Per Email (PDF und Word) an:
isabel.grueninger@finma.ch

Eidgenössische Finanzmarktaufsicht FINMA
Laupenstrasse 27
CH-3003 Bern

Zürich, 25. Januar 2021

Teilrevision FINMA-Rundschreiben 2016/7 Video- und Online-Identifizierung – Stellungnahme SFTI

Sehr geehrte Frau Grüninger

Wir beziehen uns auf die Mitteilung der FINMA vom 16. November 2020, mit welchem die Vernehmlassung zur Teilrevision des Rundschreibens 2016/7 Video- und Online-Identifizierung betreffend die Sorgfaltspflichten bei der Aufnahme von Geschäftsbeziehungen über digitale Kanäle eröffnet wurde. Gerne nehmen wir diese Gelegenheit zur Stellungnahme wahr, nachdem wir uns bereits im Rahmen der Vorkonsultation geäussert haben.

Der Verband Swiss Fintech Innovations (SFTI, www.swissfintechinnovations.ch) vertritt die Interessen seiner Mitglieder (vorab Banken und Versicherungen) im Bereich der Digitalisierung und Innovation in der Finanzindustrie. Die Arbeitsgruppe „Regulations" beschäftigt sich mit Gesetzgebung und Regulation rund um Innovation und Digitalisierung in der Finanzindustrie. Die Unter-Arbeitsgruppe „Auto-Identifikation" fokussiert dabei auf digitale Onboarding-Prozesse.

1. **SFTI begrüsst** die Anpassung des Rundschreibens an neue technologische Möglichkeiten.

2. Die Technologie entwickelt sich jedoch rasch weiter, weshalb SFTI einen **kürzeren Aktualisierungszyklus** für das vorliegende Rundschreiben begrüssen würde. Dies würde auch ermöglichen, die Entwicklungen ausländischer Regularien und damit mögliche Vorteile der Mitbewerber im Ausland rasch zu kompensieren.

3. Ausserdem gehen die vorgeschlagenen Anpassungen deutlich zu wenig weit. Es braucht weitere Alternativen, um die gegebenen **technologischen Möglichkeiten auszuschöpfen** und mit **ausländischer Konkurrenz mithalten** zu können. Solche Schritte wären ohne Einbussen bei der Sicherheit und Qualität von Onboardings möglich.

Konkret fordert SFTI folgende Alternativen für digitale Kunden-Onboardings:

4. Die Variante **Auto-Identifizierung,** bei welcher nicht ein Mensch sondern ein Software-basiertes System durch den Identifikationsprozess führt, **soll der persönlichen Vorsprache gleichgestellt werden**, wie dies auch im Europäischen Umfeld der Fall ist (vgl. Ziff. 2)

5. Bei der Variante der **Online-Identifizierung** soll auf das **Erfordernis der Geldüberweisung und ihre Alternativen (wie Chip-Scan) verzichtet** werden, weil der in Rz 32 verlangte Lichtbildabgleich in Verbindung mit der nach Rz 34 verlangten Wohnsitzadresseüberprüfung für eine sichere Identifizierung genügend sind (vgl. Ziff. 3).

6. Eventualiter, d.h. für den Fall, dass nicht auf zusätzliche Erfordernisse verzichtet werder können soll, muss bei der vorgeschlagenen **Chip-Scan** im Rahmen einer Online-Identifizierung auf eine **Prüfung der Signatur des Chips mittels staatlichen Zertifikaten verzichtet** werden können, um eine – wenigstens teilweise – praxistaugliche Variante zu bilden (vgl. Ziff. 4).

7. Ebenfalls in Zusammenhang mit einer Online-Identifizierung soll schliesslich als Alternative zur Überprüfung der Wohnsitzadresse eine **Geolokalisation** zugelassen werden (vgl. Ziff. 5).

1 Grundsatz: Beibehaltung Sicherheitsniveau

Regeln für digitale Lösungen sollen ermöglicht werden, solange das gesetzlich geforderte Sicherheitsniveau sichergestellt ist. Dabei ist zu beachten, dass die Regeln für digitale Lösungen nicht deshalb viel höheren Ansprüchen als ihr analoges Pendant genügen müssen, nur weil dies theoretisch (technisch) möglich wäre. **Das Gebot der Gleichbehandlung muss immer auch zwischen und unter den analogen und digitalen Lösungen gelten.**

Dieser Grundsatz ist beim vorliegend zur Diskussion stehenden Rundschreiben besonders wichtig, denn technische Verfahren ermöglichen teilweise sehr viel genauere und tiefere Analysen als beispielsweise eine persönliche Vorsprache. Dieser Tatsache ist Rechnung zu tragen, indem nicht jede theoretisch mögliche Sicherheitsmassnahme auch zwingend vorzuschreiben ist. Beispielhaft kann hier die Tatsache angeführt werden, dass bei einer persönlichen Vorsprache keine Archivierungen (Gesprächsaufzeichnungen, Fotos etc.) erforderlich sind.

