Autorità federale di vigilanza sui mercati finanziari FINMA
Isabel Grüninger
Laupenstrasse 27
CH-3003 Berna

isabel.grueninger@finma.ch

Lugano, 24 marzo 2018

Presa di posizione sul progetto di Circolare FINMA 16/7

Gentile Signora Grüninger

Come previsto con comunicazione del 13 febbraio 2018, ci permettiamo di inoltrare la presente presa di posizione di BitIncubator & Ventures SA (di seguito BIV) e Eidoo Sagl (di seguito Eidoo, entrambe indicate come le Società) alla al progetto di Circolare FINMA 16/7.

1. Generalità sulle società e interessate alla consultazione

La scopo di BIV è quello di operare nel settore Fintech commerciando e cambiando criptovalute o token sia in biglietti di banca che in divise che in altre criptovalute o token. La società è attiva nel settore della consulenza di criptovalute e blockchain. La società potrà sviluppare, commercializzare e distribuire programmi informatici, siti web, applicazioni in genere nel settore Fintech e Blockchain. La creazione e la gestione di punti di vendita per criptovalute e merce di ogni genere relativi allo scopo sociale. La fornitura di servizi di pubblicità, di marketing e di networking. BIV è attualmente assoggettata all'OAD VQF per i suoi obblighi di riciclaggio di denaro, ma intende inoltrare una richiesta di autorizzazione a questa lodevole autorità quale borsa e/o Multilateral trading Facility. La società gestisce attualmente l'exchanger in criptovalute www.bitmax.ch.

Eidoo è una società attiva nello sviluppo, vendita, licenza di software; produzione, sviluppo, marketing e vendita di programmi informatici e applicazioni nei settori Blockchain e Ethereum; creazione di app mobile, pubblicazioni digitali e applicazioni web; sviluppo e vendita di token. La società può detenere brevetti, licenze e altri diritti immateriali. Eidoo ho completato una ICO per finanziare le sue attività e già oggi offre ai suoi utenti un wallet di criptovalute, mentre a breve è atteso il lancio di un exchanger

BitIncubator & Venture SA
Via Motta 10
6830 Chiasso CH

Email: info@bitmax.ch
Web: https://www.bitmax.ch

Eidoo Sagl
Via Motta 10
6830 Chiasso CH

Email: info@eidoo.io
web: https://eidoo.io

decentralizzato. Trovate maggior informazioni sul sito www.eidoo.io. Eidoo è attualmente in procinto di ottenere l'autorizzazione in ambito di lotta al riciclaggio di denaro presso l'OAD VQF.

Le Società gestiscono il sito www.icoengine.net, che viene utilizzato per l'identificazione online di persone che intendono partecipare alle ICO tramite il wallet Eidoo o il portale bitmax. Benché conformemente alle linee guida della FINMA sulle ICO queste attività non risultano soggette alla legge sul riciclaggio di denaro in caso di utility token, le società richiedono a tutti i partecipanti una verifica KYC, che nella maggioranza dei casi sarà chiesta seguendo i dettami della Circolare FINMA sull'identificazione online. Le Società in questo modo stanno raccogliendo esperienza per quando l'attività di identificazione online sarà svolta per le attività obbligatoriamente soggette alle normative sul riciclaggio di denaro.

Le Società ha pertanto un interesse a partecipare alla consultazione essendo la loro attività direttamente collegate alle norme legali in discussione.

2. Presa di posizione

2.1. In generale

Le Società sostengono il progetto in consultazione e la volontà di FINMA di sviluppare le attività tecnofinanziarie. In questa fase di globale incertezza sulle nuove tecnologie digitali, in particolare sulle criptovalute, è importante fornire agli attori del ambiente legislativo stabile, chiaro, aperto e soprattutto accessibile, eliminando barriere d'entrata che possano essere di ostacolo allo sviluppo della tecnofinanza. Il progetto normativo segue questi principi e deve pertanto essere salutato con favore.

Ciononostante, le Società ritengono che sussistano alcuni punti che debbano essere maggiormente chiariti al fine di assicurare delle regole chiare per tutti i partecipanti al mercato e la salvaguardia degli interessi degli utenti del servizio di tecnofinanza, nonché la reputazione della piazza finanziaria svizzera.

Di seguito ci permettiamo di elencare quelli che a nostro avviso sono i punti che del progetto che richiedono una precisazione o una nuova regola. In considerazione del fatto che le Società non sono attive nell'ambito della video identificazione, solo le regole sull'identificazione online saranno oggetto della presa di posizione.

2.2. Possibilità di delegare le verifiche

L'identificazione online è un elemento indispensabile dell'attività tecnofinanziaria. I servizi nell'era digitale si rivolgono al mondo e attualmente, almeno per quanto riguarda l'ambito blockchain i numeri di clienti acquisiti tramite identificazione online è molto importante. Risulta pertanto importante per le imprese poter garantire un controllo dei dati forniti dai clienti in modo rapido ed economicamente sostenibile. È pertanto molto probabile che la parte più operativa e meno specializzata dei controlli

venga delegata a società terze. La cifra 31.1 del progetto di Circolare prevede che "l'identificazione online sia affidata a collaboratori dell'intermediario finanziario appositamente formati a tale scopo". Le Società convengono con questa disposizione, tuttavia ritengono necessaria la possibilità di delegare le funzioni operative quali il confronto dei documenti raccolti a terzi o la verifica dei criteri ottici, nel rispetto dei dettami della Circolare FINMA 18/3 sull'outsourcing. Ad oggi infatti le maggiori società specializzate nella fornitura di sistemi di identificazione dei sistemi ottici come pure di riconoscimento faciale sono estere e svolgono solo questo servizio. Un intermediario finanziario avrà difficoltà a competere con queste strutture e i costi per implementare un servizio di identificazione dei sistemi ottici sono molto importanti. Anche il semplice confronto dei documenti forniti è un'attività che potrebbe richiedere un notevole numero di persone e che deve poter essere delegata a terzi, sempre sotto la responsabilità dell'intermediario finanziario. In questo modo, l'intermediario finanziario sarà sempre responsabile del corretto svolgimento dell'identificazione online, ma potrà delegare a società più specializzate le attività più tecniche o con più mole di lavoro, mantenendo comunque la responsabilità per il corretto funzionamento del sistema di identificazione online. Si ritiene pertanto opportuno apportare la seguente modifica.

Cifra 31.1

Nell'identificazione online, la qualità dell'immagine deve essere adeguata al fine di permettere un'identificazione inconfutabile. L'intermediario finanziario può impiegare supporti tecnici per compensare condizioni di illuminazione difficili. L'identificazione online è affidata a collaboratori dell'intermediario finanziario appositamente formati a tale scopo. Le attività tecniche quali la verifica dei sistemi ottici o il confronto dei documenti d'identificazione con i riferimenti che figurano nella banca dati dei documenti può essere delegato a terzi.

2.3. Machine Readable Zone e caratteri non latini

Ai sensi della cifra marginale 32, con il supporto di strumenti tecnici idonei che permettono per lo meno la lettura e la decifratura delle informazioni contenute nella MRZ, l'intermediario finanziario verifica che le informazioni decifrate coincidano con gli altri dati riportati sul documento d'identità e con le informazioni fornite dalla controparte al momento dell'avvio della relazione d'affari. Tuttavia, vi sono diverse Stati che non usano caratteri latini nei documenti di identità, bensì caratteri cirillici o ideogrammi asiatici, che la maggior parte delle MRZ non sono in grado di leggere.

Fino a quando la tecnologia non permetterà di ovviare a questo problema l'identificazione online potrebbe essere limitata ai soli paesi con passaporti con caratteri latini, fatto questo che si scontra contro l'elemento globale della FinTech. Come per la video identificazione dunque, la verifica della MRZ dovrebbe essere complementare con quella svolta dai sistemi ottici, mentre la verifica della conformità dei dati riportati dall'utente con quelli riportati nel documento di identità dovrebbero poter essere svolti anche manualmente (dunque non soltanto tra dati riportati dall'utente e dati ripresi dalla MRZ, ma pure tra dati riportati dall'utente e dati verificati dall'intermediario finanziario sul documento di identità, con tre elementi di sicurezza verificati).

BitIncubator & Venture SA
Via Motta 10
6830 Chiasso CH

Email: info@bitmax.ch
Web: https://www.bitmax.ch

Eidoo Sagl
Via Motta 10
6830 Chiasso CH

Email: info@eidoo.io
web: https://eidoo.io

Si propone pertanto di modificare la cifra marginale 32 come segue.

L'intermediario finanziario chiede alla controparte di consegnargli le fotografie di tutte le pagine rilevanti del proprio documento d'identificazione e altre fotografie in cui è ritratta. Verifica che la fotografia scattata della controparte corrisponda alla fotografia che figura sul documento d'identificazione e confronta il documento d'identificazione con i riferimenti che figurano in una banca dati di documenti d'identità per quanto riguarda gli elementi di sicurezza, il tipo e la dimensione dei caratteri e la struttura grafica. L'intermediario finanziario verifica i) con il supporto di strumenti tecnici idonei che permettono per lo meno la lettura e la decifratura delle informazioni contenute nella MRZ, ~~l'intermediario finanziario verifica~~ che le informazioni decifrate coincidano con gli altri dati riportati sul documento ~~d'identità~~ d'identificazione e con le informazioni fornite dalla controparte al momento dell'avvio della relazione d'affari, oppure ii) manualmente tenendo traccia dei controlli svolti, che le informazioni riportate sul documento d'identificazione coincidano con gli altri dati riportati sul documento. L'intermediario finanziario valuta in ogni caso l'autenticità del documento d'identificazione per mezzo di almeno tre elementi di sicurezza ottici selezionati casualmente, se possono essere esaminati su un fotogramma. Inoltre, l'intermediario finanziario garantisce che la fotografia della controparte è stata scattata nel quadro della procedura di identificazione, per esempio mediante riconoscimento interattivo *(selfie with liveness detection)*.

* * *

Restiamo a vostra disposizione per ogni ulteriore domanda che dovreste avere nel corso dell'evasione della nostra richiesta.

In attesa di un vostro riscontro l'occasione ci è grata per porgervi i nostri cordiali saluti.

BitIncubator & Ventures SA **Eidoo Sagl**

BitIncubator & Venture SA
Via Motta 10
6830 Chiasso CH

Email: info@bitmax.ch
Web: https://www.bitmax.ch

Eidoo Sagl
Via Motta 10
6830 Chiasso CH

Email: info@eidoo.io
web: https://eidoo.io

Autorité fédérale de surveillance des
marchés financiers (FINMA)
A l'attention de Madame
Isabel Grüninger
Laupenstrasse 27
3003 Berne

Neuchâtel, le 28 mars 2018

Objet : Audition de la FINMA – Révision partielle de la circulaire 2016/7 « Identification par vidéo et en ligne »

Madame,

Par communiqué de presse du 13 février 2018, l'Autorité fédérale de surveillance des marchés financiers (FINMA) a indiqué qu'elle menait une audition sur la révision partielle de sa circulaire sur l'identification par vidéo et en ligne (Circulaire 2016/7).

Bity SA est un intermédiaire financier, affiliée à l'Association d'assurance-qualité pour les prestations de services financières (VQF), qui est un organisme d'autorégulation reconnu par la FINMA. A ce titre, Bity SA est directement concernée par la révision de la circulaire mentionnée sous objet, qu'elle applique pour l'établissement de relations d'affaires.

Dans ce contexte, je vous fait part de ma position sur le projet de révision : à mon sens, le chiffre 31.1 du projet de circulaire 2016/7 (version française) devrait être reformulé comme suit :

> *« Lors de la vérification d'identité en ligne, la qualité de l'image doit être appropriée pour permettre une identification parfaite. L'intermédiaire financier peut utiliser des moyens techniques pour compenser des conditions de luminosité difficiles. ~~L'identité est vérifiée en ligne par des collaborateurs de l'intermédiaire financier ayant suivi une formation correspondante.~~ La vérification de l'identité en ligne doit être effectuée par des collaborateurs de l'intermédiaire financier ayant suivi une formation correspondante. »*

En effet, cette reformulation serait moins ambiguë, dans la mesure où l'accent serait mis sur les qualités que doivent avoir les personnes qui effectuent des vérifications (collaborateur de l'intermédiaire financier au bénéfice d'une formation). Cette proposition serait également plus fidèle à la version allemande du projet de circulaire 2016/7.

Tout en vous souhaitant bonne réception de la présente, je vous prie d'agréer, Madame, l'expression de mes sentiments distingués.

Bity SA

Alexis Roussel
Adm. Président

DecentAge AG
Albisriederstrasse 199
8047 Zürich

Eidgenössische Finanzmarktaufsicht FINMA
Frau Isabel Grüninger
Laupenstrasse 27
CH-3003 Bern

Zürich, 28. März 2018

Anhörung zur Teilrevision des FINMA-Rundschreibens 2016/7 "Video- und Online-Identifizierung"

Sehr geehrte Frau Grüninger

Bezugnehmend auf die am 13. Februar 2018 eröffnete Anhörung bezüglich Teilrevision des FINMA-Rundschreibens 2016/7 "Video- und Online-Identifizierung" ("FINMA-RS 2016/7") möchten wir mit Ihnen unsere Ansichten mitteilen. Wir bedanken uns für die Möglichkeit einer Stellungnahme.

DecentAge ist ein Startup im Gebiet von neuen offenen und dezentralisierten Softwarearchitekturen wie der Blockchain und erbringt Dienstleistungen in den Bereichen Regulierungsvorhaben, Compliance, Softwareentwicklung sowie Projektmanagement. Die Firma verfolgt rund um die Thematik der digitalen Identifizierung von Vertragsparteien folgende Interesse: Einerseits bietet sie in Zusammenarbeit mit fidentity GmbH (nachfolgend „Partner“ genannt) eine Schnittstelle für die Kundenidentifikation mittels Online-Identifizierung für Drittparteien an. Die Kunden sind hauptsächlich in der Schweiz und in Liechtenstein domizilierte Firmen, welche meist ein dezentrales Ökosystem aufbauen und dafür mittels Initial Coin Offering (ICO) ein Crowdfunding betreiben. Andererseits ist DecentAge bestrebt, der Blockchain-Gesellschaft langlebige Innovationen bereitzustellen und die Brücke zur traditionellen Finanzbranche zu schlagen.

Unsere Stellungnahme bezieht sich auf das Verfahren der Online-Identifizierung, dabei wird auf die Thematik im Kontext von ICOs detailliert eingegangen. Das Eröffnen eines Bankkontos ist für Blockchain-Firmen momentan ein Stolperstein. Die oberste politische Führung und die Regulatoren sind offen gegenüber neuen innovativen Technologien und die damit verbundenen Prozesse. Sowohl Finanzminister Ueli Maurer wie auch

Wirtschaftsminister Johann Schneider-Ammann haben sich der Thematik persönlich angenommen. So äusserte Schneider-Ammann Mitte Januar die Hoffnung, dass die Schweiz zur Krypto-Nation werde.

Im Gegensatz dazu zeigt sich der Bankensektor als sehr konservativ und verhindert damit eine breite Massenadoption der Technologie, indem sie keine Dienstleistungen wie Kapitaleinzahlungskonten für Startups anbieten, welche Services im Zusammenhang von ICOs anbieten. Die macht eine Alternative zum Erfordernis der Geldüberweisung ab einem Bankkonto nötig. Ansonsten besteht das Risiko, dass die politischen Bemühungen ohne Wirkung bleiben, weil es der Schweiz in der rasanten Entwicklung von Blockchain-Lösungen nicht gelingt, Beziehungen zwischen den traditionellen Banken und Firmen aus dem digitalen Finanzbereich herzustellen.

Damit eine Kunden-Identifizierung für ICOs mit der Online-Identifizierung weiter an Attraktivität gewinnt, regen wir für Token-Zeichnungen unter einem bestimmten Schwellwert eine Erleichterung an. Wir schlagen vor, dass als Alternative zum Erfordernis der Geldüberweisung ab einem Bankkonto stattdessen **eine Verknüpfung des Blockchain-Wallets mittels digitaler Signatur an die Online-Kundenidentifikation gebunden wird.** Die Überweisung des Zeichnungsbetrages in Kryptowährung und die im Rahmen des ICOs geschaffenen Token werden ausschliesslich über die identifizierte Wallet-Adresse durchgeführt.

Im Anhang wird ein möglicher Identifikationsprozess schematisch dargelegt. Aus diesem Diagramm ist ersichtlich, dass sich eine Vertragspartei mit ihrem eigenen Blockchain-Wallet verbindet. Das ist wichtig, denn die Vertragspartei muss im Besitz des privaten Schlüssels (engl. Private Key) sein, ansonsten kann sie die Transaktion nicht signieren. Die Signierung der Email- mit der Wallet-Adresse ist der Kernpunkt einer sicheren Einbindung vom Partner in den Identifikationsprozess.

Mit der Übergabe einer kryptographischen Hashfunktion an den Partner wird verhindert, dass jemand den Identifikationsprozess überlistet und damit ohne Identifizierung an einem ICO teilnehmen kann. DecentAge speichert die Email- und Wallet-Adresse sowie die Signatur der vorgenannten Parameter auf einem Identifikations-Server ab. Die Antwort des Partners wird mit den Daten aus der eigenen Datenbank verglichen. Stimmen diese überein, wird der Vertragspartner für die Teilnahme am ICO zugelassen und die Wallet-Adresse erhält eine sogenannte KYC Bestätigung, welche in der Blockchain unwiderruflich und unveränderbar gespeichert wird.

Dies eröffnet neue Möglichkeiten und eine effiziente Identifikation von Blockchain-Wallets, ohne Kundendaten abzuspeichern.

Wir sind der Überzeugung, dass mit der Verknüpfung von Blockchain-basierten Wallets eine rechtskonforme Kundenidentifikation gemacht werden kann und diese eine Gleichwertigkeit zum Kriterium der Banküberweisung darstellt.

Besten Dank für die Prüfung unser Anliegen. Gerne stehen wir für eine weitergehende Erläuterung unserer Sichtweise zur Verfügung.

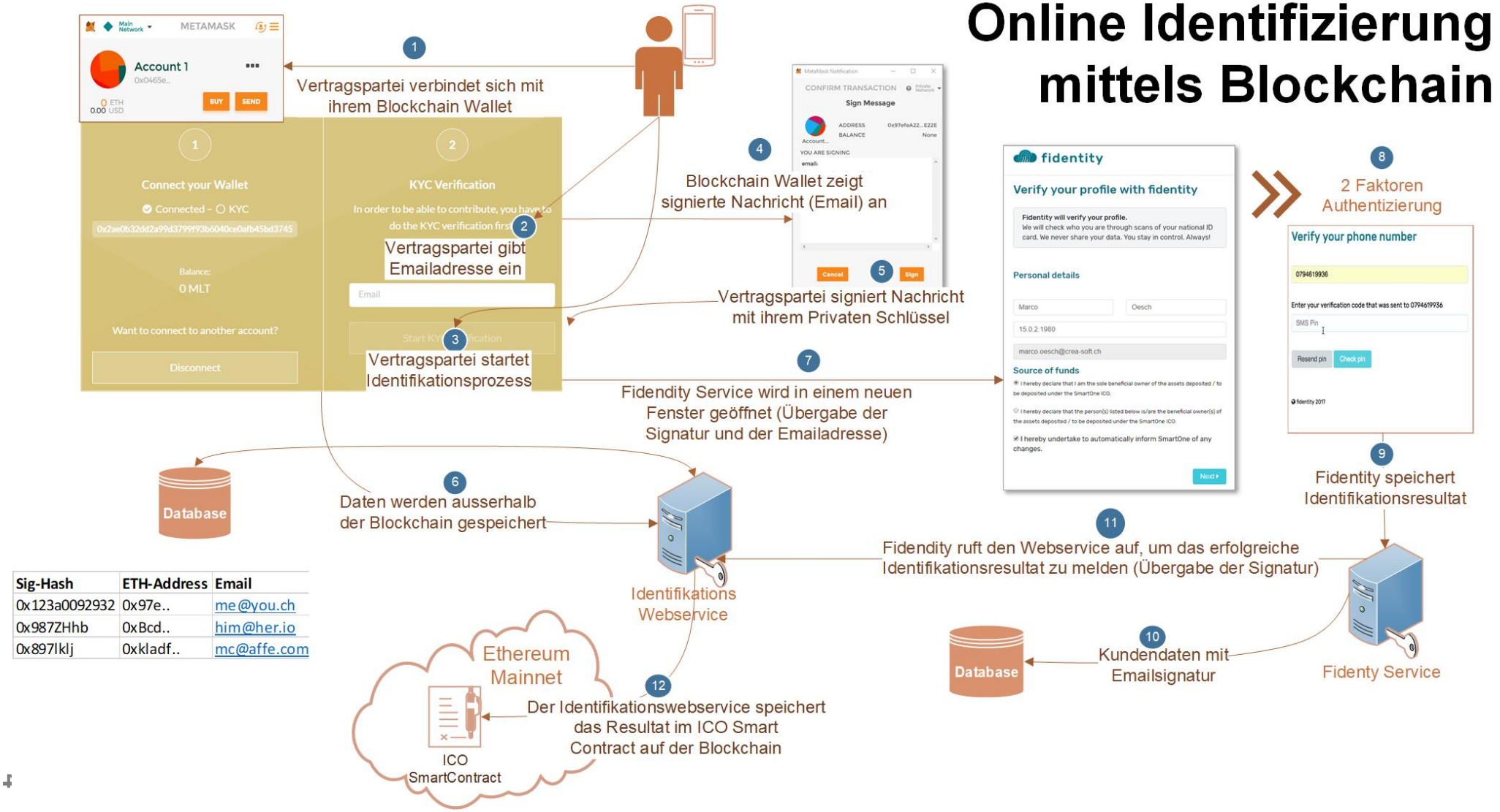
Freundliche Grüsse

DecentAge AG

Patrick Salm
Mitglied des Verwaltungsrates

Marco Oesch
Mitglied des Verwaltungsrates

Anhang



Sig-Hash	ETH-Address	Email
0x123a0092932	0x97e..	me@you.ch
0x987ZHhb	0xBcd..	him@her.io
0x897lklj	0xkladf..	mc@affe.com

Weitere Informationen zum Online-Identifikationsprozess

Zusammen mit der Firma fidentity bietet DecentAge einen mehrstufigen Prozess zur Identifikation von natürlichen Personen an. Zuerst wird die Vertragspartei zur Selbstdeklaration aufgefordert (Adressdaten, Mittelherkunft usw.). Anschliessend tätigt die Vertragspartei Lichtbilder von allen relevanten Seiten ihres Identifizierungsdokuments, von sich selbst (sog. Selfie - beispielsweise mit einem Identifikationsdokument in der Hand als Lebendbeweis). Alle Dokumente werden hochgeladen und mit einer eindeutigen Identifikationsnummer versehen. Zum Schluss wird ein SMS-TAN an die Person versendet, um die Kontrolle über die Mobilnummer zu verifizieren.

Aus den Dokumenten werden die Text-Daten der MRZ (Maschinenlesbare Zone) ausgelesen und mit den vom Nutzer eingegebenen Daten abgeglichen sowie den restlichen Daten auf dem Identifikationsdokument verglichen. Das Selfie wird mit dem Bild auf dem ID Dokument abgeglichen. Dies geschieht mittels modernster Technologie. Nicht auswertbare Bilder werden manuell geprüft und die Ergebnisse werden entweder korrigiert oder als nicht identifizierbar gekennzeichnet. Das SMS TAN verfahren dient auch der Bestätigung der Erklärung über die wirtschaftliche Berechtigung.

Zusätzlich führt fidentity einen Abgleich mit übliche Registern für politisch exponierte Personen (PEP) und Sanktionslisten durch. fidentity ist in Kombination mit Verfahren zur Video Identifikation nutzbar. Hierbei können beispielsweise Investoren unterhalb eines Schwellenwertes mittels fidentity identifiziert werden. Zur Durchführung einer echtheitsbestätigten Identifikation für hohe Investitionsvolumen wird ein Video Verfahren wie der DIS Service von Swisscom verwendet. Eine Integration zwischen beiden Lösungen ist vorhanden.

DUKASCOPY
Swiss Forex Bank & Marketplace

Dukascopy Bank SA

International Center of Cointrin (ICC)
Route de Pré-Bois 20, CH-1215 Geneva 15

Tel: + 41 22 799 4888
Fax: + 41 22 799 4880

http: www.dukascopy.com

Autorité fédérale de surveillance
des marchés financiers FINMA
Att. Madame Isabel Grüninger
Laupenstrasse 27
3003 Berne

isabel.grueninger@finma.ch

Genève, le 28 mars 2018

Audition relative à la circulaire FINMA 2016/7 Identification vidéo et en ligne

Chère Madame Grüninger,

Nous nous référons à la procédure d'audition ouverte par la FINMA le 13 février 2018 concernant le projet de révision partielle de la circulaire susmentionnée (ci-après "la Circulaire").

Nous vous remercions de nous donner ainsi l'occasion d'exprimer notre avis sur un sujet particulièrement important pour notre établissement. En effet, depuis que la circulaire 2016/7 est entrée en vigueur, nous identifions environ 80% de nos clients via vidéo. Depuis 2016, nous avons ouvert environ 4'000 relations d'affaires via ce canal.

D'une manière générale, nous saluons les propositions de la FINMA allant dans le sens de l'élimination d'obstacles inutiles dans l'utilisation de canaux numériques pour établir des relations d'affaires. A cet égard, nous accueillons favorablement l'usage de l'identification-vidéo pour les clients à risque accru (ce qui évite la rupture de média) et de pouvoir accepter un premier virement depuis une banque sise hors de Suisse, dans le cadre de l'identification en ligne.

Dans le même temps, nous déplorons que, bien qu'elle s'en défende, la FINMA continue d'ériger des obstacles, que nous jugeons inutiles, dans l'usage des canaux numériques.

Concernant le TAN, nous entendons continuer à l'utiliser car celui-ci est aisé et s'intègre bien dans notre modèle d'affaire.

1- Analyse des risques

Le "Rapport explicatif de la FINMA sur la révision partielle de la Circ. FINMA 16/7" (ci-après "le Rapport") nous renseigne sur le fait que la FINMA justifie les contrôles d'authenticité qu'elle exige des intermédiaires financiers (ci-après les "IF") utilisant des canaux numériques par un risque accru de fraude causé par l'absence de "contact analogique" avec le document d'identité (ci-après "ID") et par l'absence de "contact personnel" avec le prospect, qui abaisseraient le "seuil d'inhibition en vue de l'utilisation de pièces d'identités fausses et falsifiées", pour reprendre exactement les termes du Rapport.

Selon notre propre analyse des risques, nous identifions effectivement un risque accru de fraude sur l'identité dans le cadre de l'identification en ligne (basée sur des copies électroniques d'ID). En effet, il est aisé de modifier des copies de documents d'identité à l'aide de logiciels courants. Par ailleurs, dans le cas de l'identification en ligne, l'IF ne voit généralement ni le prospect en vrai ni l'ID original durant l'ouverture du compte. Un service de la police fédérale à Berne nous a confirmé l'existence de ce risque en nous informant que des personnes étaient parvenues à obtenir des crédits à la consommation sous de fausses identités, grâce à des copies falsifiées d'ID.

Nous relevons que le risque de fraude est quasiment le même lorsque, dans le cadre d'une ouverture de compte par correspondance, l'IF identifie le client sur la base d'une copie d'ID certifiée conforme par un tiers car il est également très aisé de falsifier une telle certification. **Curieusement, il n'est pas requis des IF qu'ils vérifient l'authenticité de ces certifications alors que le risque qu'elles soient fausses est bien réel.** Il n'est pas non plus requis des tiers (notaires, etc.), certifiant la conformité à l'original des copies d'ID, qu'ils vérifient l'authenticité des ID originaux qui leur sont présentés. Nous doutons que, par exemple les notaires, utilisent un quelconque procédé pour vérifier l'authenticité des ID dont ils certifient les copies.

Il est également établi qu'un risque de fraude sur l'identité existe lorsqu'une personne se présente personnellement dans les locaux d'un IF avec son ID, par exemple dans une agence bancaire, pour ouvrir un compte. En effet, il est possible de se procurer des ID falsifiées de bonne qualité et de tromper l'employé de l'IF chargé de faire une copie de l'ID original pour ouvrir le compte. **La police cantonale de Genève nous a informés de cas de personnes séjournant en Suisse sans autorisation ayant utilisé de faux papiers d'identité dans le but de toucher leur salaire auprès de banques en Suisse. Nous relevons que lorsque le compte est ouvert en personne, auprès d'un bureau de l'IF, aucun contrôle particulier n'est exigé par la FINMA sur l'authenticité de l'ID alors que le risque de fraude existe. Ce risque concerne la majeure partie des relations d'affaires puisque la plupart d'entre elles sont établies de la sorte**.

Du point de vue des exigences de contrôles d'authenticité, la différence entre les canaux numériques et les autres est saisissante. Selon nous elle ne se justifie en tout cas pour l'identification-vidéo.

En effet, selon notre analyse et nos échanges avec des prestataires de services d'identification-vidéo, le risque de fraude dans l'identification-vidéo est infime, car le prospect doit montrer son visage et l'ID original face à une caméra au cours d'une cession vidéo dont il a été informé qu'elle serait enregistrée. Ceci semble avoir un effet dissuasif sur d'éventuels fraudeurs. L'identification-vidéo n'offre en effet aucun anonymat et permet de conserver des preuves (images et voix enregistrées) d'une tentative de fraude. Bien que l'IF ne puisse pas toucher le prospect, il le voit et l'entend en temps réel, parle avec lui, lui pose des questions et analyse sa manière de répondre. De notre point de vue, le processus d'identification-vidéo n'est pas "purement numérique" contrairement à ce que la FINMA indique dans son Rapport, un "contact personnel" existe bel et bien et ce contact renseigne beaucoup plus qu'une simple copie d'ID reçue dans le cas d'une identification en ligne. Par ailleurs, bien que l'IF ne puisse pas toucher l'ID, il peut demander au prospect de le montrer sous tous les angles, près de la caméra s'il le faut. Grâce à une bonne qualité d'image, l'examen de l'ID n'est pas entravé, sauf en ce qui concerne le toucher. Toutefois, il est peu plausible que le toucher constitue une aide déterminante pour détecter un ID falsifié.

Nous renvoyons au site Internet du prestataire eID qui présente une analyse proche de la nôtre concernant le risque de fraude dans l'identification-vidéo (voir annexe ou https://www.electronicid.eu/video-identification-vid-secure-face-face-identification/).

Pour compléter notre analyse, nous avons contacté les autorités de police fédérale et du Canton de Genève, les organisations faîtières des banques en Suisse, les principales firmes d'audit actives dans l'audit bancaire en Suisse, nos concurrents directs utilisant l'identification-vidéo afin de savoir s'ils avaient constaté des cas de fraude liés à l'identification-vidéo. Nos recherches n'ont mis en évidence aucun cas de fraude en Suisse lié à l'identification-vidéo.

Par conséquent, le renforcement des contrôles d'authenticité envisagés par la FINMA dans l'identification-vidéo ne semble pas nécessaire et nous prions la FINMA de bien vouloir y renoncer. Si la FINMA souhaite effectuer un sondage régulier auprès des établissements pratiquant l'identification-vidéo et l'identification en ligne, afin d'évaluer l'intérêt pour l'industrie financière et les risques y relatifs, nous participerons volontiers.

2- Compétitivité des banques en Suisse

Comme relevé par la FINMA dans son Rapport, les canaux digitaux sont appelés à jouer un rôle très important pour certains acteurs suisses particulièrement tournés vers l'international, donc très actifs dans les opérations transfrontières. Ceci est par exemple notre cas.

Dans cette optique, il est crucial que la Circulaire n'érige pas de nouveaux obstacles inutiles limitant l'applicabilité des canaux numériques pour une clientèle non domestique.

A cet égard, nous prenons l'exemple de l'identification en ligne pour laquelle la FINMA a initialement exigé un premier virement depuis une banque en Suisse. **A notre avis, cette seule restriction explique pourquoi l'identification en ligne ne s'est pas développée en Suisse**. En ce qui concerne notre établissement, depuis 2016, nous avons effectué tout au plus une trentaine d'identifications en ligne, parce que notre clientèle réside très majoritairement hors de Suisse.

Nous félicitons la FINMA de revenir sur sa position initiale et d'admettre qu'exiger un premier virement depuis une banque en Suisse était trop restrictif. Bien qu'elle aille dans la bonne direction, nous sommes d'avis que la nouvelle proposition de la FINMA incluant le Liechtenstein et certains pays du GAFI est à nouveau inutilement limitative et de surcroît compliquée à interpréter.

Nous jugerions adéquat que la FINMA formule un principe général que le premier dépôt doive provenir d'une banque d'un pays disposant d'une supervision et d'une règlementation anti-blanchiment adéquates et qu'elle laisse aux IF la responsabilité de déterminer eux-mêmes la liste des pays "adéquats". Considérer que seule la Suisse disposerait d'un dispositif approprié de lutte contre le blanchiment peut faire sourire. Nul doute que notre pays et ses régulateurs font partis des meilleurs du monde, toutefois, nous voulons croire que les pays sachant combattre le blanchiment d'argent sont plus nombreux que les membres du GAFI bien notés.

Selon notre compréhension, le renforcement des contrôles d'authenticité sur les ID voulus par la FINMA s'inspire principalement de l'exemple de la BaFin et des leaders allemands de services d'identification-vidéo. De notre point de vue, suivre l'exemple allemand est une mauvaise idée, pour la raison suivante.

Contrairement aux IF suisses, les IF allemands ont accès au marché de l'Union Européenne ("UE") qui est énorme. Les IF allemands peuvent se satisfaire de ce marché. Par contre, les IF suisses ne peuvent pas tous vivre grâce au seul marché suisse, ceci est une évidence. La technologie d'identification-vidéo qui s'est imposée en Allemagne est adaptée au marché européen dans le sens que les ID européens sont compatibles avec l'exigence de vérifier trois éléments de sécurité optique. La même exigence est incompatible avec nombre d'ID de pays non-européens avec lesquels, pourtant, beaucoup d'établissements suisses font des affaires. **Si cette nouvelle exigence était imposée, il ne serait plus possible d'utiliser l'identification-vidéo pour un nombre important de ressortissants étrangers et de types d'ID.** A titre d'illustration, les leaders allemands d'identification-vidéo peuvent contrôler des ID (principalement les passeports) de moins de 60 pays. Pour notre établissement ce n'est pas assez car nous avons des clients dans presque tous les pays du monde et parce qu'un nombre important de personnes n'ont simplement pas de passeport.

Les IF suisses n'ont pas accès au marché européen alors pourquoi entraver leur accès aux autres marchés? Soyons réalistes, l'UE n'est pas prête d'ouvrir son marché aux IF suisses et le peuple suisse n'est pas près de voter pour une adhésion à l'UE.

Dans ces conditions, il apparaît raisonnable de songer un instant aux intérêts nationaux suisses, en tant qu'Etat durablement non membre de l'UE. Sachant que la règlementation est un élément déterminant de la compétitivité des IF, nous prions la FINMA de ne pas nous imposer les règles allemandes, qui ont été élaborées dans et pour un autre environnement que le nôtre. Cela reviendrait à se tirer une balle dans le pied inutilement, sans aucune contrepartie.

3- "One size does not fit all"

Afin de voir si la volonté de la FINMA d'accroître les contrôles sur l'identification-vidéo s'inscrivait dans une tendance générale observée au plan international, nous avons comparé les règlementations relatives à l'identification-vidéo suisse, maltaise, liechtensteinoise, espagnole, autrichienne, singapouroise et allemande.

Cet exercice nous a permis de constater que de grandes différences existent entre les règles de ces pays et que les exigences allemandes sont les plus détaillées/strictes. Nous avons été aussi très satisfaits de constater que certains régulateurs donnent explicitement aux IF la responsabilité de choisir, dans un cadre minimal, les mesures de réduction du risque de fraude adaptées à leur situation spécifique lorsqu'ils utilisent des canaux digitaux pour ouvrir des relations d'affaire. Dans certains cas, le régulateur se contente de lister des mesures de réduction du risque à titre exemplatif, et non de manière exhaustive et limitative comme le font la FINMA et la BaFin. Donner de la flexibilité dans la gestion du risque s'inscrit dans l'idée que les IF sont responsables de gérer leurs risques.

Nous regrettons vivement que concernant l'utilisation des canaux digitaux, la FINMA se substitue aux instances de gestion des risques des IF en leur imposant un carcan détaillé de mesures de réduction du risque, dont certaines réclament de surcroît de recourir à des systèmes informatisés car leur exécution manuelle requerrait trop de ressources. Nous pensons en particulier à la nouvelle exigence voulue par la FINMA de comparer les éléments visuels (structure, éléments de sécurité optiques, police et taille des caractères) des ID avec une base de données. Un tel contrôle ne semble raisonnablement pas faisable sans l'aide d'intelligence artificielle.

Nous déplorons ce qui nous apparaît être une inclination de la FINMA à imposer toujours plus de contrôles automatisables dans l'usage des canaux numériques. Le seul fait qu'un contrôle puisse être automatisé ne rend pas un tel contrôle nécessaire. En outre, le rapport coût/bénéfice du contrôle doit être raisonnable.

Nous faisons remarquer que la FINMA pourrait aussi imposer, par exemple aux banques, d'utiliser certains systèmes pour vérifier l'authenticité des ID que les prospects leur présentent lorsqu'ils ouvrent un compte dans une agence. **Nous notons que la FINMA s'abstient de le faire et pourtant le risque de fraude existe.**

Comme souligné par la FINMA dans son Rapport, seule une minorité de relations d'affaire sont établies via des canaux numériques. **Pourtant cette minorité est soumise aux règles les plus strictes. Si l'objectif est de diminuer les cas de fraude, nous trouvons que la réglementation de la FINMA répartit l'effort de lutte contre la fraude de manière très inefficace car au lieu de viser la majorité des nouvelles relations elle se concentre sur une petite minorité**.

De notre point de vue, la Circulaire ignore aussi que la réalité des risques est très différente selon les activités et les clientèles. Par exemple, nous comprenons qu'il y ait un intérêt à obtenir un crédit sous une fausse identité. Par contre, nous ne voyons pas de raisons de tromper un IF pour ouvrir un compte sous une fausse identité lorsque l'IF exige du client que les fonds soient obligatoirement virés depuis un compte au nom du client et retirés vers un compte au nom du client, ce qui est notre politique. Notre politique réduit presque à néant le risque de fraude sur l'identité. Pourtant nous sommes soumis aux mêmes exigences de contrôles d'authenticité que les autres IF utilisant les canaux digitaux.

Nous souhaitons que la Circulaire permette une approche orientée-risque en introduisant une flexibilité concernant le choix des mesures de réduction du risque de fraude, sur la base d'une analyse des risques faite par l'IF. Nous pensons avoir démontré que la FINMA surévalue beaucoup les risques de fraude s'agissant de l'identification-vidéo. La FINMA devrait faire confiance aux IF pour évaluer et gérer leurs risques, à tout le moins aux IF soumis à sa supervision. Nous comprenons qu'en général, la FINMA est favorable à l'approche orientée-risque. Nous ne voyons pas pourquoi la Circulaire fait exception.

Pour ces raisons, nous espérons que la FINMA renoncera à imposer aux IF un contrôle obligatoire de la structure, des éléments de sécurité optique, de la taille et de la police des caractères des ID. Tout au plus, un tel contrôle pourrait être mentionné comme exemple de mesure jugée adéquate pour réduire le risque de fraude ou pour lever un doute. **En effet, d'autres mesures devraient être possibles comme par exemple demander au prospect de montrer, durant l'identification-vidéo, un deuxième ID**.

Dans certains pays, les cartes d'identité ou d'autres ID officiels tels que les permis de conduire ne comportent pas de MRZ. A notre avis, l'absence de MRZ ne devrait pas constituer un défaut rédhibitoire mais nécessiter, selon les circonstances, une mesure compensatoire de réduction du risque comme par exemple demander et examiner un deuxième ID ou obtenir un premier virement depuis un compte bancaire au nom du client. **Nous regrettons que la FINMA impose un train de mesures si détaillé pour gérer un risque si spécifique.** Nous ne connaissons pas d'équivalent dans la réglementation financière suisse. Nous ne sommes pas convaincus que la FINMA puisse mieux que les IF juger des mesures de réduction du risque adaptées à leur modèle d'affaire.

4- Pourquoi pareille hâte dans l'accroissement des contrôles? Quid de la neutralité technologique?

Nous pensons avoir démontré que concernant l'identification-vidéo, il n'est pas nécessaire d'accroître les contrôles d'authenticité des ID par rapport à ce qui existe déjà.

Dans ce contexte, nous espérons que la FINMA tienne également compte des investissements importants consentis par les quelques établissements suisses ayant développé leur propre technologie d'identification-vidéo afin de rester indépendants des prestataires de services d'identification-vidéo et de mieux maîtriser la confidentialité des données. Deux ans à peine après que la Circulaire ait été émise, nous avons peine à admettre qu'il faille à nouveau investir dans des développements technologiques encore plus complexes, alors que la nécessité de tels changements n'a pas été établie.

Enfin, nous souhaitons que la FINMA se garde d'émettre des prescriptions si détaillées inspirées de technologies disponibles sur le moment car cela revient à favoriser les fournisseurs de telles technologies dont les intérêts sont clairement en conflit avec les nôtres.

Nous restons volontiers à votre disposition pour tout renseignement complémentaire et pour discuter de ce sujet crucial pour notre établissement.

Nous vous prions d'agréer, Chère Madame Grüninger, nos salutations distinguées.

Dukascopy Bank SA

Laurent Bellières
CRO

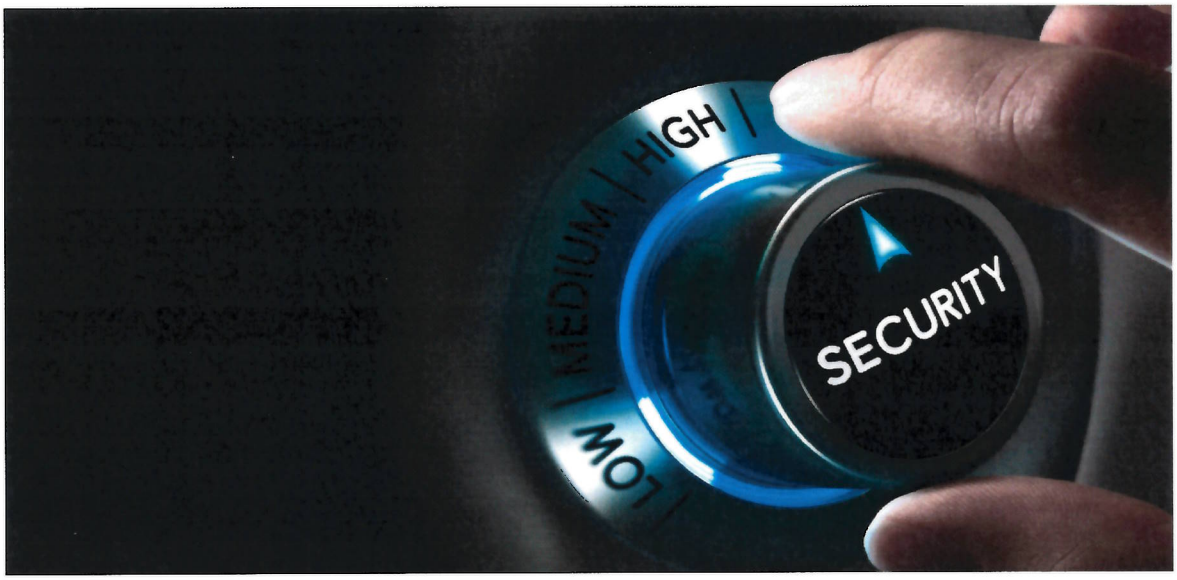
Veronika Duka
co-CEO-CAO

Annexe: mentionnée

https://www.electronicid.eu/video-identification-vid-secure-face-face-identification/

Video IDentification: Why is VID more secure than Face-to-Face IDentification?

by Patricia Diez | May 3, 2017 | Video IDentificacion | 0 comments



Video Identification

When businesses require trustable confirmation for the proper identification of people, those processes traditionally begin and end in an office to carry out face-to -face identification. Examples like: opening a bank account, contracting a mobile telephone operator, having dealings with government departments or even voting at a shareholders' meeting or in general elections.

Nowadays this is in the process of being digitalised. In the financial sector due to the new regulations against money laundering and financing terrorism (PBCFT) and will be appearing in other sectors shortly.

Accompanying any change of paradigm, is at times the tendency to give into scepticism or feelings of insecurity. However, we would do well to remember that electronic and digital identification afford greater control than traditional methods and in this field particularly. eID has been a pioneer in the world of video identification with leading technology VideoID. In this article, we would like to draw on our cutting edge experience, since our inception in 2013, to illustrate just how and why video identification is more secure than face-to face.

https://www.electronicid.eu/video-identification-vid-secure-face-face-identification/

First, the Video Technology.

VideoID lets you record a video in real time of the process of identification of the person during which he shows the front and back of his passport or ID document. Only when conditions are favorable is a high definition video recorded, with the process that allows one to clearly see the person, alive, without coercion, in great detail and full legibility and his identify document, with the video recorded and sealed electronically for its integrity, as well as the main data on the position and device of the client, such as his ip address and position recorded as main electronic evidence of the act of identification. This high quality video record, immutable in time, far exceeds the test evidence we currently have in face-to -face verification, which never goes beyond a mere photocopy of the ID document. The process of recording by video also has a deterrent effect on persons who want to commit fraud, as they have to step in front of a camera and record themselves in order to try and impersonate or supply phony ID's. Both these circumstances have meant that fraud cases using our video technology identification has been zero per cent up till now.

Second. Artificial Intelligence

The technology of Artificial Intelligence (IA) and specifically our algorithm IA for the verification of identity allows you to perform verifications during the process, in real time, where with a live bodily presence, the following verifications are not possible.

- Detects the version of the identity document and country of issue verify in real time that the document patterns and the security measures in the image are equivalent to the originals of the authentic source of identity.
- Permits verify that the front and back of the document belong to the same identidy card and that the integrity of its construction is intact, this being unattainable with a human presence as this requires a process that would take hours to calculate.
- Generates an automatic comparison and in real time of the biometric pattern of the person who it identifies and the image that contains the identidy document in the process. The biometric pattern is a unique and inequivocable mathematica model of each person.. This capacity of vision and calculation is also unattainable for the capacities of a human physically present.

It is the combination of the treatment in video and the application of the algorithms of IA in multiple images of the process of recording the video which is the only model that permits sufficient precision to improve security. There are, in the market, similar solutions that deal with isolated images of the document and of the person's face (selfies) that cannot reach the standard of precision or security given by solutions of video identification. Habitually, this type of solutions based on selfies or images are

being used very frequently for low risk processes but they have no equivalent to the security of ours and they are below face-to-face identification too.

Third, A specialised human team

In a financial entity, a telecommunications operator, asking for a Registration Authority from a Certification Authority there can be thousands of people who nowadays do a face-to-face identification and as a necessary process within another more general process which tends to be the contracting of a product or service. Normally, these people are not qualified to undertake the identification. Even with the automatic security methods explained in previous paragraphs, video identification in the regulars sectors, like in banks for money laundering, it is an indispensable requisite that a qualified human team ends up checking the identification process and the different tests, to be able to conclude that the person is who he says he is: this model changes from being decentralized and without qualification to being centralized and specialized, with the advantages that this confers. In our case, for example, we don't only look for a random identity verification to avoid possible fraud but we also keep the entire custody chain from the beginning until the verifying human agent who does the last checks and proofs.

Some data from the technology leader in video identification, Video ID:

- Identifications done up to now >100.000
- Precision current algorithm IA: 99,99%
- Precision OCR Data Extraction: 97,98%
- Precision Biometric Scoring: 94,76 %
- Availability Platform SaaS: 99,98%
- Identity Fraud Cases: 0
- Average time identification process by the client: 18 Segundos
- Record time for the identification process by the client: 9 Segundos
  If you would like to get to know the leading technology of Video IDentificación, contact us!

EXPERT suisse
Wirtschaftsprüfung
Steuern
Treuhand

E-Mail: Isabel.Grüninger@finma.ch
Eidgenössische Finanzmarktaufsicht FINMA
Isabel Grüninger
Laupenstrasse 27
3003 Bern

Zürich, 28. März 2018

Betreff: Anhörung Teilrevision FINMA-RS 2016/7 „Video- und Online-Identifizierung“

Sehr geehrte Frau Grüninger

Für die Zustellung der Unterlagen im Zusammenhang mit der eingangs erwähnten Anhörung danken wir Ihnen bestens. Die Kommission für Bankenprüfung von EXPERTsuisse hat die Anhörungsvorlage eingehend studiert.

Unsere Hinweise und Bemerkungen haben wir in der Beilage zusammengefasst.

Für Fragen stehen Ihnen die Unterzeichnenden gerne zur Verfügung.

Freundliche Grüsse
EXPERTsuisse

Dr. Thorsten Kleibold
Mitglied der Geschäftsleitung

Rolf Walker
Präsident der Kommission
für Bankenprüfung

Rz	Bezeichnung	Text	Bemerkungen / Änderungsvorschläge
III. Videoidentifizierung			
14	Identitätsprüfung	Des Weiteren überprüft der Finanzintermediär die Echtheit der Identifizierungsdokumente einerseits durch das maschinelle Auslesen und Entschlüsseln der Informationen in der MRZ und andererseits anhand von mindestens drei zufällig ausgewählten optischen Sicherheitsmerkmalen ~~eines von mehreren optisch variablen Merkmalen~~ des Identifizierungsdokuments (bspw. Kinegramm). Letzteres kann mittels technischer Unterstützung oder visueller Überzeugung (bspw. Kippen des Ausweises) erfolgen. Der Finanzintermediär prüft die Übereinstimmung der entschlüsselten Informationen mit den restlichen Angaben auf dem Ausweis und mit den von der Vertragspartei im Rahmen der Eröffnung der Geschäftsbeziehung angegebenen Daten. Er vergleicht das Identifizierungsdokument mit Referenzen aus einer Ausweisdatenbank bezüglich Sicherheitsmerkmalen, Zeichenart sowie -grösse und Layout.	Im Erläuterungsbericht wird empfohlen, dass jeweils verschiedene Kategorien der Sicherheitsmerkmale berücksichtigt werden. Es ist unklar, ob die Merkmale jeweils pro Identifizierung oder zumindest in bestimmten Zeitabständen (Tag / Wochen / Monate) alterniert werden müssen.
16	Identitätsprüfung	~~Die Identität der Vertragspartei ist mittels einer TAN oder einer ähnlichen Methode zu verifizieren.~~	Die Verifizierung der Vertragspartei mittels TAN wird gemäss Erläuterungsbericht aufgehoben, da diese im Identifizierungsprozess nur einen geringen Mehrwert bietet. Hingegen biete TAN ein zusätzliches Sicherheitselement für einzelne Dienstleistungen, nachdem die Vertragspartei identifiziert wurde. Es ist unklar, ob TAN noch eine geeignete Methode für die Erklärung der wirtschaftlichen Berechtigung darstellt, insbesondere vor dem Hintergrund, dass die Telefonnummer der Vertragspartei nicht zwingend erhoben werden muss (vgl. VSB16). Wäre hingegen die Telefonnummer der Vertragspartei bei deren Identifizierung mittels TAN überprüft worden, könnte diese auch für zukünftige Bestätigungen der Vertragspartei zugeordnet werden, sofern keine Zweifel vorliegen.

IV. Online-Identifizierung			
32	Elektronische Ausweiskopie mit Echtheitsprüfung durch den Finanzintermediär	Der Finanzintermediär holt von der Vertragspartei Lichtbilder von allen relevanten Seiten ihres Identifizierungsdokuments und von ihr selbst ein. Er prüft die Übereinstimmung des erstellten Lichtbilds der Vertragspartei mit dem Lichtbild des Identifizierungsdokuments und vergleicht das Identifizierungsdokument mit Referenzen aus einer Ausweisdatenbank bezüglich Sicherheitsmerkmalen, Zeichenart sowie -grösse und Layout. Mit Unterstützung geeigneter technischer Hilfsmittel, welche mindestens das Auslesen und Entschlüsseln der Informationen in der MRZ erlauben, prüft er die Übereinstimmung der entschlüsselten Informationen mit den restlichen Angaben auf dem Ausweis und mit den von der Vertragspartei im Rahmen der Eröffnung der Geschäftsbeziehung angegebenen Daten. Der Finanzintermediär beurteilt die Echtheit des Identifizierungsdokuments anhand von mindestens drei zufällig ausgewählten optischen Sicherheitsmerkmalen, soweit sich diese auf einem Standbild überprüfen lassen. Zudem stellt der Finanzintermediär sicher, dass das Lichtbild der Vertragspartei im Rahmen des Identifizierungsvorgangs erstellt worden ist, beispielsweise durch eine Lebenderkennung (*selfie with liveness detection*).	Siehe Rz. 14 betreffend Sicherheitsmerkmale.
38-39	Elektronische Ausweiskopie mit qualifizierter elektronischer Signatur	Der Finanzintermediär holt auf einem elektronischen Kanal von der Vertragspartei eine elektronische Kopie von allen relevanten Seiten ihres Identifizierungsdokuments und deren Authentifizierung mit einer von einem in der Schweiz anerkannten Anbieter von Zertifizierungsdiensten ausgestellten qualifizierten elektronischen Signatur gemäss Bundesgesetz (ZertES; SR 943.03) ein. Der Finanzintermediär überprüft die Übereinstimmung der Angaben auf dem Ausweis mit denjenigen der qualifizierten elektronischen Signatur. Ferner verifiziert er die Identität der Vertragspartei mittels Überweisung ab einem auf den Namen der Vertragspartei lautenden Konto bei einer Bank in ~~der Schweiz~~ einem Land gemäss Rz 33 ~~oder einem Land mit gleichwertiger Geldwäschereiregulierung und -aufsicht sowie einer TAN oder einer ähnlichen Methode~~ und überprüft die Wohnsitzadresse nach Rz 34–37.	Der Finanzintermediär holt auf einem elektronischen Kanal von der Vertragspartei eine elektronische Kopie von allen **für die Identifizierung** relevanten Seiten ihres Identifizierungsdokuments…. Präzisierung
V. Erklärung über die wirtschaftliche Berechtigung			
48	TAN-Verfahren oder ähnliche Methode	Anstelle der qualifizierten elektronischen Signatur kann die Bestätigung der Vertragspartei ~~im Rahmen der Video- und Online-Identifizierung~~ auch mittels TAN oder einer ähnlichen Methode erfolgen, sofern sie eine verlässliche Zuordnung zur Vertragspartei ermöglicht.	….auch mittels TAN **(transaction authorisation number)** oder….. Erklärung der Abkürzung TAN in Klammern, da Glossar gestrichen wird. Siehe auch Kommentar zu Rz. 16.

Anhang			
	Glossar	~~**Einfache Ausweiskopie**~~ ~~Ausweiskopie, die nicht echtheitsbestätigt ist. Sie wurde entweder bei persönlicher Vorsprache oder bei Eröffnung auf dem Korrespondenzweg bzw. über digitale Kanäle im Rahmen von vereinfachten Sorgfaltspflichten erstellt, für welche die Echtheitsbestätigung aufgrund von Ausnahmebestimmungen nicht erforderlich ist.~~ ~~***Machine Readable Zone*, MRZ**~~ ~~Der maschinenlesbare Bereich ist derjenige sichtbare Teil eines Ausweisdokuments, der speziell dafür angelegt wurde, durch optische Texterkennung gelesen zu werden.~~ ~~**TAN**~~ ~~Transaktionsnummer, welche der Finanzintermediär seiner Vertragspartei als Einmalpasswort zustellt, damit sie für die Zwecke der Video- und Online-Identifizierung und der Feststellung des wirtschaftlich Berechtigten eingesetzt werden kann. Dabei sind verschiedene Verfahren bekannt, insbesondere:~~ ~~**Indizierte TAN-Liste, iTAN:** Liste mit nummerierten (indizierten) und zeitlich unbegrenzten TANs.~~ ~~**mTAN:** Mobile und zeitlich begrenzt gültige TAN, die der Finanzintermediär dem Nutzer per SMS auf eine auf dessen Namen registrierte Mobiltelefonnummer sendet.~~ ~~**photoTAN/QR-TAN:** App-basierte TAN-Verfahren, bei welchen ein auf dem Bildschirm angezeigter far-biger resp. schwarz-weisser Code in Form einer Mosaikstruktur einzulesen ist, wodurch eine TAN er-zeugt wird.~~ ~~**pushTAN:** App-basierte TAN-Verfahren von Finanzintermediären. Im Rahmen der Video- und Onlinei-dentifizierung kommen jene App in Betracht, welche vom Finanzintermediär zur Bereitstellung seiner Dienstleistungen zur Verfügung gestellt werden und durch ein Passwort geschützt sind.~~ ~~**TAN-Generator:** Mit einem TAN-Generator können TANs elektronisch erzeugt werden.~~ ~~**TAN-Liste**: Liste mit zeitlich unbegrenzten TANs.~~ ~~Der Einsatz von TAN-Verfahren setzt voraus, dass:~~ ~~die TAN vom Finanzintermediär dem Kunden über einen zweiten, unabhängigen Kanal zuzustellen ist; oder~~ ~~die App passwortgesichert sein muss.~~	Siehe Kommentar zu Rz. 16.

IDnow GmbH · Auenstr. 100 · 80469 München ·Deutschland

Eidgenössische Finanzmarktaufsicht FINMA
Frau Isabel Grüninger

Per Email: Isabel.Grueninger@finma.ch

28.03.2018

Stellungnahme IDnow GmbH / Intrum AG zum Entwurf der „Teilrevision des FINMA-Rundschreibens 2016/7 „Video- und Online-Identifizierung“

Sehr geehrte Frau Grüninger,
sehr geehrter Herr Mauerhofer
sehr geehrte Damen und Herren,

IDnow GmbH (nachfolgend ‚IDnow‘) ist einer der weltweit führenden Lösungsanbieter im Bereich der Video-Legitimation. Unsere Softwarelösung zur Identifikation per Videochat kommt in ganz Europa und darüber hinaus zum Einsatz. In der Schweiz haben wir gemeinsam mit der UBS und in Abstimmung mit der FINMA eine Video-Ident-Lösung als erstes Unternehmen am Markt platziert. Bis heute nutzen neben der UBS eine Vielzahl weiterer geldwäscherechtlich verpflichteter Unternehmen und Finanzinstitute die IDnow-Software. Eine Vermarktung unserer Lösung findet in der Schweiz durch unseren Partner Intrum AG (nachfolgend ‚Intrum‘) statt. Der Einfachheit halber enthält diese Eingabe die gemeinsamen Kommentare von IDnow und Intrum.

Nachfolgend nehmen wir, IDnow und Intrum, gemeinschaftlich Stellung zu dem Entwurf zur „Teilrevision des FINMA-Rundschreibens 2016/7 „Video- und Online-Identifizierung““. Einer Veröffentlichung unserer Stellungnahme oder Teilen daraus stimmen wir zu.

Seit April 2014 ist es erstmalig möglich, Nutzer in rechtlicher Vereinbarkeit mit dem Geldwäschegesetz über einen Videochat (Videoidentifikation oder auch Video-Legitimation gegannt) zu identifizieren. Erlaubt hat dies als erste Regulatorik die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in Deutschland. Seit 18. März 2016 ist ein vergleichbares System ebenfalls in der Schweiz rechtlich anerkennt. In die Freigabe eines solchen Systems ist die Erfahrung von 2 Jahren Betrieb in Deutschland eingeflossen. Jetzt, nach weiteren 2 Jahren und den ergänzend gewonnen Erkenntnissen begrüßen wir grundsätzlich die Überarbeitung des FINMA-

Rundschreibens 2016/7 „Video- und Online-Identifizierung“. Vorab möchten wir jedoch betonen, dass die Berücksichtigung von Sicherheitsaspekten unserer Meinung nach nicht weit genug geht. Hier kann durchaus nachgebessert werden. Entsprechende Punkte greifen wir an der jeweiligen Stelle explizit auf.

Zur besseren Übersichtlichkeit kennzeichnen wir nachfolgend die von uns kommentierten Bereiche jeweils durch deren Überschrift und Absatznummer:

III. Videoidentifizierung; A. Der persönlichen Vorsprache gleichgestellte Videoidentifizierung einer natürlichen Person; a) Technisches und Organisatorisches

Absatz (6): Die hier aufgeführte, „sichere Übertragung“ sollte spezifiziert werden. Eine Spezifizierung kann erfolgen durch die Forderung einer minimalen Schlüssellänge von idealerweise 2048 Bit.

Absatz (8): Eine Beschränkung auf die Aufzeichnung der Audiospur ist unseres Erachtens nicht ideal um die Korrektheit einer Identifikation nachzuvollziehen. Eine bessere Nachvollziehbarkeit ist dann gegeben, wenn eine audiovisuelle Aufnahme des Prozesses erfolgt. Wir schlagen deshalb die folgende Formulierung vor: „*Die Identifizierung der Vertragspartei erfolgt durch entsprechend geschulte Mitarbeitende des Finanzintermediärs. Die gesamte Dauer des Gesprächs muss audiovisuell festgehalten werden.*“

Hieraus ergeben sich ebenfalls Änderungen in den Absätzen (12) und (17), in denen die Bezeichnung „*Audioaufzeichnung*“ entsprechend geändert werden sollte in „*audiovisuelle Aufzeichnung*“.

III. Videoidentifizierung; A. Der persönlichen Vorsprache gleichgestellte Videoidentifizierung einer natürlichen Person; b) Identitätsprüfung

Absatz (14): Die Echtheit eines Identifizierungsdokuments kann unmöglich durch das maschinelle Auslesen, sehr wohl aber durch das maschinelle Entschlüsseln der Informationen der MRZ erfolgen. Wir schlagen deshalb vor, das maschinelle Auslesen als Anforderung zu streichen.

Ergänzend macht es Sinn, dass nicht nur drei zufällig ausgewählte optische Sicherheitsmerkmale überprüft werden, sondern diese idealerweise auch noch aus verschiedenen Bereichen stammen. Wir schlagen deshalb nachfolgende Anpassung vor:

„*Des Weiteren überprüft der Finanzintermediär die Echtheit der Identifizierungsdokumente einerseits durch das maschinelle Entschlüsseln der Informationen in der MRZ und andererseits anhand von mindestens drei zufällig ausgewählten optischen Sicherheitsmerkmalen aus verschiedenen Kategorien des Identifizierungsdokuments. Zu den optischen Sicherheitsmerkmalen zählen jeweils unter anderem (je nach Dokument): 1) beugungsoptisch wirksame Merkmale (Hologramme, Identigram, Kinematische Strukturen), 2) Personalisierungstechnik (Laserkippbilder, Ausfüllschrift), 3) Material (Fenster (z.B. personalisiert), Sicherheitsfaden (personalisiert), optisch variable Farbe) und 4) Sicherheitsdruck (Mikroschrift, Guillochenstruktur).*“

Absatz (16): Die Streichung des Absatzes (16) begrüßen wir, da sie keinerlei Sicherheitsrelevanz hat.

III. Videoidentifizierung; A. Der persönlichen Vorsprache gleichgestellte Videoidentifizierung einer natürlichen Person; c) Abbruch des Identifizierungsvorgangs per Video

Absätze (18-21): Der Abbruch eines Identifizierungsvorgangs per Video macht dann keinen Sinn, wenn der die Identifizierung durchführende Mitarbeitende in dem Prozess von einem Betrugsfall ausgeht. An diesem Punkt gibt es zwei Mögliche Ereignisse:

1) Ein vermeintlicher Betrugsfall ist keiner und der Mitarbeitende hat sich getäuscht. Dies kann durch das Anwenden eines 4-Augen-Prinzips am Ende des Prozesses im Sinne des zu Identifizierenden positiv aufgelöst werden.
2) Er handelt sich tatsächlich um einen Betrugsfall. Hier sollte der Prozess zwingend bis zum Ende durchgeführt werden, um einem potentiellen Betrüger keine Anhaltspunkte zu geben, an welcher Stelle des Prozesses der Betrug aufgedeckt wurde. Ein Abbruch ermöglicht Betrügern ihre Betrugsansätze zu justieren und über kurz oder lang ein System zu entwickeln, um die Videoidentifikation zu überlisten. Das wird durch die Fortführung des Prozesses bis zum Ende ohne vorherigen Abbruch erreicht.

Aufgrund der hier aufgezeigten Punkte schlagen wir folgende Anpassung der Formulierung von Absatz (21) vor: *„Sofern der Finanzintermediär Hinweise auf erhöhte Risiken erlangt oder Zweifel an der Echtheit des Ausweisdokuments oder der Identität der Vertragspartei aufkommen, darf er den Identifizierungsvorgang zwar fortführen. Er stellt jedoch sicher, dass die Geschäftsbeziehung erst aufgenommen wird, wenn die erforderliche Zustimmung einer vorgesetzten Person, einer verantwortlichen Person oder Stelle oder der Geschäftsführung gemäss Art. 18 GwV-FINMA vorliegt.“*

IV. Online-Identifizierung; B. Online-Identifizierung mittels elektronischer Ausweiskopie

Absatz (31.1*): Im Rahmen der Online-Identifizierung wird aktuell nur von einem manuellen Verfahren unter Beihilfe eines entsprechend geschulten Mitarbeitenden des Finanzintermediärs ausgegangen. Aufgrund der heute bereits weit fortgeschrittenen Technik schlagen wir vor, diesen Absatz offener und damit technikfreundlicher zu formulieren: *„Bei der Online-Identifizierung muss die Bildqualität geeignet sein, um eine einwandfreie Identifizierung zu ermöglichen. Der Finanzintermediär kann technische Mittel einsetzen um schwierige Lichtverhältnisse zu kompensieren. Die Online-Identifizierung erfolgt entweder durch entsprechend geschulte Mitarbeitende des Finanzintermediärs oder durch ein automatisiertes System, das mindestens dem Sicherheitsgrad eines Prozesses mit einem entsprechend geschulten Mitarbeitenden entspricht.“*

Absatz (31.2*): Bei einer Anpassung des vorgenannten Absatzes für (31.2*) wird die folgende Formulierung vorgeschlagen: *„Sofern im Rahmen der Online-Identifikation Hinweise auf erhöhte Risiken bestehen, darf der Identifizierungsvorgang nur dann positiv abgeschlossen und die Geschäftsbeziehung aufgenommen werden, wenn die Zustimmung einer vorgesetzten Person, einer verantwortlichen Person oder Stelle oder der Geschäftsführung gemäss Art. 18 GwV-FINMA vorliegt.“*

IV. Online-Identifizierung; B. Online-Identifizierung mittels elektronischer Ausweiskopie; a) Elektronische Ausweiskopie mit Echtheitsprüfung durch den Finanzintermediär

Absatz (32*): Auch bei der Online-Identifizierung sollte vergleichbar Absatz (14) eine Prüfung der Sicherheitsmerkmale aus verschiedenen Kategorien erfolgen.

Absatz (33*): Die Überweisung eines Geldbetrags von einem Referenzkonto als weiteres Sicherheitskriterium macht dann Sinn, wenn der Prozess der Online-Identifikation auf einem niedrigeren Sicherheitsniveau stattfindet, als dies bei einer Identifizierung bei persönlicher Vorsprache oder einer Videoidentifizierung entsprecht den Grundsätzen nach III stattfindet. Sollte die Sicherheit mindestens auf gleichem Niveau oder sogar auf höherem Niveau sein, als bei den Identifikationsverfahren nach III, macht der Verzicht auf eine Referenzüberweisung Sinn. Wir schlagen deshalb folgende ergänzende Formulierung vor: *„Eine Überweisung ist dann nicht notwendig, wenn das Sicherheitsniveau der Online-Überweisung mindestens dem der Identifikationsverfahren nach III entspricht.“*

Absatz (34): Die Streichung des erstens Satzes des Absatzes (34) begrüßen wir, da sie keinerlei Sicherheitsrelevanz aufweist.

IV. Online-Identifizierung; B. Online-Identifizierung mittels elektronischer Ausweiskopie;
b) Elektronische Ausweiskopie mit qualifizierter elektronischer Signatur

Absatz (39): Eine mögliche Anpassung des Absatzes sehen wir entsprechend der Anpassung von Absatz (33*). Eine qualifizierte elektronische Signatur (QES) ist bereits per Definition mit einem sehr hohen Sicherheitsniveau ausgestattet:

1) Um ein für eine QES nutzbare Signatur zu erhalten, muss der zu Identifizierende zwingend nach den strengen Vorgaben der Signaturgesetzgebung identifiziert werden. Eine weitere Identifikation nach ähnlichen Vorgaben führt den Identifikationsprozess im Rahmen der Signaturvergabe ad absurdum, da er doppelt absolviert werden müsste.
2) Auch kann eine elektronische Signatur nicht einfach entlehnt und durch Dritte verwendet werden. Zur Nutzung muss sie der zu Identifizierende mit mindestens zwei Faktoren aus unterschiedlichen Bereichen freigeben (Faktoren ergeben sich aus Besitz, Wissen und Sein (=biometrisches Merkmal)). Dies entspricht dem gleichen Sicherheitsniveau, wie dies die europaweit eingesetzte eID aufweist.

Bei einer Identifikation mit einer eID ist ebenfalls kein weiterer Nachweis über eine Banküberweisung gefordert Eine Andersbehandlung sehen wir deshalb nicht als zweckmäßig und sogar diskriminierend an.

V. Erklärung über die wirtschaftliche Berechtigung; B. TAN-Verfahren oder ähnliche Methode

Absatz (48): Wir halten die Identifizierung einer Person mittels TAN für ein äußerst schwaches Sicherheitsmerkmal und sprechen uns deshalb für eine komplette Streichung des Absatzes (48) aus.

Resümee:

Wie schon aufgezeigt, begrüßen wir die Anpassung des Rundschreibens 2016/7 „Video- und Online-Identifizierung“ der FINMA. In der aktuellen, überarbeiteten Version sehen wir jedoch vor allem in den beiden nachfolgenden Punkten Justierungsbedarf:

1) Sicherheit: Der Aspekt der Sicherheit sollte umfassender als bisher berücksichtigt werden. Ergänzende Maßnahmen müssen so ausgelegt sein, dass potentielle Betrugsversuche als solche erkannt werden. Idealerweise passiert das, ohne dass das die betrügerisch agierenden Personen mitbekommen. Hierdurch können maßgebliche Erfolge in der Verhinderung von Geldwäscherei erzielt werden.

2) Automatisierung: Die aktuellen Möglichkeiten zur Identifikation sind stark manuell geprägt und beziehen maßgeblich den Menschen als durchführende und damit notwendige Komponente ein. Nach heutigem Stand der Technik ist dies jedoch nicht zwingend notwendig und in vielen Bereichen sogar kontraproduktiv. Bereits heute werden die Mitarbeitenden in dem Prozess einer Videoidentifikation umfassend von technischen Routinen unterstützt. Ohne diese wäre eine sichere Identifikation und das Aufdecken betrügerischer Manipulationsversuche kaum möglich. Die heute im Einsatz befindliche Software kann jedoch nicht nur unterstützend agieren, sondern zum großen Teil autark arbeiten. Trainierte Algorithmen auf Basis von Künstlicher Intelligenz (KI) sind in der Lage, effektiver, effizienter und fehlerfreier zu agieren. Dem Faktor Mensch ist eben auch (leider) immer eine Unsicherheitskomponente zuzuordnen.

Durch automatisierte Verfahren besteht ergänzend die Möglichkeit, skalierbare Systeme zu jeder Tages- und Nachtzeit anzubieten. Wartezeiten gehören damit der Vergangenheit an. Bei mindestens gleichem, idealerweise jedoch höherem Sicherheitsniveau wie dies im Rahmen einer Identifikation nach III des Rundschreibens gegeben ist, bitte wir deshalb die Möglichkeit eines automatisierten Verfahrens wohlwollend zu prüfen.

Wie bereits in unseren persönlichen Gesprächen aufgezeigt, stehen wir gerne jederzeit für eine Demonstration des hohen Sicherheitsniveaus automatisierter Prozesse vor Ort zur Verfügung.

Mit freundlichen Grüßen

Michael Sittek
Geschäftsführer IDnow GmbH

LOYENS & LOEFF

POSTAL ADDRESS P.O. Box 1908
8027 ZURICH
OFFICE ADDRESS Alfred-Escher-Strasse 50
8002 ZURICH
Switzerland
TELEPHONE +41 43 434 67 28
INTERNET loyensloeff.ch

Per E-Mail: isabel.grueninger@finma.ch
Eidgenössische Finanzmarktaufsicht FINMA
Frau Isabel Grüninger
Laupenstrasse 27
CH-3003 Bern

FROM Andrea Huber, Dr. Sandro Germann
DATE 26. März 2018

RE Stellungnahme von Loyens & Loeff Schweiz GmbH zur Revision des Rundschreibens «2016/7 Video- und Online-Identifizierung»

Sehr geehrte Frau Grüninger
Sehr geehrte Damen und Herren

Für die Einladung zur Stellungnahme zur Revision des Rundschreibens «2016/7 Video- und Online-Identifizierung» («**RS 16/7**») danken wir Ihnen bestens und nehmen dazu wie folgt Stellung:

A. Grundsätzliches

Wir begrüssen die Revision des RS 16/7, da diese einerseits mit gewissen Erleichterungen für die Video- und Online-Identifizierung potentieller Kunden einhergeht und anderseits gewisse Unklarheiten des bestehenden Rundschreibens bereinigt.

Wie im Erläuterungsbericht zur Teilrevision des FINMA-Rundschreibens 16/7 vom 13. Februar 2018 («**Erläuterungsbericht**»), S. 6 festgehalten, ist die Möglichkeit eines administrativ und kostenmässig durchführbaren digitalen Onboardings potentieller Kunden für die Finanzdienstleiter, insbesondere Fintech Anbieter, von herausragender Bedeutung. Der Finanzplatz Schweiz und dessen Regulatoren tun gut daran, unter Berücksichtigung und Vermeidung möglicher Missbrauchs-Risiken, aber auch der Technologieneutralität zeitgerechte, innovative sowie umsetzbare Lösungen anzubieten bzw. zuzulassen.

Insgesamt bleibt es dabei, dass im Rahmen der elektronischen Überprüfung der Echtheit eines Ausweisdokuments höhere Anforderungen aufgestellt werden als dies bei den herkömmlichen Eröffnungen von Geschäftsbeziehungen der Fall ist. Insofern wäre es zu begrüssen, wenn der Detaillierungsgrad bei den Vorgaben zu den zu verwendenden technischen und technologischen Mitteln auch zukünftig nochmals reduziert sowie die Regelungen zur Erreichung der Technologie-Neutralität entsprechend der technischen Entwicklung angepasst werden.

In terminologischer Hinsicht sei die Anmerkung erlaubt, dass einerseits bzgl. des Rundschreibens von der «Video- und Online-Identifizierung» sowie bei IV. von «Online-Identifizierung», jedoch dann gleichzeitig bei III. und folgenden Titeln von «Videoidentifizierung» gesprochen wird. Aus Gründen der Einheitlichkeit sei entweder der Term «Video-Identifizierung» oder alternativ «Onlineidentifizierung» im gesamten Rundschreiben zu verwenden.

B. Zu den einzelnen Randziffern («Rz»):

III. Videoidentifizierung

Rz 14: Die revidierte technische Umsetzungsanweisung zwingt den Markt dazu, verbesserte Technologien zu entwickeln und den Identifikationsprozess zu optimieren. Inwiefern sich diese Vorgabe in hohen Kosten niederschlagen wird oder ob der Aufwand für die Anpassungen vielmehr gemäss Aussage im Erläuterungsbericht, S. 11 ganz unten «[...] überschau- und vertretbar» sein werden, wird sich weisen. Fraglich ist allerdings, ob mit der *Zufälligkeit* der Auswahl der drei Kriterien viel gewonnen ist, oder ob es nicht mehr Sinn machen würde, im Rahmen der Prüfung zumindest bei Bedarf auch drei Sicherheitsmerkmale auswählen zu können, die im konkreten Identifikationsprozess – beispielsweise aus Erfahrung – am ehesten einer Fälschung unterliegen könnten bzw. mit Bezug auf das konkrete Dokument am einfachsten so gefälscht werden können, ohne entdeckt zu werden.

Rz 16: Die Streichung dieser Rz bzw. des Erfordernisses der TAN-Verifizierung wird begrüsst, ging diese Anforderung doch deutlich weiter als diejenige, die diesbezüglich bei der herkömmlichen Aufnahme einer Geschäftsbeziehung verlangt wird.

Rz 18 ff.: Die Streichung von Rz 20 sowie die Anpassung von Rz 22 werden ebenfalls begrüsst, da bei Hinweisen auf erhöhte Risiken ein Abbruch des Identifizierungsvorgangs nicht zwingend notwendig erscheint (hingegen – wie stipuliert – eine nochmals erhöhte Sorgfalt zwecks Identifikation ausgeübt werden sollte). Die bis anhin aufgeworfene Unklarheit, ab wann von solchen Hinweisen auszugehen ist, wird damit zwar nicht beseitigt. Allerdings hat diese Unsicherheit nicht mehr zur Folge, dass der Identifizierungsvorgang abgebrochen werden muss, was zu begrüssen ist.

IV. Online-Identifizierung

Rz 31 ff.: Die Konkretisierung der formellen Anforderungen für die Online-Identifizierung schafft zusätzliche Rechtssicherheit und wird daher begrüsst.

Rz 33: Die Zulassung von Überweisungen von einer Bank in Lichtenstein oder einem Mitgliedstaat der FATF wird gerade im Hinblick auf die international tätigen Finanzintermediäre oder Fintech Unternehmen begrüsst. Es ist sinnvoll, die Überweisung zumindest von denjenigen Banken zuzulassen, die einer angemessenen Aufsicht und Regelung in Bezug auf Geldwäscherei und Terrorismusfinanzierung unterstehen. Mit der neuen Regelung wird nicht nur ein ausreichendes

LOYENS & LOEFF

Mass an Kontrolle erreicht, sondern gleichzeitig der Nachteil für derzeit betroffene Finanzdienstleister erheblich reduziert.

In terminologischer Hinsicht erscheint es besser, deutsche Begriffe wie «Sorgfaltspflichten» oder «Zahlungsaufträge» zu verwenden, sowie dies im Erläuterungsbericht, S. 10 auch gemacht wurde, anstatt sich englischer Begriffe wie «Customer due diligence» und «wire transfers» etc. im Rundschreiben zu bedienen.

Wir danken Ihnen für die Kenntnisnahme unserer Stellungnahme, deren Berücksichtigung sowie die wertvolle Zusammenarbeit. Selbstverständlich stehen wir Ihnen für Fragen oder Anregungen jederzeit zur Verfügung.

Mit freundlichen Grüssen,
Loyens & Loeff Schweiz GmbH

Andrea Huber

Dr. Sandro Germann

MovingMedia

Moving Media GmbH
Bahnhofplatz 1-3/PF 445
CH-9430 St. Margrethen SG
Switzerland

Eidgenössische Finanzmarktaufsicht FINMA
z.Hd. Isabel Grüninger
Laupenstrasse 27
CH-3003 Bern
Schweiz

St. Margrethen, SG am 27. März 2018

Teilrevision des FINMA-Rundschreibens 2016/7 „Video- und Online-Identifizierung"

Sehr geehrte Frau Grüninger, sehr verehrte Damen und Herren!

Vielen Dank für die Möglichkeit zur Stellungnahme.

Gerne beteiligen wir uns als unmittelbar betroffener Finanzintermediär an dieser Anhörung. Es erscheint uns immanent wichtig, dass das neue Regelwerk praktikabel ist. Zur nachhaltigen Stärkung des Finanzplatzes Schweiz ist es aus unserer Sicht sachgerecht, wenn die FINMA in der geplanten Verordnung folgende Aspekte berücksichtigt:

- Ergänzend schlagen wir vor, dass eine einfache Kopie der Bankkarte oder eine einfache Kopie eines Kontoauszuges zur Identifizierung des Kontos in einem FATFA-Land ausreicht.

- Falls derartige Kopien nicht vorhanden sind, sollte eine Überweisung des Finanzintermedärs an den Kontoinhaber bis zu CHF 200.00 ausreichend sein, und nicht zwingend eine Überweisung des potentiellen Kunden an den Finanzintermediär vorab erfolgen müssen.

- Darüber hinaus soll es aus praktischen Gründen möglich sein, diese Banküberweisungen in geringer Höhe (bis zu CHF 200.00) im Rahmen der kommerziellen Transaktionen durchzuführen, sodass diese nicht abgehoben vom wirtschaftlichen Geschäft und ausschliesslich für den Zweck der Video-Identifizierung vorab durchzuführen sind.

Bei allfälligen Verständnisfragen stehen wir jederzeit zur Verfügung.

Mit freundlichen Grüssen

Gez.
Bernhard Kaufmann
Geschäftsführer
Moving Media GmbH
Tel +41 71 740 1629

Email: corporate@payment21.com

SwissBanking

Eidgenössische Finanzmarktaufsicht FINMA
Frau Isabel Grüninger
Laupenstrasse 27
CH-3003 Bern

Per Mail zugestellt an:
isabel.grueninger@finma.ch

Basel, 5. April 2018
J.22.4 | LWI | +41 61 295 92 58

Anhörung zur Teilrevision des FINMA-Rundschreibens 2016/7 „Video- und Online-Identifizierung“

Sehr geehrte Frau Grüninger
Sehr geehrte Damen und Herren

Wir beziehen uns auf die am 13. Februar 2018 eröffnete Anhörung zum teilrevidierten FINMA-Rundschreiben 2016/7 „Video- und Online-Identifizierung“ (nachstehend: das Rundschreiben).

Wir bedanken uns bestens für die Konsultation in dieser für die Finanzbranche wichtigen Angelegenheit und für die gewährte Fristverlängerung. Gerne nehmen wir die Gelegenheit zur Stellungnahme wahr und unterbreiten Ihnen nachfolgend unsere Anliegen. Soweit zu einer geänderten Randziffer des Rundschreibens keine Bemerkungen erwähnt werden, sind wir mit den vorgeschlagenen Änderungen einverstanden.

I. Allgemeine Bemerkungen

- Die Digitalisierung stellt über einen einfachen Technologie- und Prozesswechsel hinaus ein Geschäftsmodell dar, welches für viele Akteure des Finanzsektors von zentraler Bedeutung ist und einem signifikanten und raschen technologischen Wandel unterliegt. Es ist daher von entscheidender Bedeutung, dass sich die regulatorischen Vorschriften auf die zu bewältigenden Risiken und die Festlegung von allgemeinen Grundsätzen für die Durchführung von Massnahmen zur Risikominderung konzentrieren. Eine übermässige Beeinträchtigung der technischen Lösungen, die zum Zeitpunkt des Erlasses einer Regulierung bestehen, muss vermieden werden (Technologieneutralität).

- Die SBVg begrüsst die grundsätzliche Stossrichtung der Anhörungsvorlage, insbesondere im Hinblick auf die vorgesehenen Erleichterungen (bspw. Verzicht auf Einmal-Passwort, der sog. Transaktionsnummer [TAN] in der Online-Identifikation) und die Erweiterung auf ausgewählte FATF-Mitgliedsstaaten, aus denen die Erstüberweisung bei Eröffnung einer Geschäftsbeziehung mittels Online-Identifizierung stammen kann. Ebenfalls explizit begrüsst wird die Möglichkeit, neu den Identifizierungsvorgang fortzuführen, wenn Hinweise auf erhöhte Risiken bestehen.
- Abgelehnt wird das für die Video-Identifizierung neu geschaffene Erfordernis, mindestens drei zufällig ausgewählte optische Sicherheitsmerkmale des Identifizierungsdokuments zu überprüfen. Dadurch entstehen empfindliche Einschränkungen im Kundensegment, da längst nicht alle weltweit ausgestellte Identifizierungsdokumente über drei unterschiedliche optische Sicherheitsmerkmale verfügen. Schliesslich erscheint dieses neue Erfordernis im internationalen Vergleich als zu weitgehend, wodurch ein unerwünschter Swiss Finish entsteht. Ebenfalls abgelehnt wird die generelle Pflicht, das Identifizierungsdokument mit Referenzen aus einer Ausweisdatenbank bezüglich Sicherheitsmerkmale, Zeichenart sowie -grösse und Layout abzugleichen.
- Abschliessend weisen wir noch darauf hin, dass zur Reduktion der Risiken für die Banken (vgl. die Bemerkung zu Rz. 2 ff.) das Datum des Inkrafttretens des revidierten Rundschreibens zumindest mit dem Publikationsdatum der revidierten VSB (voraussichtlich VSB 20) abzustimmen ist.

II. Zu den einzelnen Bestimmungen

Ad Rz. 2 – 4

Die Bestimmungen von Rz 2 – 4, wonach das Rundschreiben direkt für Banken zur Anwendung gelangt, schafft für Banken nicht unerhebliche Risiken. Schliesslich gelten für Banken bekanntlich aufgrund des Verweises von Art. 35 GwV-FINMA im Bereich der formellen Sorgfaltspflichten (Art. 3 – 5 GwG) die Bestimmungen der jeweils geltenden Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken (VSB). Die Einhaltung der Vorgaben der VSB wird durch die Aufsichtskommission VSB überwacht und bei Verletzungen werden vertragsrechtliche Konventionalstrafen ausgesprochen. Die Aufsichtskommission VSB gründet ihre rechtlichen Einschätzungen alleine auf die jeweils anwendbare VSB. Auch der von der SBVg zur VSB erstellte Kommentar ist für die Aufsichtskommission nicht bindend, sondern dient lediglich als Materialie (vgl. Art. 3 VSB 16). Entsprechend besteht für Banken folglich ein Risiko von allfälligen Verletzungen der VSB bei der Anwendung der Bestimmungen dieses neuen Rundschreibens. Dies zumindest so lange, als diese Bestimmungen nicht im Wortlaut der VSB reflektiert sind bzw. über einen Verweis ihre Grundlage finden. Die überarbeitete VSB 16 (voraussichtlich VSB 20), die am 1.1.2020 in Kraft treten soll, wird dies entschärfen. Um die Risiken für die Banken bis dahin zu reduzieren, ist die Inkraftsetzung der neuen Bestimmungen des Rundschreibens mit der Publikation der VSB 20 (voraussichtlich im Mai 2018) abzustimmen.

Ad Rz 14

Die SBVg lehnt das neue Erfordernis, im Rahmen der Eröffnung einer Geschäftsbeziehung mittels Video-Identifizierung mindestens drei zufällig ausgewählte optische Sicherheitsmerkmale des Identifizierungsdokuments zu überprüfen, entschieden ab. Dies aus folgenden Gründen:

- Es ist nicht ersichtlich, aus welchem Grund neu drei optische Sicherheitsmerkmale überprüft werden sollen. So wissen Personen, welche eine Geschäftsbeziehung mittels Video-Identifizierung eröffnen wollen, dass sie während einer aufgezeichneten Videoübermittlung (Sprache und/oder Bild) vor der Kamera sprechen müssen und zumindest die Tonspur gespeichert wird. Dies hat eine wirksame Abschreckung in Bezug auf einen möglichen Identitätsbetrug, da keine Anonymisierung besteht, welche die Hemmschwelle für illegale Handlungen allenfalls senken würde. Zudem scheint es seit Inkrafttreten des Rundschreibens nicht zu einer signifikanten Zunahme von Betrugsversuchen gekommen zu sein. Zumindest wird dies von der FINMA weder behauptet noch nachgewiesen. Eine systematische Erhöhung der Anforderungen ist damit nicht gerechtfertigt.
- Des Weiteren würde diese zusätzlichen Anforderungen die Möglichkeit der Eröffnung einer Geschäftsbeziehung mittels Video-Identifizierung für international tätige Finanzintermediäre deutlich reduzieren. Tatsächlich verfügen weltweit gesehen bei weitem nicht alle ausgestellten Identifizierungsdokumente über drei optische Sicherheitsmerkmale, die in öffentlichen Ausweisdatenbanken aufgeführt sind. Die Identifizierungsdokumente, die von einer erheblichen Anzahl von Ländern ausgestellt werden (z.B. Frankreich, Grossbritannien, Italien, Norwegen, Türkei und Israel), ermöglichen es nicht, auf den Identifizierungsdokumenten drei optische Sicherheitsmerkmale mit blossem Auge zu überprüfen. Dazu gehört auch die Schweizer Identitätskarte. Insbesondere für Finanzintermediäre, die weltweit Kunden betreuen und Geschäftsbeziehungen mittels Video-Identifizierung eröffnen, ist es von grösster Bedeutung, dass die Identifizierungsanforderungen nicht erschwert werden. Eine Erhöhung auf drei Sicherheitsmerkmale, die überprüft werden müssen, erscheint daher auch aus diesem Blickwinkel als nicht gerechtfertigt und nicht praktikabel.
- Zudem zeigt ein Blick auf andere Länder, die eine Video-Identifizierung zulassen (u.a. Deutschland, Liechtenstein, Luxemburg, Malta, Österreich, Spanien und Singapur), dass die Schweiz mit diesen neuen Bestimmungen mithin die strengsten Anforderungen an die Video-Identifizierung statuieren würde. Der überwiegende Teil dieser Jurisdiktionen verfolgt einen risikobasierten Ansatz bei der Echtheitsprüfung des Identifizierungsdokuments. Um nicht in einen Wettbewerbsnachteil zu geraten, wäre es deshalb sinnvoll, auch in diesem Bereich einen risikobasierten Ansatz zu wählen.
- Schliesslich würde die von der FINMA in Betracht gezogene neue Anforderung, das Identifizierungsdokument mit Hilfe einer Datenbank auf die optischen Sicherheitsmerkmale, die Struktur, die Schriftart und die Schriftgröße zu überprüfen, einen erheblichen Zeit- und Arbeitsaufwand erfordern, da diese Überprüfung meist manuell erfolgt. Dies bedeutet, dass der Einsatz eines automatisierten Systems erforderlich wäre, was wiederum zusätzliche Investitions- und Implementierungskosten nach sich ziehen würde, die aus unserer Sicht weder risikogerecht noch verhältnismässig sind. Auch möchten wir darauf hinweisen, dass nicht davon auszugehen ist, dass der Aussteller einer echtheitsbestätigten Kopie eines Identifikationsdokuments gemäss Art. 11 VSB 16 (erforderlich im Rahmen der Eröffnung einer Geschäftsbeziehung auf dem Korrespondenzweg) eine solche Überprüfung vornimmt.

Aus diesen Gründen beantragen wir folgende Anpassung der Rz 14:

Rz 14
Des Weiteren überprüft der Finanzintermediär die Echtheit der Identifizierungsdokumente einerseits durch das maschinelle Auslesen und Entschlüsseln der Informationen in der MRZ und andererseits anhand von ~~mindestens drei zufällig ausgewählten~~ einem optischen Sicherheitsmerkmal~~en~~ des Identifizierungsdokuments (bspw. Kinegramm). Letzteres kann mittels technischer Unterstützung oder visueller Überzeugung (bspw. Kippen des Ausweises) erfolgen. Der Finanzintermediär prüft die Übereinstimmung der entschlüsselten Informationen mit den restlichen Angaben auf dem Ausweis und mit den von der Vertragspartei im Rahmen der Eröffnung der Geschäftsbeziehung angegebenen Daten. ~~Er vergleicht das Identifizierungsdokument mit Referenzen aus einer Ausweisdatenbank bezüglich Sicherheitsmerkmalen, Zeichenart sowie -grösse und Layout.~~

Ad Rz 21
Wir empfehlen, dass analog zu Art. 46 VSB 16 dem Finanzintermediär die Möglichkeit gegeben werden soll, allfällige Zweifel mittels weiteren Abklärungen auszuräumen, bevor der Identifizierungsvorgang per Video abgebrochen werden muss.

Rz 21
wenn Zweifel an der Echtheit des Ausweisdokuments oder der Identität der Vertragspartei aufkommen und diese Zweifel nicht durch weitere Abklärungen ausgeräumt werden können (beispielsweise durch Vergleich mit Referenzen aus einer Ausweisdatenbank hinsichtlich Art, Struktur, Aufbau oder Sicherheitsmerkmalen des vorgelegten Identifizierungsdokuments).

Ad Rz 31.1 (neu)
Der Zusatz „des Finanzintermediärs“ im letzten Satz sollte gestrichen werden, da der Finanzintermediär gemäss Rz 51 des Rundschreibens (vgl. auch Art. 43 VSB 16) die Identifizierung der Vertragspartei, die Feststellung des Kontrollinhabers wie auch die Feststellung des wirtschaftlich Berechtigten an einen Dritten delegieren kann.

Rz 31.1 (neu)
Bei der Online-Identifizierung muss die Bildqualität geeignet sein, um eine einwandfreie Identifizierung zu ermöglichen. Der Finanzintermediär kann technische Mittel einsetzen um schwierige Lichtverhältnisse zu kompensieren. Die Online-Identifizierung erfolgt durch entsprechend geschulte Mitarbeitende ~~des Finanzintermediärs~~.

Ad Rz 31.3 (neu)
Unseres Erachtens ist nicht ersichtlich, wie optische Sicherheitsmerkmale auf einer dem Finanzintermediär zugestellten elektronischen Kopie des Ausweisdokuments geprüft werden können. Das ginge nur mit dem Identifizierungsdokument selbst, welches aber nicht vorliegt. Aus diesem Grund empfehlen wir folgende Anpassung:

Rz 31.3 (neu
Im Rahmen dieses Verfahrens können nur amtliche Ausweisdokumente des jeweiligen Ausstellerlandes als Identifizierungsnachweis dienen, die über eine MRZ ~~und optische Sicherheitsmerkmale wie bspw. holografisch-kinematische Merkmale oder Druckelemente mit Kippeffekt~~ verfügen.

Ad Rz 32
Aus unserer Sicht beinhaltet der Anpassungsvorschlag zu Rz 32 verschiedene problematische Aspekte:

- Systematischer Vergleich mit einer Ausweisdatenbank: Vgl. Ausführungen zu Rz 14.
- Erstellung des Lichtbildes im Rahmen des Identifizierungsvorgangs („selfie with liveness detection"): Wie bereits unter Rz 14 erwähnt, wird seitens FINMA nicht dargelegt, inwiefern es zu einer signifikanten Zunahme von Betrugsversuchen gekommen ist, welche die Erhöhung der Anforderungen rechtfertigen würde. Der Einsatz von „selfies with liveness detection" sollte deshalb im Zweifelsfall risikobasiert zur Anwendung gelangen und nicht systematisch vorgeschrieben werden.

Rz 32
Der Finanzintermediär holt von der Vertragspartei Lichtbilder von allen relevanten Seiten ihres Identifizierungsdokuments und von ihr selbst ein. Er prüft die Übereinstimmung des erstellten Lichtbilds der Vertragspartei mit dem Lichtbild des Identifizierungsdokuments ~~und vergleicht das Identifizierungsdokument mit Referenzen aus einer Ausweisdatenbank bezüglich Sicherheitsmerkmalen, Zeichenart sowie -grösse und Layout~~. Mit Unterstützung geeigneter technischer Hilfsmittel, welche mindestens das Auslesen und Entschlüsseln der Informationen in der MRZ erlauben, prüft er die Übereinstimmung der entschlüsselten Informationen mit den restlichen Angaben auf dem Ausweis und mit den von der Vertragspartei im Rahmen der Eröffnung der Geschäftsbeziehung angegebenen Daten. Der Finanzintermediär beurteilt die Echtheit des Identifizierungsdokuments anhand von einem optischen Sicherheitsmerkmal, soweit sich dies auf einem Standbild überprüfen lässt. ~~mindestens drei zufällig ausgewählten optischen Sicherheitsmerkmalen, soweit sich diese auf einem Standbild überprüfen lassen. Zudem stellt der Finanzintermediär sicher, dass das Lichtbild der Vertragspartei im Rahmen des Identifizierungsvorgangs erstellt worden ist, beispielsweise durch eine Lebenderkennung (selfie with liveness detection).~~ Hat der Finanzintermediär Zweifel an der Echtheit des Identifizierungsdokuments, so trifft er weitere Abklärungen (beispielsweise durch Vergleich mit Referenzen aus einer Ausweisdatenbank hinsichtlich Art, Struktur, Aufbau oder Sicherheitsmerkmalen des vorgelegten Identifizierungsdokuments).

Ad Rz 33
Neu ist anstelle von einer Überweisung von einer Schweizer oder Liechtensteinischen Bank unter bestimmten Bedingungen auch eine Überweisung von Banken, die in einem Mitgliedstaat der Financial Action Task Force (FATF) ansässig sind, möglich, was grundsätzlich zu begrüssen ist. Wir schlagen jedoch vor zu prüfen, ob auf diese Anforderung nicht gänzlich verzichtet werden kann. Die VSB 16 enthält keine entsprechende Regelung. Zudem ist diese Anforderung gerade in Hinblick auf das online-affine jugendliche Klientel bei der Eröffnung eines Erst-Kontos nicht praktikabel: Eröffnet eine (jugendliche) Person mittels Video-Identifizierung ein Erst-Konto, so verfügt diese Person über kein anderes auf den eigene Namen lautendes Konto, von dem eine Überweisung auf das Erstkonto getätigt werden könnte.

Im Sinne eines modernen und konsequenten Online-Identifizierungsprozesses müsste aus unserer Sicht auf das Zusatzerfordernis der Geldüberweisung von einer Bank gänzlich verzichtet und Rz 33 gesamthaft gestrichen werden.

Sollte auch weiterhin an einer Beschränkung auf gewisse FATF-Mitgliedsstaaten festgehalten werden, erlauben wir uns folgende Ausführungen:

- Gemäss den von der FATF veröffentlichten Informationen wurde nur ein Drittel der FATF-Mitgliedsstaaten nach der neuesten Methodik bewertet. Die vorgeschlagene Formulierung lässt Zweifel aufkommen, wie die verbleibenden zwei Drittel der FATF-Mitgliedstaaten zu behandeln sind. Beispielsweise wurden die folgenden Länder bei der 3. Bewertung als nicht konform zu den einschlägigen Empfehlungen eingestuft und wurden noch nicht nach der neuesten Methodik geprüft: Island, Japan, Neuseeland, Türkei.
- Die verschiedenen AML-Regulierungen beinhalten bereits heute das Konzept der "angemessenen Aufsicht und einer Regelung in Bezug auf die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung“, um die Anwendung bestimmter Ausnahmen zu rechtfertigen (vgl. die Ausstellung von Echtheitsbestätigungen durch ausländische Finanzintermediäre, sofern diese einer gleichwertigen/angemessenen Aufsicht und Regelung in Bezug auf die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung unterstehen, Art. 49 GwV-FINMA sowie Kommentar zu Art. 11 VSB 16). Dieses Konzept sollte genutzt werden, um den Kreis derjenigen Jurisdiktionen zu bestimmen, die unter Rz 33 subsumiert werden können. Die Mitgliedschaft in der FATF und die Bezugnahme auf die Arbeit der FATF (gegenseitige Evaluationen) und deren Ergebnisse (Rating) bleiben natürlich ein nützliches Instrument, um diese Frage beantworten zu können. Möchte ein Finanzintermediär die Anwendung dieser Bedingung auf andere Jurisdiktionen (z.B. Nichtmitglieder der FATF) ausdehnen, müsste er nachweisen, auf welcher Grundlage er dies tun will.

Aus diesen Gründen wäre Rz 33 zumindest wie folgt anzupassen:

Rz 33
Der Finanzintermediär lässt sich bzw. der Depotbank überdies von der Vertragspartei Geld ab einem auf den Namen der Vertragspartei lautenden Konto bei einer Bank in der Schweiz oder Liechtenstein überweisen. Anstelle eines Kontos bei einer Bank in der Schweiz oder Liechtenstein ist ebenfalls ein solches bei einer ausländischen Bank, ~~in ei-~~

~~nem Mitgliedstaat der Financial Action Task Force (FATF) ausreichend, sofern dieser Staat im Rahmen der FATF-Länderprüfung in Bezug auf die Empfehlungen zu Customer due diligence und Wire transfers nicht mit non-compliant und bei den Immediate Outcomes 3 (Supervision) und 4 (Preventive measures) nicht mit low bewertet wurde.~~ die einer angemessenen prudentiellen Aufsicht und einer Regelung in Bezug auf die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung untersteht, ausreichend.

Ad Rz 37

Um klarzustellen, dass die Wohnsitzadresse der Vertragspartei entweder mittels eines öffentlichen Registers oder mittels einer Datenbank bzw. eines Verzeichnisses, das durch einen vertrauenswürdigen Privaten geführt wird, zu überprüfen ist, empfehlen wir nachfolgende sprachliche Anpassung.

Rz 37

- eines öffentlichen Registers~~,~~ oder einer/eines durch einen vertrauenswürdigen Privaten geführten Datenbank oder ~~eines solchen~~ Verzeichnisses.

Ad Rz 38/39

Mit Anbringung der qualifizierten elektronischen Signatur nach Schweizer Recht („QES“) sollte sich die zusätzliche „Prüfung der Identität“ mittels Kontoüberweisung oder Wohnsitzbestätigung erübrigen, da die Person zwingend für die Erstellung der QES gemäss Bundesgesetz identifiziert wurde. Wichtig und zu prüfen ist jedoch, dass es sich um ein echtes Identifikationsdokument der betreffenden Person handelt. Aus diesem Grund sollte anstelle eines Verweises auf Rz 33 bzw. 34-37 eine Prüfung analog Rz 32 vorgesehen sein.

Zudem erscheint uns die Einschränkung in Rz 38, wonach der Anbieter von Zertifizierungsdiensten in der Schweiz anerkannt sein muss, als sehr einschränkend. Wir empfehlen deshalb die Ausweitung auf von der EU anerkannte Anbieter von Zertifizierungsdiensten.

Rz 39

Der Finanzintermediär ~~über~~prüft die Übereinstimmung der Angaben auf dem Ausweis mit denjenigen der qualifizierten elektronischen Signatur. ~~Ferner verifiziert er die Identität der Vertragspartei mittels Überweisung ab einem auf den Namen der Vertragspartei lautenden Konto bei einer Bank in einem Land gemäss Rz 33 und überprüft die Wohnsitzadresse nach Rz 34–37.~~ Zusätzlich prüft er die Übereinstimmung des erstellten Lichtbilds der Vertragspartei mit dem Lichtbild des Identifizierungsdokuments. Hat der Finanzintermediär Zweifel an der Echtheit des Identifizierungsdokuments, so trifft er weitere Abklärungen (beispielsweise durch Vergleich mit Referenzen aus einer Ausweisdatenbank hinsichtlich Art, Struktur, Aufbau oder Sicherheitsmerkmalen des vorgelegten Identifizierungsdokuments).

Ad Rz 40
Das Erfordernis, die Datei mit einem Mitarbeitervisum zu versehen, ist aus unserer Sicht nicht notwendig, da dadurch kein Mehrwert erlangt werden kann. Wir empfehlen deshalb die Streichung des Mitarbeitervisums.
Sollte die FINMA am Erfordernis des Mitarbeitervisums festhalten, ist es aus unserer Sicht unklar, ob das Mitarbeitervisum zwingend eine physische Unterschrift des Mitarbeiters darstellen muss, was aus unserer Sicht nicht praktikabel wäre. Wir empfehlen deshalb, einen entsprechenden Hinweis zu formulieren, wonach kein physisches Mitarbeitervisum notwendig ist, sondern ein „elektronischer Hinweis" auf den im Einzelfall handelnden Mitarbeiter ausreichend ist.

Ad Rz 52
Eine Präzisierung, dass die Aufnahme von Geschäftsbeziehungen mittels Video- oder Online-Identifikation ausschliesslich schweizerischem Recht untersteht, wäre zu begrüssen. Der entsprechende Text könnte in Rz 52 oder alternativ als Rz 4.1 in das Rundschreiben eingefügt werden.

VII. ~~Aufgehoben~~ Anwendbares Recht
Rz 52
~~Aufgehoben~~ Die Aufnahme von Geschäftsbeziehungen über digitale Kanäle durch einen Finanzintermediär gemäss Rz 2 untersteht ausschliesslich schweizerischem Recht.

Wir danken Ihnen für die Kenntnisnahme unserer Stellungnahme und die Berücksichtigung unserer Überlegungen für die weiteren Arbeiten. Gerne stehen wir Ihnen für ergänzende Auskünfte zur Verfügung.

Freundliche Grüsse
Schweizerische Bankiervereinigung

Rolf Brüggemann
Leiter Tax, Legal & Compliance und Regulatory

Frank Kilchenmann
Leiter Compliance, Geldwäscherei und Datenschutz

SRO-SLVASSL
Selbstregulierungsorganisation des
Schweizerischen Leasingverbandes SRO/SLV

Eidgenössische Finanzmarktaufsicht FINMA
Frau Isabel Grüninger
Laupenstrasse 27
CH-3003 Bern

Per Mail zugestellt an:
isabel.grueninger@finma.ch

Zürich, 6. April 2018

Stellungnahme zur Teilrevision des RS FINMA 2016/7 „Video- und Online-Identifizierung"

Sehr geehrte Frau Grüninger
Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, zur Teilrevision von RS FINMA 2016/7 Stellung nehmen zu können. Sie haben uns dazu die Frist freundlicherweise bis heute Freitag, 6. April 2018, erstreckt. Innert Frist reichen wir Ihnen somit unsere nachfolgende Stellungnahme ein und danken Ihnen für eine Berücksichtigung unserer Anträge und Argumente.

Zusammenfassung

1) Wir begrüssen die Weiterentwicklung des RS FINMA 2016/7 unter dem Vorbehalt des Grundsatzes der Technologieneutralität, der Vorhersehbarkeit der Regulierung und der Beachtung eines risikobasierten Ansatzes.
2) Die Prüfung von mindestens drei Sicherheitsmerkmalen sowie eine systematische Abgleichung von Identifizierungsdokumenten mit Ausweisdatenbanken gemäss Rz. 14 lehnen wir ab. Eventuell soll ein Abgleich mit Ausweisdatenbanken risikobasiert eingeführt und sollen (mehrere) Ausweisdatenbanken genannt werden, welche den Anforderungen der FINMA genügen.
3) Vor Abbruch des Identifizierungsvorganges wegen Zweifeln an der Echtheit des Ausweisdokumentes im Sinne von Rz. 21 Abs. 1 soll der Finanzintermediär seine Zweifel durch angemessene Massnahmen ausräumen dürfen.
4) Die Online-Identifizierung soll auch durch Delegierte vorgenommen werden können (Rz. 31.1).
5) Auf die Anforderung in Rz. 31.3 (neu), dass bei der Online-Identifizierung nur Ausweise mit optischen Sicherheitsmerkmalen verwendet werden dürfen, ist mangels Überprüfbarkeit derselben im Online-Prozess zu verzichten.
6) Auf das Erfordernis einer Banküberweisung zur „Prüfung der Identität" in Rz. 32 ist zu verzichten oder als Alternative einzuführen. Die Lebenderkennung (selvie with liveness detection) bei der Online-Identifizierung ist nicht systematisch, sondern risikobasiert einzuführen.
7) Auf das Erfordernis einer Wohnsitzbestätigung und einer Banküberweisung ist bei der Verwendung einer qualifizierten elektronischen Signatur zu verzichten. Es sollen auch qualifizierte elektronische Signaturen ausländischer Anbieter mit Anerkennung in der EU zugelassen werden (Rz. 38 f.)

1. Vorbemerkungen

1.1 Die Digitalisierung von Geschäftsabläufen schreitet immer schneller voran. Gleichermassen flankierend entstehen laufend Möglichkeiten, Sicherheitsanforderungen und Regulierungsvorgaben wiederum digital zu erfüllen. Bekanntlich ist in allen Bereichen der Digitalisierung das Entwicklungstempo sehr hoch. Dies hat jede Regulierung in Betracht zu ziehen. Es erstaunt deshalb nicht, dass das RS FINMA 2016/7 bereits wieder einer Teilrevision unterzogen wird. Es muss aber das Bestreben jedes Regulators sein, das **Gebot der Technologieneutralität und die Voraussehbarkeit der Regulierung** bestmöglich zu wahren, um den Regulierungsunterworfenen die Möglichkeit zu geben, getätigte Investitionen, neue Prozesse und Technologien gewinnbringend einsetzen zu können.

1.2 Ebenso sind neue Regelungen im GwG-Bereich stets unter **Berücksichtigung eines risikobasierten Ansatzes** zu erlassen und es ist den Regulierungsunterworfenen zu gestatten, bei der Umsetzung der Sorgfaltspflichten selbst einen risikobasierten Ansatz zu wählen.

Gerade bei digitalisierten Abläufen wird oft vergessen, dass diese zwar grosse Sicherheit versprechen, aber bei ihrer Integration in die Geschäftsabläufe sehr hohe Kosten auslösen. Diese potenzieren sich, wenn immer wieder neue Regelungen geschaffen werden. Mit der konsequenten Anwendung des risikobasierten Ansatzes hat sich der Regulator einerseits zu fragen, ob und welche neuen Regularien überhaupt nötig sind, und andererseits den Finanzintermediären risikobasierte und effiziente (mithin auch kostengünstige) Lösungen in der Umsetzung zu gestatten.

1.3 Mit diesen Vorbehalten **begrüssen wir die Stossrichtung der Teilrevision des RS FINMA** 2016/7. Insbesondere begrüssen wir, dass neue technischen Möglichkeiten zugelassen und zum Beispiel auf das Erfordernis von Einmalpasswörtern (Transaktionsnummern) verzichtet, die Fortsetzung des Identifizierungsvorganges auch bei Hinweisen auf erhöhte Risiken unter bestimmten Voraussetzungen ermöglicht wird, und einer schriftlichen Notiz auch elektronische Dateien (so zum Beispiel im pdf-Format) und entsprechende Bildformate gleichgestellt werden.

2. Zu einzelnen Bestimmungen

2.1 **Randziffer 14** bestimmt neu, dass der Finanzintermediär im Rahmen der Eröffnung einer Geschäftsbeziehung mit Video-Identifizierung mindestens drei zufällig ausgewählte optische Sicherheitsmerkmale des Identifizierungsdokumentes zu überprüfen habe. Damit wird ausser Acht gelassen, dass längst nicht alle zulässigen Identifizierungsdokumente überhaupt drei Sicherheitsmerkmale aufweisen. International tätige Finanzintermediäre könnten deshalb die Video-Identifikation für Bürger vieler Staaten nicht anwenden.

Im Vergleich zu anderen Ländern (wie u.a. Deutschland, Liechtenstein, Spanien und Singapur), die keine solchen Anforderungen an die Video-Identifizierung stipulieren und sich mit der Anwendung eines risikobasierten Ansatzes begnügen, besteht kein Anlass, dass die Schweiz hier vorprescht. Gegenteils gilt es, einen Wettbewerbsnachteil zu verhindern. Der Finanzintermediär soll deshalb die Echtheit des Identifizierungsdokumentes wie bisher auf Grund „eines von mehreren optisch variablen Merkmalen" prüfen.

Die neue Anforderung, das Identifizierungsdokument in jedem Fall mit Referenzen aus einer Ausweisdatenbank bezüglich Sicherheitsmerkmalen, Zeichenart sowie –grösse und Layout zu vergleichen, ist abzulehnen. Sie würde einen erheblichen Zeit- und Kostenaufwand bedeuten, da die Abgleichung mit der Datenbank wohl manuell erfolgen müsste. Es sollte auch hier der risikobasierte Ansatz gelten.

Zusammenfassend lehnen wir die Änderungen in Randziffer 14 ab. Eventualiter ist ein Abgleich mit Ausweisdatenbanken nach risikobasierten Ansatz einzuführen und sollten (im Sinne einer Unterstützung der Finanzintermediäre) mehrere Ausweisdatenbanken genannt werden, welche den Anforderungen der FINMA genügen.

2.2 Gemäss **Randziffer 21 Abs. 1 zweiter Punkt** hat der Finanzintermediär den Identifizierungsvorgang abzubrechen, wenn Zweifel an der Echtheit des Ausweisdokumentes oder der Identität der Vertragspartei entstehen. Die Bestimmung sollte dahingehend ergänzt werden, dass der Finanzintermediär allfällige Zweifel durch weitere Abklärungen ausräumen kann, so beispielsweise durch Abgleichung mit einer Ausweisdatenbank.

Wir schliessen uns dem diesbezüglichen ausformulierten Antrag der Schweizerischen Bankiervereinigung zu Rz. 21 an.

2.3 **Randziffer 31.1 (neu)** beschränkt die Online-Identifizierung auf Mitarbeitende des Finanzintermediärs. Dies widerspricht den bisherigen anerkannten Grundsätzen, wonach u.a. die Identifikation der Vertragspartei an einen Dritten delegiert werden kann. Es wird im Erläuterungsbericht nicht dargelegt, dass und weshalb eine Einschränkung der Delegationsmöglichkeit notwendig sei. Es handelt sich deshalb wohl um ein redaktionelles Versehen.

Der letzte Satz von Rz. 31.1 sollte deshalb wie folgt ergänzt werden (Ergänzung fett gedruckt):

> „Die Online-Identifizierung erfolgt durch entsprechend geschulte Mitarbeitende des Finanzintermediärs **oder dessen Delegierten**."

2.4 Gemäss **Randziffer 31.3 (neu)** sollen nur amtliche Ausweisdokumente des jeweiligen Ausstellerlandes als Identifizierungsnachweis dienen, die über eine MRZ und optische Sicherheitsmerkmale wie beispielsweise holografisch-kinematische Merkmale oder Druckelemente mit Kippeffekt verfügen. Wir sind allerdings der Auffassung, dass solche Sicherheitsmerkmale aufgrund der übermittelten Kopie des Ausweises im Online-Prozess nicht geprüft werden können, weshalb auf diese Anforderung zu verzichten ist.

Wir schliessen uns dem diesbezüglichen Antrag der Schweizerischen Bankiervereinigung zu Rz. 31.3 an.

2.5 **Randziffer 32** enthält mehrere problematische Änderungen. Dass auf einen systematischen Abgleich mit Ausweisdatenbanken verzichtet werden sollte, haben wir bereits unter Ziffer.2.1 zu Rz. 14 ausgeführt. Wir halten auch mit Bezug auf Rz. 32 fest, dass diese Anforderung zu streichen oder eventualiter nur mit einem risikobasierten Ansatz einzuführen ist sowie (mehrere) Beispiele von der FINMA genehmen Ausweisdatenbanken aufzuführen sind.

Gleich wie bei der Video-Identifizierung muss auch hier das Prüfen eines optischen Sicherheitsmerkmals genügen, wobei auch dies im Rahmen der Online-Identifizierung nur möglich

ist, wenn sich das optische Sicherheitsmerkmal auf einem Standbild überprüfen lässt. Eine entsprechende Einschränkung ist im Text von Rz. 32 einzufügen.

Sinnvoll wäre es, analog der Ausführungen in Ziffer 2.2 oben zu Rz. 21. Abs. 1 eine Ausräumung von Zweifeln an der Echtheit des Identifizierungsdokumentes durch weitere Abklärungen zuzulassen.

In Rz. 32 am Ende wird im Rundschreiben selbst sodann ausgeführt:

„Zudem stellt der Finanzintermediär sicher, dass das Lichtbild der Vertragspartei im Rahmen des Identifizierungsvorgangs erstellt worden ist, beispielsweise durch eine Lebenderkennung (selfie with liveness detection)".

Demgegenüber kann der dazu gehörige Wortlaut in den Erläuterungen so verstanden werden, dass immer eine Lebenderkennung (selvie with liveness detection) nötig sei. In Nachachtung des Gebotes der Technologieneutralität sowie der Anwendung des risikobasierten Ansatzes sollte der Wortlaut des Rundschreibens wie von der FINMA vorgeschlagen stehen bleiben und derjenige im Erläuterungsbericht angepasst werden. Es muss auf jeden Fall verhindert werden, dass eine systematische Lebenderkennung (selvie with liveness detection) nötig wird.

Auch an dieser Stelle unterstützen wir im Übrigen den ausformulierten Textvorschlag der Schweizerischen Bankiervereinigung zu Rz. 32.

2.6 Die in **Randziffer 33** nach wie vor enthaltene Überweisung eines Betrages von einem Bankkonto als zusätzliche „Überprüfung der Identität" des Vertragspartners sollte ersatzlos gestrichen oder dann als Alternative eingeführt werden.

Vorab werden sonst Kunden, die ein erstes Mal ein Konto eröffnen, vom Online-Identifizierungsprozess ausgeschlossen, ohne dass dafür ein nachvollziehbarer Grund ersichtlich wäre. Gerade technoaffine Personen, die ihre Bankgeschäfte mit Vorliebe digital abwickeln möchten, würden dafür mit Recht kein Verständnis aufbringen. Es gibt sodann keinen ersichtlichen Grund, weshalb mit einer Banküberweisung mehr Sicherheit gewonnen wäre. Zumal der Grundsatz gilt, dass sich Finanzintermediäre nicht auf die Einhaltung der Sorgfaltspflichten anderer Finanzintermediäre verlassen dürfen.

Hingegen ist eine Überprüfung der Identität der Kunden mittels Banküberweisungen ein probates und beliebtes Mittel, welches auch alternativ statt kumulativ einsetzbar wäre.

Die Ausdehnung der Möglichkeit zur Überweisung von Konten von Schweizer Banken auf solche von Liechtenstein und von FATF-Mitgliedern, die über ein bestimmtes Prädikat im Rahmen einer FATF-Länderprüfung verfügen, erscheint sinnvoll, erfordert aber eine zusätzliche Hilfestellung an die FI:

Vorab wurden längst noch nicht alle Länder nach dem neuen Prüfstandard geprüft. Sodann können die Einschätzungen der FATF nach einer weiteren Länderprüfung jeweils ändern. Die umfangreichen FATF-Berichte müssten also mit einem grossen Aufwand laufend analysiert werden. Dies ist dem einzelnen Finanzintermediär nicht zuzumuten. Mindestens aber müsste im Rundschreiben selbst klargestellt werden, dass für die Einschätzung auf die Zusammenfassung der FATF zu den Länderprüfberichten abgestellt werden kann (Consolidated assessment ratings FATF: www.fatfgafi.org/media/fatf/documents/4th-Round-Ratings.pdf).

2.7 In den **Randziffern 38 und 39** werden die Regelungen bei Verwendung einer qualifizierten elektronischen Signatur an das restliche Rundschreiben angeglichen. Allerdings kann in solchen Fällen auf eine Wohnsitzbestätigung sowie eine „Kontrolle der Identität" der Vertragspartei mittels Banküberweisung problemlos verzichtet werden. Denn die Personen mussten sich bei der Einholung der qualifizierten elektronischen Signatur zwangsläufig identifizieren.

Die Einschränkung auf Anbieter von Schweizer Zertifizierungsdiensten erscheint als unnötig. Zumindest sollten aus Gründen der Technologieneutralität auch qualifizierte elektronische Signaturen von Anbietern, die in der EU anerkannt sind, gleich behandelt werden.

Wir schliessen uns aus diesen Gründen dem Antrag der Schweizerischen Bankiervereinigung betreffend Streichung der Anforderung einer Wohnsitzbestätigung und einer Banküberweisung an. Hingegen sehen wir keine Notwendigkeit, Rz. 39 mit einem Zusatz analog Rz. 32 zu ergänzen. Die allgemein geltenden Bestimmungen für eine Online-Identifizierung mittels elektronischer Ausweiskopie in Rz. 31 und den dortigen Verweisen sind ausreichend reguliert.

Wir wurden vor dem Verfassen der vorliegenden Eingabe über die Stellungnahme der Schweizerischen Bankiervereinigung in Kenntnis gesetzt. Dies machte Sinn, da viele Banken Mitglieder des Schweizerischen Leasingverbandes (SLV) sind. Als Träger der SRO/SLV setzt sich der SLV deshalb seit Jahren für eine einheitliche Regulierung ein, soweit dies mit Blick auf ein Level Playing Field als sinnvoll erscheint. Dies ist mit der Regelung der Video- und Online-Identifizierung der Fall, weshalb wir die Anliegen der Schweizerischen Bankiervereinigung insgesamt unterstützen, soweit wir dies bei den einzelnen Punkten angegeben haben. Um die vorliegende Eingabe nicht unnötig auszuweiten, haben wir darauf verzichtet, die detaillierten Anträge der Bankiervereinigung zu kopieren.

Wir danken Ihnen für die Kenntnisnahme unserer Anliegen und bitten Sie um deren Berücksichtigung bei Ihren weiteren Arbeiten. Gerne stehen wir Ihnen für Rückfragen oder ergänzende Auskünfte zur Verfügung.

Mit freundlichen Grüssen

Dr. Markus Hess
Sekretär der SRO-Kommission

Dr. Cornelia Stengel
Stv. Geschäftsführerin SLV

SRO-SVV
OAR-ASA

Selbstregulierungsorganisation des SVV
Organisme d'autorégulation de l'ASA

Eidgenössische Finanzmarktaufsicht FINMA
Frau Isabel Grüninger
Laupenstrasse 27
3003 Bern

Per Mail zugestellt an:
isabel.grueninger@finma.ch

Zürich, 5. April 2018

Anhörung zur Teilrevision des FINMA Rundschreibens 2016/7 «Video- und Online-Identifizierung»

Sehr geehrte Frau Grüninger

Wir bedanken uns für die eingeräumte Möglichkeit, zur Teilrevision des FINMA-Rundschreibens 2016/7 "Video- und Online-Identifizierung" Stellung nehmen zu können und für die uns in diesem Zusammenhang gewährte Fristerstreckung.
Die SRO-SVV hat die publizierten Dokumente geprüft und in den zuständigen Gremien beraten. Sie schlägt Ihnen folgende Anpassungen vor:

Rz. 14: Prüfung von drei (statt einem) zufällig ausgewählten optischen Sicherheitsmerkmalen

Wir erachten es als sinnvoll, wenn die möglichen Ausweisdatenbanken beispielhaft aufgeführt werden.

Ergänzungsvorschlag (unterstrichene Passage): Er vergleicht das Identifizierungsdokument mit Referenzen aus einer Ausweisdatenbank (bspw. PRADO) bezüglich Sicherheitsmerkmalen, Zeichenart sowie -grösse und Layout.

Rz. 32: Deckungsgleichheit zum Erläuterungsbericht fehlt

Der letzte Teilsatz von Randziffer 32 und die diesbezüglichen Aussagen im Erläuterungsbericht (S. 10 2. Abschnitt "...neu eine Lebenderkennung (selfie with liveness detection) gefordert") sind aus unserer Sicht nicht deckungsgleich. Wir regen an, die Formulierungen zu prüfen und in weiteren Publikationen anzugleichen.

Geschäftsstelle SRO-SVV, c/o Schweizerischer Versicherungsverband SVV
Conrad-Ferdinand-Meyer-Strasse 14 | Postfach | CH-8022 Zürich | Zentrale +41 44 208 28 28 | Fax +41 44 208 28 00 | www.sro-svv.ch
Thomas Jost | thomas.jost@sro-svv.ch | Direkt +41 44 208 28 64 | Fax Direkt +41 44 208 28 43

Rz. 33: Zugelassene Länder für Überweisung von Geldern im Rahmen des Online-Identifizierungsprozesses

Wir erachten die Einschränkung, dass nur bestimmte FATF-Mitgliedstaaten im Rahmen des Online-Identifizierungsprozesses akzeptiert werden können (bei der Überweisung von Vermögenswerten) als zu einschränkend und in der Praxis schwer umsetzbar. Die Umsetzung der FATF-Standards wird in den Mitgliedstaaten regelmässig geprüft und bei Feststellen von Mängeln besteht ein genau definierter Massnahmenprozess. Es erweist sich deshalb als sachgerecht, dass alle FATF-Mitgliedstaaten akzeptiert werden können. Wir schlagen deshalb vor, dass in Rz. 33 alle FATF-Mitgliedstaaten als zugelassene Länder für die Überweisung von Gelder aufgeführt werden.

Eine differenzierte Haltung ist gemäss unserer Einschätzung zudem in der Praxis schwer umsetzbar, da die Einschätzungen regelmässig ändern und die Analyse der umfangreichen FATF-Berichte einen grossen Aufwand mit sich bringt. Mindestens müsste bei Beibehaltung der Einschränkung klargestellt werden, dass für die Einschätzung auf die Zusammenfassung der FATF zu den Länderprüfberichten abgestellt werden kann (www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf , Consolidated assessment ratings FATF).

Abschliessend möchten wir Ihnen gegenüber anregen, ob sich die Anbieter von Video- und Online-Identifizierungslösungen auf freiwilliger Basis bei der FINMA zertifizieren lassen könnten. Auf diese Weise könnte die notwendige Überwachung der Tatsache, ob einzelne Lösungen den Anforderungen im FINMA-Rundschreiben entsprechen, zentralisiert werden. Damit würde der Umfang der notwendigen Prüfungsmassnahmen durch die interessierten Finanzintermediäre wesentlich erleichtert, was einer gewissen Effizienzsteigerung gleichkommen dürfte.

Gerne hoffen wir, Ihnen mit diesen Zeilen zu dienen und stehen für weitere Auskünfte jederzeit gerne zur Verfügung.

Freundliche Grüsse

SRO-SVV

Thomas Jost
Leiter der Geschäftsstelle

Simplewealth AG
Uetlibergstrasse 38
8045 Zurich

19 March 2018

Swiss Financial Market Supervisory Authority (FINMA)
Attn: Isabel Grüninger
Laupenstrasse 27
CH-3003 Bern
isabel.grueninger@finma.ch

Dear Frau Grüninger,

1. This is a submission provided by Simplewealth AG in respect of the proposed changes to FINMA Circular 2016/7 "Video and online identification" (**Draft Circular**).

2. While we are not directly supervised by FINMA, we are supervised by VQF. VQF has adopted the current FINMA Video and Identification Circular and that current Circular applies to us. We anticipate that VQF will also adopt this Draft Circular and so we make submissions on the assumption that this Draft Circular will also apply to us.

Overview comments

3. We support FINMA's efforts to allow smarter and more efficient online identification of clients. This is positive and is required for us to assist younger clients invest for their futures.

4. We submit, however, that there should be three changes to the Draft Circular. These changes will improve the Draft Circular and assist Swiss asset managers to onboard clients faster and more efficiently. We consider that they should not increase AML risks for us.

5. The three suggested changes are:

   (a) To assist the reader of the Draft Circular, some of the information that is included in the Explanatory Note to the Draft Circular should also be included in the Draft Circular;

   (b) When onboarding a client via Online Identification, additional documents for proof of address should be permitted; and

   (c) The wording regarding the requirement for a bank transfer should be clearer that it is acceptable for a transfer to go from the client's bank account to a custodian bank account.

To assist the reader of the Draft Circular, some of the information that is included in the Explanatory Note to the Draft Circular should also be included in the Draft Circular

6. We consider that there is additional helpful information that is included in the Explanatory Note to the Draft Circular that is not included in the Draft Circular. Such information is helpful as it clarifies statements in the Draft Circular, and should be included in the Draft Circular. For example:

   (a) The Draft Circular states that at least 3 security features should be checked, provided that they can be checked in a photo. However, the Explanatory Note seems to suggest that a client should submit more than 1 photo of their identification so that the pages with the security features, photo and personal details can be checked. We suggest that the Draft Circular state that a sufficient number of photos should be provided by the client to ensure at least 3 security features are checked.

   (b) The Draft Circular states that the identification document should be checked against a database of identity documents. The Explanatory Note suggests that a suitable database is PRADO. We consider that a specific reference to PRADO (or an equivalent acceptable databases) should also be included in the Draft Circular. This is to make it clear the type of database and check that is required. Without the reference to PRADO, the Draft Circular could be interpreted to require a check against an *actual* database of identification documents, and we are not sure that there is such a publically available database.

When onboarding a client via Online Identification, additional documents for proof of address should be permitted

7. In the current Circular, and in the new Draft Circular, it is stated that a client's proof of address can be checked by a utility bill, sending something by post to the client, or checking against an official register or database.

8. We submit that there should be additional proof of address evidence permitted. A lot of our clients are "millennial" clients and do not have utility bills. This may be the case where a client is living in shared accommodation, or if the utilities are included in the rent. As an example, in the apartment I rent, all of the water, power and heating is charged to one account for our building. Those utilities are then split up according to separate meter readings. The utility invoices are not in my name and so I cannot provide a traditional "utility" invoice to prove my residential address.

9. While the option of postal confirmation is helpful, it creates a regulatory "time-block". This delays client onboarding. Younger clients favor speed and we have lost clients due to fact that there has been a time delay because we have needed to get postal confirmation.

10. We submit that the Draft Circular should specifically state that other "proof of address" is permitted. This is to assist asset managers onboard clients faster. We submit that there are also other sources of proof of address that should be acceptable. This could include, for example, copies of: letters from the client's Canton or from a Federal Agency, Billag invoices, accommodation rental agreements, bank statements or bank letters, and in the case of registered foreigners, their Ausländerausweis (as they have been checked by their Canton).

The wording regarding the requirement for a bank transfer should be clearer that it is acceptable for a transfer to go from the client's bank account to a custodian bank account

11. We support the broadening of acceptable bank accounts for bank transfers to include transfers from bank accounts in suitable FATF compliant countries.

12. We submit, however, that the Draft Circular should also be clearer that the transfer from the bank account in the name of the client can go to an account that the Financial Intermediary oversees. This could be a bank account of the Financial Intermediary, or it could be a custodial account with an independent custodian, broker or securities dealer. The important detail should be that the Financial Intermediary is able to trace the payment back to a bank account in the name of the client.

13. We make this submission because in many cases asset managers do not touch any client money. A client transfers money directly to an account controlled by a custodian, broker or securities dealer. The asset manager can see the account from where the payment came.

14. For example, Article 16 of the *Rules of Conduct of the Industry Organisation for Asset Management of the VQF Financial Services Standards Association regarding the Practice of Asset Management* states:

> *Unless the asset manager is authorised by FINMA to act as a securities dealer, he accepts no assets from the client and manages no transaction accounts. Assets entrusted to the asset manager for his management which are deposited with a bank or securities dealer are managed on the basis of clearly defined authorisation given in writing.*

15. Accordingly, we submit that asset managers in those circumstances should also be able to clearly rely on the Draft Circular.

16. If you would like to discuss any of these comments further please contact mark@simplewealth.ch.

Yours sincerely

Mark Ainsworth
Head of Legal and Compliance
Simplewealth AG

Swiss Payment Association

Ohmstrasse 11, 8050 Zürich
office@swiss-p-a.ch, +41 (0)58 426 25 55

Eidgenössische Finanzmarktaufsicht
Frau Isabel Grüninger
Laupenstrasse 27
3003 Bern

Per Mail: isabel.grueninger@finma.ch

Zürich, 21. März 2018

Anhörung zur Teilrevision des FINMA-Rundschreibens 2016/7 „Video- und Online-Identifizierung“: Stellungnahme der Swiss Payment Association

Sehr geehrte Frau Grüninger
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf das am 13. Februar 2018 eröffnete Anhörungsverfahren zur Teilrevision des FINMA-Rundschreibens 2016/7 „Video- und Online-Identifizierung“ und bedanken uns für die Möglichkeit zur Stellungnahme. Vorab gestatten wir uns den Hinweis, dass der Swiss Payment Association (SPA) alle grossen Schweizer Herausgeber[1] von Kreditkarten der internationalen Kartenorganisationen mit rund 6.6 Millionen ausgegebenen Karten angehören.

1. Grundsätzliche Ausführungen

Mit der Teilrevision des FINMA-Rundschreiben 2016/7 „Video- und Online-Identifizierung“ soll knapp zwei Jahre nach Inkrafttreten des Rundschreibens dem technischen Wandel, den erkannten Missbrauchsrisiken sowie den erfolgten Rückmeldungen aus der Finanzdienstleistungsbranche Rechnung getragen werden.

Die SPA begrüsst es, dass das Rundschreiben zeitnah an den technologischen Fortschritt und an die Anforderungen der Branche angepasst wird. Gleichzeitig gilt es aber auch zu beachten, dass einerseits in den vergangenen zwei Jahren noch keine umfassenden Erfahrungen mit dem Rundschreiben gesammelt werden konnten und dass andererseits der technische Wandel mit grossen Schritten weiter voranschreitet. Es besteht daher das Risiko, dass auch das teilrevidierte Rundschreiben schon bald wieder angepasst werden muss. Solch kurze Änderungszyklen bieten Chancen (die Regulierung ist nah an den tatsächlichen Ent-

[1] Mitglieder der Swiss Payment Association sind die Schweizer Kreditkarten-Herausgeber BonusCard.ch AG, Cembra Money Bank AG, Cornèr Bank AG, PostFinance AG, Swisscard AECS GmbH, UBS Switzerland AG und Viseca Card Services SA.

wicklungen und an Innovationen dran), sie beinhalten aber auch Risiken bzw. sind anforderungsreich für die Finanzintermediäre. So müssen in kurzen Abständen Prozesse angepasst bzw. neu gestaltet, neue Informatiklösungen bereitgestellt oder Mitarbeitende geschult werden. Das erhöht einerseits das Risiko von Fehlern und ist andererseits stets mit nicht unerheblichen Kosten verbunden. Um den Nachteilen von kurzen Änderungszyklen bei Rundschreiben entgegenzuwirken, sollte nach Auffassung der SPA generell das Prinzip verfolgt werden, dass bei Teilrevisionen bisherige Lösungen – sofern sie nicht völlig unhaltbar geworden sind – beibehalten werden und dass zusätzlich – dem technologischen Fortschritt entsprechend – neue Lösungen angeboten werden.

Die SPA begrüsst es, dass mit der aktuellen Teilrevision die Möglichkeit geschaffen wird, den Identifizierungsvorgang auch dann fortsetzen zu können, wenn Hinweise auf erhöhte Risiken vorliegen. Dies wurde bereits 2016 in mehreren Anhörungsstellungnahmen angeregt und hat nun berechtigterweise Eingang in das zu revidierende Rundschreiben gefunden.

Weiter begrüsst es die SPA, dass bei der Online-Identifizierung im Rahmen der Echtheitsprüfung eine Überweisung nicht mehr zwingend durch eine in der Schweiz domizilierte Bank vorgenommen werden muss.

Andere in Aussicht genommene Änderungen des Rundschreibens führen nach Auffassung der SPA dagegen nicht zu Verbesserungen bzw. schränken die Risikoentscheide von Finanzintermediären teilweise unnötig ein. Darauf wird unmittelbar nachstehend unter Ziffer 2 eingegangen.

2. Ausführungen zu einzelnen Randziffern / Kritikpunkte und Anträge der Swiss Payment Association

2.1 Videoidentifizierung: Identitätsprüfung (Rz 14 und Rz 16)

Im Rahmen der Videoidentifizierung wird in Rz 14 vorgeschlagen, dass der Finanzintermediär die Echtheit der Identifizierungsdokumente unter anderem anhand von mindestens drei zufällig ausgewählten optischen Sicherheitsmerkmalen zu überprüfen hat. Dies erscheint zwar grundsätzlich praktikabel, beinhaltet aus Sicht der SPA aber das Risiko, dass in Zukunft weniger Identifizierungsdokumente akzeptiert werden könnten, da allenfalls nicht alle Ausweisdokumente (auch solche neueren Datums nicht) über mehr als drei Sicherheitsmerkmale verfügen, aus denen drei zufällig ausgewählt werden können. Die SPA plädiert daher dafür, dass im Rundschreiben nicht nur eine einzige Methode zur Identitätsprüfung vorgesehen wird. Vielmehr sollen – in Anlehnung an die bisherige Rz 16 des RS – auch „ähnliche Methoden“, welche gleichermassen zuverlässig und sicher sind, zugelassen sein.

Im Weiteren bedarf die neu vorgesehene Anforderung, wonach Identifizierungsdokumente bezüglich Sicherheitsmerkmale, Zeichenart/Zeichengrösse sowie Layout mit Referenzen aus einer Ausweisdatenbank zu vergleichen sind, aus Sicht der SPA einer Flexibilisierung. Unbestritten ist, dass der Finanzintermediär eine Prüfung der Echtheit des Identifizierungsdokuments vorzunehmen und dass diese Beurteilung anhand klarer Vorgaben zu erfolgen hat. Eine zwingende Konsultation einer Ausweisdatenbank bei jeder einzelnen Identifikation ist allerdings weder angebracht noch praktikabel. Sachgerechter wäre es, dem Finanzintermediär die Entscheidung zu überlassen, anhand welcher Referenzen er die Echtheit des Identifizierungsdokuments überprüfen will, wobei er dies risikoorientiert vorzunehmen hat. Die Konsultation einer Ausweisdatenbank stellt hierzu nur eine der denkbaren und zweckmässi-

gen Möglichkeiten dar. Alternativ ist – allein schon aus Praktikabilitätsüberlegungen – die Möglichkeit zu schaffen, die Verifikation anhand von intern erlassenen Vorgaben vorzunehmen, welche z.B. ihrerseits auf einer Ausweisdatenbank basieren können. Die SPA beantragt daher, Rz 14 am Ende offener zu formulieren.

Rz 14: Von der starren Anforderung, dass bei jeder einzelnen Prüfung der Echtheit eines Identifizierungsdokuments eine Ausweisdatenbank konsultiert werden muss, ist abzusehen. Es soll eine offenere Formulierung gewählt werden, welche dem Finanzdienstleister mehr Flexibilität gewährt, anhand welcher Referenzen er die Echtheit des Identifizierungsdokuments risikobasiert überprüfen will.

Rz 16: Die bisherige Konzeption, wonach zur Identitätsprüfung nicht nur eine einzige Methode zur Verfügung steht, sondern auch „ähnliche Methoden" als genügend bzw. zulässig angesehen werden, ist beizubehalten.

2.2 Online-Identifizierung: Elektronische Ausweiskopie mit Echtheitsprüfung durch den Finanzintermediär (Rz 32 und Rz 34)

In Rz 32 soll neu verlangt werden, dass der Finanzintermediär die Echtheit des Identifizierungsdokuments anhand von mindestens drei zufällig ausgewählten optischen Sicherheitsmerkmalen beurteilt, *soweit sich diese auf einem Standbild überprüfen lassen*. Diese an die bei der Videoidentifizierung neu in Aussicht genommene Regelung angelehnte Vorschrift ist nach Auffassung der SPA klärungsbedürftig: So ist aufgrund der gewählten Formulierung unklar, ob bei der Online-Identifizierung an die Überprüfung des Ausweisdokuments weniger strenge Anforderungen als bei der Videoidentifizierung gestellt werden. Weiter ist unklar, wie zu verfahren ist, wenn das Standbild eine Überprüfung von drei Sicherheitsmerkmalen nicht zulässt. Die SPA beantragt, die erforderlichen Klärungen vorzunehmen, wobei an die Überprüfung des Standbildes des Identifizierungsdokuments keine zu hohen Anforderungen gestellt werden dürfen, da das Standbild Limitierungen aufweist. Aufgrund dieser Limitierungen sollten auch hier – in Anlehnung an die bisherige Rz 34 – „ähnliche Methoden" als zulässig angesehen werden.

Andernfalls hätte dies zur Folge, dass beispielsweise eine Identifikation mittels Schweizerischem Führerausweis im Kreditkartenformat unnötig erschwert bzw. möglicherweise verhindert würde. Der Führerausweis im Kreditkartenformat kennt als Sicherheitsmerkmale Hologramme, Mikroprint Text, sich ändernde Farben bei Kippbewegung, perlmuttartiger Glanz bei Lichteinfall sowie eine Rohlingnummer. Eine hinreichende Überprüfung von drei dieser Sicherheitsmerkmale auf einem Standbild dürfte nicht gelingen, da sich diese Merkmale mehrheitlich erst durch (Kipp-)Bewegungen respektive durch Lichteinfall auf ihre Echtheit überprüfen lassen. In solchen Fällen müsste dann eine erneute Online-Identifizierung vorgenommen werden (d.h. dem Kunden müsste mitgeteilt werden, dass die Echtheit seiner Ausweiskopie nicht bestätigt werden konnte). Dies wäre der Akzeptanz dieser wichtigen Alternative zur Einholung einer echtheitsbestätigten Ausweiskopie nicht förderlich.

Bezüglich der auch bei der Online-Identifizierung neu vorgesehenen Anforderung, das Identifizierungsdokument bezüglich Sicherheitsmerkmale, Zeichenart/Zeichengrösse sowie Layout mit Referenzen aus einer Ausweisdatenbank zu vergleichen, wird auf die entsprechenden Ausführungen zur Videoidentifizierung (Ziffer 2.1) verwiesen, welche für die Online-Identifizierung analog gelten.

Rz 32: Die in Rz 32 enthaltene Anforderung, wonach der Finanzintermediär die Echtheit des Identifizierungsdokuments anhand von mindestens drei zufällig ausgewählten optischen Sicherheitsmerkmalen beurteilt, soweit sich diese auf einem Standbild überprüfen lassen, ist zu präzisieren. Insbesondere ist das Vorgehen für den Fall zu regeln, dass das Standbild eine Überprüfung von drei Sicherheitsmerkmalen nicht zulässt.

Von der starren Anforderung, dass bei jeder einzelnen Prüfung der Echtheit eines Identifizierungsdokuments eine Ausweisdatenbank konsultiert werden muss, ist abzusehen. Es soll eine offenere Formulierung gewählt werden, welche dem Finanzdienstleister mehr Flexibilität gewährt, anhand welcher Referenzen er die Echtheit des Identifizierungsdokuments risikobasiert überprüfen will.

Rz 34: Die bisherige Konzeption, wonach zur Identitätsprüfung nicht nur eine einzige Methode zur Verfügung steht, sondern auch „ähnliche Methoden“ als genügend bzw. zulässig angesehen werden, ist beizubehalten.

2.3 Videoidentifizierung/Online-Identifizierung: Abbruch des Identifizierungsvorgangs (Rz 22 und Rz 31.2)

In den Rz 22 und 31.2 wird festgehalten, dass der Finanzintermediär den Identifizierungsvorgang auch bei Hinweisen auf erhöhte Risiken fortsetzen darf, sofern er sicherstellt, dass die Geschäftsbeziehung erst aufgenommen wird, wenn die Zustimmung einer vorgesetzten Person, einer vorgesetzten Stelle oder der Geschäftsführung gemäss Art. 18 GwV-FINMA vorliegt. Wie bereits eingangs dieser Stellungnahme angesprochen, begrüsst die SPA diese Bestimmung. Allerdings stellt sich die Frage, was im Rahmen des Identifizierungsvorgangs als "Hinweise auf erhöhte Risiken" zu verstehen ist bzw. weshalb der Aspekt der „erhöhten Risiken“ Teil des Identifizierungsprozesses sein sollte (denn die Risikokategorisierung oder der „PEP-Check“ finden nachgelagert zum Identifikationsprozess statt). Falls der Aspekt Teil des Identifizierungsvorgangs bliebe, wäre zu klären, ob eine nachgelagerte Zustimmung zur Aufnahme der Geschäftsbeziehung bereits dann erforderlich wird, wenn einzelne Kriterien vorliegen, die zur Bestimmung von Geschäftsbeziehungen mit erhöhten Risiken definiert sind, oder ob das Zustimmungserfordernis erst dann besteht, wenn die Kombination der vorliegenden Kriterien dazu führt, dass eine Beziehungen als Geschäftsbeziehungen mit erhöhten Risiken qualifiziert.

Rz 22 und 31.2: Es ist zu prüfen, ob der Aspekt der „erhöhten Risiken“ als Teil des Identifizierungsprozesses nicht systemfremd ist. Falls der Aspekt Teil des Identifizierungsvorgangs bliebe, wäre zu klären bzw. zu definieren, was im Rahmen des Identifizierungsvorgangs als "Hinweise auf erhöhte Risiken" bzw. als „erhöhte Risiken“ zu verstehen ist.

2.4 Online-Identifizierung durch geschulte Mitarbeitende

In Rz 31.1 wird verlangt, dass die Online-Identifizierung „durch entsprechend geschulte Mitarbeitende des Finanzintermediärs“ zu erfolgen habe. Diese Auflage ist problematisch, da sie im Bereich der Online-Identifizierung die Möglichkeit der end-to-end systemautomatischen Identifizierung, wie sie bereits heute technisch möglich ist, ausschliesst. Dies erachtet die SPA als unzweckmässig.

Rz 31.1 Auf das Erfordernis, dass die Online-Identifizierung durch geschulte Mitarbeitende des Finanzintermediärs zu erfolgen habe, ist zu verzichten.

Wir danken Ihnen für die Prüfung unserer Ausführungen sowie für die Berücksichtigung unserer Überlegungen. Bei allfälligen Rückfragen steht Ihnen der Rechtsunterzeichnete gerne zur Verfügung.

Freundliche Grüsse

Swiss Payment Association

Dr. Daniel Bürchler
Präsident

Dr. Thomas Hodel
Geschäftsführer

swisscom | Blockchain

A-Post
Swisscom Blockchain AG, 8005 Zürich

Eidgenössische Finanzmarktaufsicht FINMA
Frau Isabel Grüninger
Laupenstrasse 27
CH-3003 Bern

Datum	28. März 2018
Ihr Kontakt	Kerstin Hansen Kerstin.Hansen@swisscom.com +41 79 853 73 84
Thema	**Stellungnahme - Teilrevision des FINMA-Rundschreibens 2016/7 "Video- und Online-Identifizierung" ("FINMA-RS 2016/7")**

Sehr geehrte Frau Grüninger
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 13. Februar 2018 eröffnete Anhörung i.S. Teilrevision des FINMA-Rundschreibens 2016/7 "Video- und Online-Identifizierung" ("FINMA-RS 2016/7") und bedanken uns für die Möglichkeit zur Stellungnahme.

Swisscom Blockchain AG erbringt Dienstleistungen im Bereich von Blockchain Anwendungen und Initial Coin Offerings (ICO). In dieser Rolle ist die Swisscom Blockchain AG an skalierbaren und auf die Gegebenheiten von ICO zugeschnittenen Identifizierungslösungen interessiert. Als Verfechterin und Treiberin der digitalen Transformation ist Swisscom Blockchain AG ferner bestrebt, digitalisierungsfreundliche und blockchaintaugliche Rahmenbedingungen in der Schweiz zu schaffen.

Im Wesentlichen verweisen wir auf die Stellungnahme der Swisscom (Schweiz) AG, möchten aber die folgenden Aspekte besonders hervorheben:

1. Online-Identifizierung

Wir begrüssen grundsätzlich, dass neu für das Online-Identifizierungsverfahren weitgehend dieselben Anforderungen hinsichtlich der Überprüfung und des Abgleichs von Sicherheitsmerkmalen von Identifizierungsdokumenten gelten sollen wie für das Video-Identifizierungsverfahren. Dies ergibt sowohl aus prozessökonomischen Gesichtspunkten wie auch aus sicherheitstechnischen Überlegungen Sinn. Jedoch bezweifeln wir, dass holografisch-kinematische Merkmale oder Druckelemente mit Kippeffekt auf Standbildern überprüft werden können und somit einen Mehrwert bieten.

Dem Grundsatz nach einverstanden sind wir mit den neu vorgeschlagenen Anforderungen an die Erstellung des Lichtbilds der Vertragspartei im Rahmen des Identifizierungsvorgangs sowie der partiellen Öffnung von Erstüberweisungen ab gleichwertig regulierten und beaufsichtigten Bankkonten.

Wir befürworten die vorgeschlagenen Änderungen grundsätzlich, sehen in den folgenden Punkten jedoch einen Anpassungs- und/oder Präzisierungsbedarf:

a) Rz. 31.1 des teilrevidierten Entwurfs des Rundschreibens

Rz. 31.1 stellt die neue Anforderung auf, wonach "Die Online-Identifizierung [...] durch entsprechend geschulte Mitarbeitende des Finanzintermediärs" zu erfolgen hat. Gemäss der Formulierung in Entwurfsform muss davon ausgegangen werden, dass es für die Durchführung eines Online-Identifizierungsvorgangs zwingend einer menschlichen Involvierung bedarf. Nach unserer Leseart drückt die Bestimmung aus, dass ein geschulter Mitarbeiter den Identifizierungsvorgang *in persona* vornehmen bzw. zumindest nachträglich die erstellten Identifizierungsunterlagen kontrollieren muss.

Unserer Auffassung nach widerspricht der materielle Gehalt des letzten Satzes von Rz. 31.1 dem Sinn und Zweck der bewusst gewählten, geltenden Differenzierung zwischen der Video-Identifizierung nach Rz. 10 – 27 einerseits und der Online-Identifizierung nach Rz. 32 - 37 (Elektronische Ausweiskopie mit Echtheitsprüfung durch den Finanzintermediär) und nach Rz. 38 - 39 (Elektronische Ausweiskopie mit qualifizierter elektronischer Signatur) andererseits.

Bei der Verfahrensart der Video-Identifizierung wird zwingend eine persönliche Komponente in Form einer Interaktion zwischen der zu identifizierenden Person und dem Bankmitarbeitenden anlässlich eines Video-Gesprächs in Echtzeit verlangt. Ferner bedarf es eines Gesprächsleitfadens sowie einer Schulung der Mitarbeiter zur Erkennung von Verdachtsmomenten. Diese Elemente führen dazu, dass die Verfahrensart der Video-Identifikation aus rechtlicher Sicht der persönlichen Vorsprache gleichgestellt ist (vgl. Rz. 5).

Demgegenüber bedarf es bei der Online-Identifikation (nach Rz. 32 - 37 und Rz. 38 – 39 der geltenden Fassung des Rundschreibens) unter Herbeiziehung einer teleologischen Auslegung keiner Interaktion zwischen zwei Personen, womit die einzelnen Prozessschritte automatisch erfolgen können. Entsprechend ist die Online-Identifizierung aus rechtlicher Sicht nicht der persönlichen Vorsprache gleichgestellt, sondern lediglich der echtheitsbestätigten Ausweiskopie (vgl. dazu Rz. 31).

Eine explizite und zwingende menschliche Prüfung verletzt überdies das Gebot der Technologieneutralität: Die Prüfung von Vollständigkeit und Korrektheit der während des Identifizierungsvorgangs erhobenen Identifizierungsunterlagen erfordert kein menschliches Ermessen und kann deshalb ohne Weiteres systemtechnisch konfiguriert werden. Bereits heute am Markt verfügbare und entsprechend erprobte Technologien erlauben eine vollautomatische Kontrolle der im Rahmen der Online-Identifizierung und gemäss Rz. 32 beizubringenden Identifizierungsunterlagen (Abgleich der Lichtbilder von Ausweis und Vertragspartner mittels biometrischer Verfahren; Auslesen und Entschlüsseln der MRZ und anderer Ausweisattribute mittels OCR; Abgleich des Ausweises mit Ausweisdatenbank; Auslesen und Entschlüsseln der Informationen auf Adressnachweis und Abgleich mit Datenbank; etc.). Diese Technologien liefern zumindest gleichwertige oder gar qualitativ bessere und beständigere Ergebnisse als Kontrollen mit rein menschlicher Involvierung.

Darüber hinaus erlauben automatische Kontrollen die Verarbeitung von grösseren Volumen in gleicher Zeit, als wenn diese Kontrollen manuell durchgeführt werden. Dies ist insbesondere in Geschäftsfeldern relevant, in denen innert kurzer Zeit eine hohe Anzahl von Identifizierungen durchgeführt werden muss, wie z.B. bei ICOs (siehe nachfolgend Ziff. 2).

Wir sind der dedizierten Auffassung, dass die regulatorischen Leitplanken dergestalt ausgestaltet sein sollten, dass die Möglichkeit zur vollautomatischen Durchführung des Prozesses der Online-Identifizierung gewahrt bleibt bzw. ermöglicht wird, insbesondere wenn dies in gleichbleibenden oder gar geringeren operationellen Risiken resultiert. Eine menschliche Interaktion im Rahmen der Online-Identifizierung sehen wir lediglich – aber immerhin – in denjenigen Fällen vor, in denen ein automatisches Auslesen und Überprüfen der Identifizierungsunterlagen nicht möglich ist und ein manuelles Eingreifen erfordert (sog. *exception handling*) sowie allenfalls bei der Durchführung von periodischen Stichproben zur Qualitätsprüfung. Entsprechend beantragen wir die ersatzlose Streichung des letzten Satzes der Rz. 31.1.

b) Rz 31.3 des teilrevidierten Entwurfs des Rundschreibens

Wir bezweifeln, dass holografisch-kinematische Merkmale oder Druckelemente mit Kippeffekt auf Standbildern überprüft werden können und somit einen Mehrwert bieten. Wir empfehlen deshalb, den zweiten Teilsatz von Rz. 31.3 ersatzlos zu streichen.

c) Rz. 32 des teilrevidierten Entwurfs des Rundschreibens

Die Bestimmung, wonach der Finanzintermediär sicher zu stellen hat, dass das Lichtbild der Vertragspartei im Rahmen des Identifizierungsvorgangs erstellt worden ist, ist zu begrüssen. Es erhöht die Sicherheit in Bezug auf falsche Ausweise und dient der Betrugsprävention. Wir teilen die Auffassung, dass ein "Lichtbild mit Lebenderkennung" hierzu eine geeignete Variante darstellt.

Hinweisen möchten wir an dieser Stelle darauf, dass in Rz. 32 der Entwurfsversion des Rundschreibens das Kriterium der Lebenderkennung beispielhaft aufgeführt wird. Dahingegen geht aus dem dazugehörigen Erläuterungsbericht (siehe Seite 10) hervor, dass das Verfahren der Lebenderkennung zwingend ist. Hier orten wir einen Klärungs- bzw. Präzisierungsbedarf. Unter dem Aspekt der Technologieneutralität scheint uns im Übrigen wichtig, dass die Formulierung dergestalt gewählt wird, dass die Lebenderkennung mittels unterschiedlichen Methoden erfolgen kann.

Wie bereits zuvor erwähnt bezweifeln wir, dass holografisch-kinematische Merkmale oder Druckelemente mit Kippeffekt auf Standbildern überprüft werden können. Es wird dem Finanzintermediär somit auch nicht möglich sein, wie in Rz. 32 gefordert die Echtheit des Identifizierungsdokuments anhand von mindestens drei zufällig ausgewählten optischen Sicherheitsmerkmalen zu beurteilen. Der Einschub, wonach dies nur notwendig ist, soweit sich diese Sicherheitsmerkmale auf einem Standbild überprüfen lassen, führt unseres Erachtens lediglich zu Rechtsunsicherheit, z.B. bei der Formulierung von Anforderungen in Outsourcingverhältnissen oder im Rahmen der Einhalteprüfung durch die Prüfgesellschaft. Wir empfehlen deshalb, den ganzen Satz ersatzlos zu streichen.

2. Video- und Online-Identifizierung im Kontext von ICOs

Im Kontext der von der FINMA am 16. Februar 2018 veröffentlichten "Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs)" ergeben sich im Lichte der beiden Verfahrensarten der Video- und der Online-Identifizierung interessante Frage- und Problemstellungen. Aus der Wegleitung resultiert, dass ein ICO-Organisator je nach Qualifikation und Maturität der im Rahmen des ICOs herauszugebenden Tokens als Finanzintermediär qualifiziert und grundsätzlich die sich aus der Geldwäschereigesetzgebung resultierenden Sorgfaltspflichten einzuhalten hat; insbesondere also die Pflicht zur Identifizierung der Vertragspartei, zur Feststellung der wirtschaftlich be-

rechtigten Person sowie zur Abklärung der Herkunft der eingebrachten Vermögenswerte und den Hintergründen einer Transaktion.

Für die Identifizierung der Token-Zeichner kann der ICO-Organisator grundsätzlich auf die Verfahrensart der Video-Identifizierung zurückgreifen. Bei den bestehenden Anbietern von Video-Identifizierungslösungen sind zumeist mehrere Dutzend ausländische Identifizierungsdokumente hinterlegt, womit auch eine Vielzahl an Zeichner aus dem Ausland rechtsgültig identifiziert werden können. Die Identifizierung von Token-Zeichner mittels Video-Identifizierung weist in der Praxis allerdings aber auch erhebliche Nachteile auf. Dies ergibt sich aus dem Zeitfenster, das im Rahmen eines ICOs für die Identifizierung von Token-Zeichner zur Verfügung steht (i.d.R. zwischen 1 bis 3 Wochen), und der mitunter grossen Zahl von Token-Zeichner, die innerhalb dieser Frist identifiziert werden müssen. Vor dem Hintergrund, dass bei einem grösseren ICO schnell mehrere Hundert bis mehrere Tausend Zeichner identifiziert werden müssen, stösst die personenabhängige und damit zeitintensive Video-Identifizierungsmethode naturgemäss schnell an ihre Grenzen. Die dadurch entstehenden Wartezeiten würden letzten Endes zu einer Vereitelung der Identifizierung aller Token-Zeichner führen und somit auch die Durchführung von ICOs bzw. die Etablierung der Schweiz als ICO-Standort gefährden.

Hinzu kommt, dass die Kosten für die Video-Identifizierung (insbesondere im Vergleich zur Online-Identifizierung) relativ hoch sind, insbesondere im Verhältnis zu den oftmals von einzelnen Token-Zeichnern gezeichneten geringen Token-Beträgen (im Gegenwert von zumeist wenigen hundert Schweizer Franken). Der Skalierbarkeit der Video-Identifizierungslösung sind folglich enge Grenzen gesetzt.

Demgegenüber ist die Verfahrensart der Online-Identifizierung in ihrer technologieneutralen und somit automatisierbaren Form für die Identifizierung von Token-Zeichner grundsätzlich geradezu prädestiniert. Die Online-Identifizierung kann relativ kostengünstig erfolgen und lässt sich unter der Voraussetzung der automatischen Durchführung gemäss obiger Erläuterungen beliebig skalieren.

Hauptgrund, weshalb sich die Online-Identifizierung bislang im Zusammenhang mit ICOs nicht durchsetzen konnte, ist in der Teilanforderung der Überweisung eines Geldbetrages ab einem Schweizer Bankkonto zu erblicken. Mit der beabsichtigten Erweiterung des Kriteriums der Bankkontoüberweisung in geografischer Hinsicht dürfte die Online-Identifizierung im ICO-Kontext jedoch kaum an Attraktivität gewinnen. In der Praxis stellt die Fallkonstellation, wo Token-Zeichner den Zeichnungsbetrag in Fiat-Währung via Bankkonto an den ICO-Organisator überweisen, eine Ausnahme dar. Zumeist erfolgt die Überweisung des Zeichnungsbetrages in Kryptowährung (Bitcoin oder Ether).

Um die Online-Identifizierung auch für ICOs praktikabel auszugestalten regen wir bei Token-Zeichnungen mit geringem Geldwäschereirisiko bzw. bei solchen mit niedrigen Beträgen eine Erleichterung hinsichtlich des Online-Identifizierungsprozesses an: Konkret soll eine Alternative zum Teilkriterium der Überweisung eines Geldbetrages ab einem Bankkonto geschaffen werden. Anstelle der Geldüberweisung ab einem Bankkonto soll eine Hintergrundprüfung der Blockchain-Wallet vorgenommen werden, ab welcher die Bezahlung für die im Rahmen des ICOs neu geschaffenen Token erfolgt.

Die Wallet-Analyse soll Aufschluss über die Historie und die Finanzierung der einzelnen Wallets der Token-Zeichner geben und eine Risikoaussage aus Geldwäschereisicht enthalten. Die dadurch gewonnenen Informationen und Erkenntnisse erlauben einem ICO-Organisator, sich eine Risikoein-

schätzung über jeden einzelnen Token-Zeichner zu machen und entsprechende Massnahmen zu treffen. Sollte die Wallet-Analyse z.B. Hinweise dafür ergeben, dass die dem Wallet zugrundeliegenden Kryptowährungen aus verbrecherischer oder betrügerischer Handlung stammen, müsste der Identifizierungsvorgang entsprechend abgebrochen werden.

Wir sind der Überzeugung, dass die Blockchain-basierte Wallet-Analyse eine verlässliche Risikoaussage über die Herkunft der für die Token-Zeichnung aufgebrachten Vermögenswerte ergibt. Nichtsdestotrotz wird eine vollständige Gleichwertigkeit zum Kriterium der Banküberweisung schwierig zu erzielen sein. Entsprechend regen wir unter Herbeiziehung eines risikobasierten Ansatzes an, die Transaktionsanalyse zumindest bis zu einem Schwellenwert von CHF 5'000.- als Alternative zur Banküberweisung gelten zu lassen. Übersteigt der Betrag, der ein Token-Zeichner im Rahmen eines ICOs zeichnet, den Schwellenwert von CHF 5'000.-, so hat der Token-Zeichner – nebst den übrigen Elementen des Online-Identifizierungsverfahren – entweder eine Banküberweisung zu tätigen oder aber eine Video-Identifizierung gemäss den geltenden bzw. neuen Anforderungen durchzuführen.

Wir regen deshalb eine neue Rz. 33.1 an, welche bspw. wie folgt lauten könnte:

> *"Wird anstelle einer Geldüberweisung gemäss Rz. 33 eine Transaktion auf der Blockchain von bis zu CHF 5'000.- Gegenwert in Kryptowährungen vorgenommen, führt der Sorgfaltspflichtige eine Hintergrundanalyse derjenigen Blockchain Wallet durch, ab der die Transaktion durchgeführt wurde."*

*****

Zusammengefasst begrüsst die Swisscom Blockchain AG die Teilrevision des FINMA-RS 2016/7 grundsätzlich. Gleichzeitig sehen wir in auserwählten Punkten Änderungsbedarf.

Für die Prüfung unserer Anliegen danken wir Ihnen im Voraus bestens.

Freundliche Grüsse

Swisscom Blockchain AG

Daniel Haudenschild
CEO
Swisscom Blockchain AG

Sven Moeller
Head of Tokenization
Swisscom Blockchain AG

Swisscom (Schweiz) AG

Per E-Mail an:
Isabel.Grueninger@finma.ch

Eidgenössische Finanzmarktaufsicht
FINMA
Frau Isabel Grüninger
Laupenstrasse 27
CH-3003 Bern

Datum	27. März 2018	**Seite**
Ihr Kontakt	Luciano Donati / 058 223 70 73 / luciano.donati@swisscom.com	1 von 1
Thema	**Stellungnahme zur Teilrevision des FINMA-Rundschreibens 2016/7 "Video- und Online-Identifizierung"**	

Sehr geehrte Frau Grüninger
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 13. Februar 2018 eröffnete Anhörung i.S. Teilrevision des FINMA-Rundschreibens 2016/7 "Video- und Online-Identifizierung" ("FINMA-RS 2016/7") und bedanken uns für die Möglichkeit zur Stellungnahme.

Swisscom verfolgt rund um die Thematik der digitalen Identifizierung von (Bank-)Kunden ein zweifaches Interesse: Einerseits bietet Swisscom selbst eine Video-Identifizierungslösung namens *Digital Identification & Signing* ("DIS") an und betreibt dieses Verfahren für eine Vielzahl von Schweizer Banken. Andererseits ist Swisscom als Verfechterin und Treiberin der digitalen Transformation bestrebt, digitalisierungsfreundliche Rahmenbedingungen in der Schweiz zu schaffen.

1. Einleitung

Die Stellungnahme der Swisscom zum revidierten Rundschreiben Video- und Online-Identifizierung erfolgt entlang der beiden Hauptverfahrensarten gemäss Rundschreiben, der Video-Identifizierung (nachfolgend Ziff. 2) und der Online-Identifizierung (nachfolgend Ziff. 3). Unter Ziff. 4 wird auf die Thematik der Video- und Online-Identifizierung im Kontext von *Initial Coin Offerings* ("ICOs") eingegangen.

2. Video-Identifizierung

Die vorgeschlagenen Änderungen hinsichtlich der erweiterten Überprüfung und des Abgleichs von Sicherheitsmerkmalen von Identifizierungsdokumenten fördern die Erkennung von Fälschungen und

Swisscom (Schweiz) AG
Enterprise Customers
Pfingstweidstrasse 51
8005 Zürich

dienen letzten Endes der Betrugsbekämpfung. Vor diesem Hintergrund – und dem Hinweis, dass etablierte Anbieter von Video-Identifizierungslösungen bereits heute vielfältige und sophistizierte Massnahmen zur Erkennung von Fälschungen implementiert haben – befürworten wir die vorgeschlagenen Neuerungen. Und auch den weiteren Änderungen und Aufhebungen hinsichtlich des Video-Identifizierungsprozesses stehen wir neutral gegenüber.

3. Online-Identifizierung

Wir begrüssen grundsätzlich, dass neu für das Online-Identifizierungsverfahren weitgehend dieselben Anforderungen hinsichtlich der Überprüfung und des Abgleichs von Sicherheitsmerkmalen von Identifizierungsdokumenten gelten sollen wie für das Video-Identifizierungsverfahren. Dies ergibt sowohl aus prozessökonomischen Gesichtspunkten wie auch aus sicherheitstechnischen Überlegungen Sinn. Jedoch bezweifeln wir, dass holografisch-kinematische Merkmale oder Druckelemente mit Kippeffekt auf Standbildern überprüft werden können und somit einen Mehrwert bieten.

Dem Grundsatz nach einverstanden sind wir mit den neu vorgeschlagenen Anforderungen an die Erstellung des Lichtbilds der Vertragspartei im Rahmen des Identifizierungsvorgangs sowie der partiellen Öffnung von Erstüberweisungen ab gleichwertig regulierten und beaufsichtigten Bankkonten.

Ungeachtet der grundsätzlichen Befürwortung der vorgeschlagenen Änderungen sehen wir in vier ausgewählten Punkten, auf die im Folgenden einzelnen eingegangen wird, einen Anpassungs- und/oder Präzisierungsbedarf:

a) Rz. 31.1 des teilrevidierten Entwurfs des Rundschreibens

Rz. 31.1 stellt die neue Anforderung auf, wonach "Die Online-Identifizierung [...] durch entsprechend geschulte Mitarbeitende des Finanzintermediärs" zu erfolgen hat. Gemäss der Formulierung in Entwurfsform muss davon ausgegangen werden, dass es für die Durchführung eines Online-Identifizierungsvorgangs zwingend einer menschlichen Involvierung bedarf. Nach unserer Leseart drückt die Bestimmung aus, dass ein geschulter Mitarbeiter den Identifizierungsvorgang *in persona* vornehmen bzw. zumindest nachträglich die erstellten Identifizierungsunterlagen kontrollieren muss.

Unserer Auffassung nach widerspricht der materielle Gehalt des letzten Satzes von Rz. 31.1 dem Sinn und Zweck der bewusst gewählten, geltenden Differenzierung zwischen der Video-Identifizierung nach Rz. 10 – 27 einerseits und der Online-Identifizierung nach Rz. 32 - 37 (Elektronische Ausweiskopie mit Echtheitsprüfung durch den Finanzintermediär) und nach Rz. 38 - 39 (Elektronische Ausweiskopie mit qualifizierter elektronischer Signatur) andererseits.

Bei der Verfahrensart der Video-Identifizierung wird zwingend eine persönliche Komponente in Form einer Interaktion zwischen der zu identifizierenden Person und dem Bankmitarbeitenden anlässlich eines Video-Gesprächs in Echtzeit verlangt. Ferner bedarf es eines Gesprächsleitfadens sowie einer Schulung der Mitarbeiter zur Erkennung von Verdachtsmomenten. Diese Elemente führen dazu, dass die Verfahrensart der Video-Identifikation aus rechtlicher Sicht der persönlichen Vorsprache gleichgestellt ist (vgl. Rz. 5).

Demgegenüber bedarf es bei der Online-Identifikation (nach Rz. 32 - 37 und Rz. 38 – 39 der geltenden Fassung des Rundschreibens) unter Herbeiziehung einer teleologischen Auslegung keiner Interaktion zwischen zwei Personen, womit die einzelnen Prozessschritte automatisch erfolgen können.

Swisscom (Schweiz) AG
Enterprise Customers
Pfingstweidstrasse 51
8005 Zürich

Entsprechend ist die Online-Identifizierung aus rechtlicher Sicht nicht der persönlichen Vorsprache gleichgestellt, sondern lediglich der echtheitsbestätigten Ausweiskopie (vgl. dazu Rz. 31).

Eine explizite und zwingende menschliche Prüfung verletzt überdies das Gebot der Technologieneutralität: Die Prüfung von Vollständigkeit und Korrektheit der während des Identifizierungsvorgangs erhobenen Identifizierungsunterlagen erfordert kein menschliches Ermessen und kann deshalb ohne Weiteres systemtechnisch konfiguriert werden. Bereits heute am Markt verfügbare und entsprechend erprobte Technologien erlauben eine vollautomatische Kontrolle der im Rahmen der Online-Identifizierung und gemäss Rz. 32 beizubringenden Identifizierungsunterlagen (Abgleich der Lichtbilder von Ausweis und Vertragspartner mittels biometrischer Verfahren; Auslesen und Entschlüsseln der MRZ und anderer Ausweisattribute mittels OCR; Abgleich des Ausweises mit Ausweisdatenbank; Auslesen und Entschlüsseln der Informationen auf Adressnachweis und Abgleich mit Datenbank; etc.). Diese Technologien liefern zumindest gleichwertige oder gar qualitativ bessere und beständigere Ergebnisse als Kontrollen mit rein menschlicher Involvierung.

Darüber hinaus erlauben automatische Kontrollen die Verarbeitung von grösseren Volumen in gleicher Zeit, als wenn diese Kontrollen manuell durchgeführt werden. Dies ist insbesondere in Geschäftsfeldern relevant, in denen innert kurzer Zeit eine hohe Anzahl von Identifizierungen durchgeführt werden muss, wie z.B. bei ICOs (siehe nachfolgend Ziff. 4).

Von einem Menschen durchgeführte Kontrollen führen überdies zu hohen Stückkosten je durchgeführte Identifikation. Die hohen Kosten können von Finanzdienstleistern, die mit geringem Volumen und/oder mit geringer Marge operieren, nicht oder nur schwer gedeckt werden. Beispiele für entsprechende Dienstleistungszweige sind im Retail Banking und insbesondere bei technologiebasierten Dienstleistungen der Bereiche Zahlungsverkehr (*mobile Payment*, *P2P Payment*), Anlegen (*Robo Advise*) oder Finanzieren (*Crowdlending*, *Crowdfunding*) zu orten. Die im Rahmen des Entwurfs vorgeschlagene Bestimmung würde entsprechend dazu führen, dass ganze Geschäftszweige des Finanzdienstleistungssektors von digitalen Formen der Identifizierung ausgeschlossen würden.

Wir sind der dedizierten Auffassung, dass die regulatorischen Leitplanken dergestalt ausgestaltet sein sollten, dass die Möglichkeit zur vollautomatischen Durchführung des Prozesses der Online-Identifizierung gewahrt bleibt bzw. ermöglicht wird. Eine menschliche Interaktion im Rahmen der Online-Identifizierung sehen wir lediglich – aber immerhin – in denjenigen Fällen vor, in denen ein automatisches Auslesen und Überprüfen der Identifizierungsunterlagen nicht möglich ist und ein manuelles Eingreifen erfordert (sog. *exception handling*) sowie allenfalls bei der Durchführung von periodischen Stichproben zur Qualitätsprüfung. Entsprechend beantragen wir die ersatzlose Streichung des letzten Satzes der Rz. 31.1.

b) Rz 31.3 des teilrevidierten Entwurfs des Rundschreibens

Wie bereits eingangs erwähnt bezweifeln wir, dass holografisch-kinematische Merkmale oder Druckelemente mit Kippeffekt auf Standbildern überprüft werden können und somit einen Mehrwert bieten. Wir empfehlen deshalb, den zweiten Teilsatz von Rz. 31.3 ersatzlos zu streichen.

c) Rz. 32 des teilrevidierten Entwurfs des Rundschreibens

Die Bestimmung, wonach der Finanzintermediär sicher zu stellen hat, dass das Lichtbild der Vertragspartei im Rahmen des Identifizierungsvorgangs erstellt worden ist, ist zu begrüssen. Es erhöht die Sicherheit in Bezug auf falsche Ausweise und dient der Betrugsprävention. Wir teilen die Auffassung, dass ein "Lichtbild mit Lebenderkennung" hierzu eine geeignete Variante darstellt.

Swisscom (Schweiz) AG
Enterprise Customers
Pfingstweidstrasse 51
8005 Zürich

Hinweisen möchten wir an dieser Stelle darauf, dass in Rz. 32 der Entwurfsversion des Rundschreibens das Kriterium der Lebenderkennung beispielhaft aufgeführt wird. Dahingegen geht aus dem dazugehörigen Erläuterungsbericht (siehe Seite 10) hervor, dass das Verfahren der Lebenderkennung zwingend ist. Hier orten wir einen Klärungs- bzw. