigtendaten vor. Sofern keine Gegenpartei vorhanden sind, sind weiterführende Massnahmen wie beispielsweise ein Proof of Ownership zu treffen.

Grundlegend hatte der Grossteil der Sorgfaltspflichtigen Systeme zur Umsetzung der Travel Rule implementiert. Dabei wurde in der Regel auf Tools von externen Service-Provider zurückgegriffen. Nur ein Kryptodienstleister hatte sich noch nicht um eine Umsetzung bemüht.

Die Umsetzungen entsprachen teils den Anforderungen der FMA-Wegleitung 2021/18, teils wurden diese Anforderungen nicht entsprechend in der Kontrolle nachgewiesen.

Im Hinblick auf den Informationsaustausch wurde bei fast allen Transfers festgestellt, dass die Gegenparteien sich noch nicht zurückgemeldet hatten, sodass der Sorgfaltspflichtige bis anhin den Austausch nicht abschliessen konnte. Dies ist im Zusammenhang mit der globalen Implementierung kritisch zu sehen.

Auffällig war, dass teilweise zwar Systeme implementiert wurden, entsprechende Daten zu den Transfers eingeholt wurden, diese jedoch nicht mit den weiteren Systemen des Sorgfaltspflichtigen verknüpft wurden und somit keine Datenplausibilisierung und Sanctions- oder PEP-Screening durchgeführt werden konnte.

Auffällig war auch, dass teilweise bei ein- oder ausgehenden Transaktionen im Zusammenhang mit sogenannten «unhosted wallets» kein «Proof of Ownership» durchgeführt wurde.

Good Practice

Bei einer Prüfung wurden die entsprechenden Nachweise über die Plausibilisierung und das Screening der Informationen sowie die Übermittlung der Informationen an die Gegenpartei bei einem ausgehenden Transfer sowie die Informationen über den «Proof of Ownership» im Zusammenhang mit dem eingehenden Transfer von einem «unhosted wallet» nachgewiesen. Zum Informationsaustausch mit der Gegenpartei erfolgten keine Rückmeldungen seitens der Gegenpartei, obwohl diesbezüglich auch weitere Nachfragen zur Bestätigung der Richtigkeit der Informationen gestellt wurden. Im Zusammenhang mit dem «Sunrise-Issue» ist der Sorgfaltspflichtigen diesbezüglich kein Vorwurf im Handeln nachweisbar.

Bad Practice

Im Rahmen einer Kontrolle wurde zwar bei wenigen Transfers ein Informationsaustausch festgestellt. Beim Grossteil der Transfers der geprüften Stichproben konnten jedoch keine Nachweise über die Einholung, Plausibilisierung oder Screening der Informationen sowie dem Informationsaustausch selbst im Rahmen der Kontrolle nachgewiesen werden. Diesbezüglich ist seitens der Intermediäre sicherzustellen, dass sämtliche Kryptowertetransfers im Einklang mit den Bestimmungen zur Travel Rule durchgeführt werden.

Empfehlung

Darüber hinaus empfiehlt sich auch eine frühzeitige Auseinandersetzung mit den euriopäischen Vorgaben zur Umsetzung der Travel Rule (Transfer of Funds Regulation, ToFR, VO (EU) 2023/1113; sowie weiterführende EBA-Guidelines), welche im Februar 2025 in Liechtenstein zur Anwendung gelangen.

G. Fazit

Zusammengefasst kann festgehalten werden, dass sich der CASP-Sektor über die vergangenen Jahre stetig weiterentwickelt hat und mittlerweile über ein solides Abwehrdispositiv hinsichtlich AML/CTF verfügt. Allerdings ist weiterhin Verbesserungspotential vorhanden und die Weiterentwicklung bestehender Tools und Systeme ist in der Zukunft unerlässlich.

Grundsätzlich war eine wesentliche Verbesserung im Zusammenhang mit der Identifikation des Vertragspartners und der wirtschaftlich berechtigten Person ohne persönlichen Kontakt feststellbar, sodass diese nunmehr grossteils im Einklang mit den gesetzlichen Vorgaben durchgeführt wird.

Alle CASPs verfügten über ein eigenes Business Risk Assessment und jede Geschäftsbeziehung wurde einem Risiko zugeordnet.

Die Plausibilisierung der Angaben im Geschäftsprofil erfolgt wenn notwendig, mit wenigen Ausnahmen mittels adäquaten Drittbelegen.

Die Nutzung von Transaktionsanalysesystemen erlaubt die Durchführung einer hohen Anzahl von Transaktionen, indem eine manuelle Bearbeitung durch die 2nd line of defence auf verhältnismässig wenige Transaktionen eingeschränkt werden kann.

Jeder kontrollierte CASP verwendet sowohl ein adäquates Blockchainanalysetool als auch ein System zur Identifikation von politisch exponierten Personen sowie zum Sanktionsscreening.

Die hinterlegten Länderlisten werden oftmals nicht unmittelbar aktualisiert und dementsprechend die Risikobewertungen nicht direkt angepasst.

Die Risikobewertung wurde nicht in allen Fällen nachvollziehbar dokumentiert.

Die Geschäftsprofilinformationen wurden in einigen Fällen nicht plausibilisiert. Dies obwohl diese im CASP-Sektor direkt aus dem Onboarding ohne persönlichen Kontakt stammen und somit direkt vom Kunden eingetragen werden.

Erlangt der Sorgfaltspflichtige neue Informationen aus einem Austausch mit dem Kunden, so sind diese Informationen in das Geschäftsprofil aufzunehmen. Dies war nicht immer der Fall.

Grössere Mängel wurden hinsichtlich des Abgleichs von Transaktionen mit dem Geschäftsprofil festgestellt. Der Abgleich wurde oftmals nicht entsprechend dokumentiert bzw. erfolgte nicht adäquater Art und Weise.

Die Weiterentwicklung der Transaktionsanalysesysteme, insbesondere auf Szenarioanalysen und das Erkennen wesentlicher Transaktionsattribute ist unabdingbar um verdächtigte Transaktionen eigenständig erkennen zu können.