In diesem Zusammenhang sollte insbesondere die immer wieder vorgebrachte Argumentation, wonach „[G]erade im digitalen Umfeld […] aufgrund des fehlenden persönlichen Kontakts und dem Wegfall der Anreise die Hemmschwelle für Missbrauchsversuche herabgesetzt“ (Erläuterungsbericht S. 6) sei, überdacht und zumindest mit vergleichendem Zahlenmaterial analysiert werden. Ein Hinweis auf „Rückmeldungen von Finanzintermediären in der Aufsicht“ und „jährlich Dutzende[…] von Verdachtsmeldungen an die Meldestelle für Geldwäscherei MROS aufgrund des Einsatzes von gefälschten oder falschen Ausweisen im Bereich des digitalen Onboarding“ (Erläuterungsbericht S. 6) genügen für sich alleine als Begründung zusätzlicher, den Einsatz neuer Technologien erschwerender Hürden unseres Erachtens jedenfalls nicht. Vielmehr müssten gerade die Meldungen an die MROS den entsprechenden Meldungen gegenübergestellt werden, welche ebenfalls aufgrund des Einsatzes von gefälschten oder falschen Ausweisen bzw. Identitäten, aber in Zusammenhang mit klassischem Onboarding eingehen.

2 Auto-Identifizierung der persönlichen Vorsprache gleichgestellt

2.1 Technisch möglich

Die heutigen Systeme zur Identifizierung von Vertragsparteien führen automatisch durch den Identifikationsprozess. Der Prozess ist dabei nahezu identisch ausgestaltet wie bei einer „klassischen" Video-Identifikation gemäss geltendem Rundschreiben. Im Unterschied zu diesem führt bei einer Auto-Identifizierung aber nicht ein Mensch, sondern ein Software-basiertes System automatisch durch den Identifizierungsprozess und nimmt die folgenden Prüfungen vor:

- Die Übereinstimmung der übermittelten Daten mit den Informationen aus der MRZ und der VIZ des Identifizierungsdokuments der Vertragspartei.
- Übereinstimmung der Vertragspartei in der Videosequenz mit dem Lichtbild auf dem Identifizierungsdokument der Vertragspartei.
- Die Echtheit des Identifizierungsdokuments durch maschinelle Überprüfung von mindestens zwei Sicherheitsmerkmalen.
- Die Lebendigkeit der Vertragspartei der Videosequenz, insbesondere die Echtheit der Videosequenz und die persönliche Präsenz der Vertragspartei im Zeitpunkt der Aufnahme der Videosequenz, um eine gefälschte oder manipulierte Videosequenz erkennen zu können.

Jeder Identifizierungsvorgang wird vom System revisionstauglich aufgezeichnet und die Aufzeichnungen können zu den Akten genommen und archiviert werden.

2.2 Keine Einbussen bei Sicherheit und Qualität

Diese Systeme sind heute bereits so weit entwickelt, dass die Qualität der Identifikation mindestens ebenso gut, wenn nicht besser ist als die Qualität einer Video-Identifikation unter menschlicher Beteiligung, welche das Rundschreiben (auch in Zukunft) in Rz. 6-9 vorschreiben will.

Die verschiedenen Algorithmen zur Gesichtserkennung und zur Lebendigkeitsprüfung stehen in ständigem Wettbewerb, werden regelmässig von unabhängigen Stellen überprüft und aufgrund neuer Erkenntnisse von den Herstellern weiterentwickelt. Es haben sich hohe Branchenstandards entwickelt für Test- und Zertifizierungsverfahren (vgl. FVRT 1:1 VERIFICATION, FVRT MORPH, aber auch NIST- und ISO Standards (30107-3)). Auf diese Weise haben sich die eingesetzten Technologien in den letzten zwei Jahren enorm weiterentwickelt und werden sich auch in Zukunft weiterhin verbessern.

Die Vorteile für Kunden und Finanzintermediäre liegen auf der Hand: Die Kunden sind nicht gezwungen, sich via Video einer fremden Person zu präsentieren. Und die Finanzintermediäre müssen kein teures 7/24-h-Callcenter für ein digitales Onboarding betreiben. Gleichzeitig sind weder in Bezug auf die (Daten-) Sicherheit noch die Qualität der Identifikationen Einbussen zu befürchten, im Gegenteil.

2.3 eIDAS-Verordnung

Im europäischen Raum ist die eIDAS (Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische

Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG) massgebend für die elektronische Identifizierung. Neben der persönlichen Vorsprache sind dort drei weitere Verfahren zulässig, darunter auch «[…] sonstige Identifizierungsmethoden, die auf nationaler Ebene anerkannt sind und gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten[…]» (vgl. Artikel 24, Abs. 1, lit. d eIDAS). Diese Gleichwertigkeit wird durch eine «Konformitätsbewertungsstelle» festgestellt. Im Bereich der Geldwäscherei verweist die Richtlinie (EU) 2018/843 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU in Artikel 13 explizit auf die eIDAS.

Damit lässt die europäische Regelung Raum für weitere Verfahren, die Bewertung der Sicherheit bzw. Äquivalenz ist an die Fachstellen delegiert. Beispielsweise hat die spanische Servicio Ejecutivo de la Comisión de Prevenicón de Blanqueo de Capitales e Infracciones Monetarias SEPBLAC ein Identifikationsverfahren basierend auf einer live Videosequenz ohne direkte Beteiligung einer Person seitens des Finanzintermediärs zugelassen. Weitere EU-Mitgliedstaaten haben diese Entwicklung bereits aufgegriffen.

2.4 Fazit

Auto-Identifizierungsverfahren müssen in der Schweiz ebenfalls der persönlichen Vorsprache gleichgestellt werden. Wenn sich Schweizer Finanzintermediäre dieser Entwicklung nicht anschliessen können, hat dies einen deutlichen Wettbewerbsnachteil zur Folge.

3 Online-Identifizierung ohne Banküberweisung oder Alternativen dazu

Bei der Online-Identifizierung in der Variante „die Elektronische Ausweiskopie mit Echtheitsprüfung durch den Finanzintermediär“ soll auf das **Erfordernis der Geldüberweisung und ihre Alternativen (wie Chip-Scan) verzichtet** werden, weil der in Rz 32 verlangte Lichtbildabgleich in Verbindung mit der nach Rz 34 verlangten Wohnsitzadressüberprüfung für eine sichere Identifizierung absolut genügend sind.

Die geforderte Banküberweisung führt – je nach Geschäftsmodell – beispielsweise zum Problem, dass der (künftigen) Vertragspartei die Konto-/IBAN-Nummer bekannt gegeben werden muss, noch bevor die Identifikation vollständig durchgeführt bzw. abgeschlossen ist. Ab Bekanntgabe der Konto-/IBAN-Nummer lassen sich eingehende Vermögenswerte im Zahlungsverkehr jedoch nicht mehr ohne Weiteres stoppen. Zur Verhinderung unerwünschter Vermögenseingänge und im Sinne des Standards einer vollständigen Identifikation vor Kontoeröffnung sollten Alternativen zu dieser Vorgabe zugelassen werden.

Der Finanzplatz Schweiz darf nicht durch unnötige Anforderungen an die Online-Identifizierung einen Wettbewerbsnachteil erleiden, indem eine rasche Instant-Kontoeröffnung, wie sie in der digitalisierten Welt benötigt wird, verhindert wird.

4 Eventualiter: Chipscan ohne Zertifikatsprüfung

Eventualiter, d.h. für den Fall, dass nicht auf zusätzliche Erfordernisse verzichtet werden können soll (vgl. Ziff. 3 vorstehend), muss bei dem vorgeschlagenen **Chip-Scan** im Rahmen einer Online-Identifizierung auf eine **Prüfung der Signatur des Chips mittels staatlichen Zertifikaten verzichtet** werden können, um eine – wenigstens teilweise – praxistaugliche Variante zu bilden. Dazu was folgt:

Als Alternative zur Banküberweisung wird nun ein **Chipscan** vorgeschlagen, was SFTI grundsätzlich begrüsst. Allerdings wird verlangt, dass jeweils nicht nur ein Abgleich der Daten (Foto, Name etc.) auf dem Chip mit jenen auf dem erstellten Lichtbild der Vertragspartei stattfindet, sondern zusätzlich auch die Signatur des Chips geprüft wird, wofür die Zertifikate der jeweiligen Herausgeberländer benötigt werden (vgl. Erläuterungsbericht S. 8). Letzteres stellt eine zusätzliche Hürde dar, die weit über die Möglichkeiten und Anforderungen bei einem analogen Onboarding hinausgehen, was abzulehnen ist (vgl. oben Ziff. 1).

Der Chip ist zudem auf vielen Identifikationsdokumenten noch nicht enthalten, so beispielsweise auf der Schweizer ID. Gerade im wenig risikoreichen Schweizer Retail Segment sind Identitätskarten sehr beliebt und häufig eingesetzt. Zudem sind Pass und NFC-fähige Gerätegenerationen auch aus Kostengründen noch nicht standardmässig anzutreffen.

Weil es sich bei dieser Voraussetzung „lediglich“ um eine Zusatzsicherung (ohne entsprechendes Pendant im analogen Bereich, was an sich bereits abzulehnen wäre [vgl. Ziff. 1]) handelt, welche allfällige Mängel der automatischen Gesichtserkennung kompensieren soll, darf die Hürde nicht hoch angesetzt werden.

Aus diesem Grund soll **auf eine Prüfung der Signatur eines Chip mittels staatlichen Zertifikaten verzichtet** werden können (vgl. oben).

5 Geolokalisation zur Plausibilisierung der Adressangaben

SFTI unterstützt das Ziel, mit der Online-Identifikation einen vollautomatischen und dennoch sicheren Eröffnungsprozess zu ermöglichen. Dies wäre theoretisch bereits unter dem geltenden Rundschreiben möglich, wie die FINMA im Erläuterungsbericht S. 5 festhält. In der Praxis hingegen ist das nicht der Fall. Und auch die Einführung der Alternative eines Chip-Scans, welcher die Banküberweisung ersetzen kann, wird daran leider nicht viel (jedenfalls nicht genügend) verändern (vgl. oben Ziff. 3).

So unterbricht auch die Überprüfung der Wohnsitzadresse mittels *Utility Bill* den heutigen Online-Identifikationsprozess, da die entsprechenden Dokumente durch im automatisierten Prozess nicht zuverlässig als Rechnung erkannt werden und Datenbanken für zugelassene *Utility Bill*-Aussteller nach unserer Kenntnis (noch?) nicht zugänglich sind, weshalb auch diesbezüglich ein automatischer Abgleich noch nicht möglich ist. Ohnehin ist die Echtheit einer elektronisch übermittelten *Utility Bill* kaum gewährleistet bzw. überprüfbar, weder durch Menschen noch durch IT-gestützte Hilfsmittel. Es bleibt im Hinblick auf eine Vollautomation nur die Anbindung an ein öffentliches Register oder ein durch einen vertrauenswürdigen Privaten geführte Datenbank mit den entsprechenden datenschutzrechtlichen Herausforderungen.

Um einen vollautomatisierten, sicheren Eröffnungsprozess praxistauglich auszugestalten, ist deshalb eine Alternative notwendig. **Die technischen Möglichkeiten ermöglichen heute, Informationen zum Aufenthaltsort über eine Geolokalisierung zu ermitteln. Diese sollen anstelle der Überprüfung der Wohnsitzadresse gemäss geltendem Rundschreiben zur Plausibilisierung der Angaben der Interessenten zu Aufenthalts- oder Wohnort hinzugezogen werden können. Dabei sollte genügen, dass der lokalisierte Ort mit der angegebenen Adresse übereinstimmt, da die Geolokalisierung in praxi betreffend Strasse und Hausnummer zu unpräzise ist.**

6 Keine handschriftliche Unterschriften für Feststellung wB

Gerne nimmt SFTI zur Kenntnis, dass bei der digitalen Feststellung des wirtschaftlich Berechtigten für alle Finanzintermediäre gilt, dass die Unterschrift des Vertragspartners nicht handschriftlich vorliegen muss (Erläuterungsbericht S. 6). **Somit ist im Rahmen der digitalen Onboarding weder eine Unterschrift des künftigen Kunden noch eine Unterschrift des wirtschaftlich Berechtigten notwendig.**

Wir bitten Sie höflich um eine wohlwollende Prüfung unserer Anträge und stehen für Rückfragen oder eine Diskussion jederzeit gerne zur Verfügung.

Freundliche Grüsse

Sig. Werner W. Wyss
Leiter der AG Regulations

Sig. Frank Kilchenmann
Leiter der Sub-AG Auto-Identifizierung

Sig. Prof. Dr. Cornelia Stengel
Mitglied der AG Regulations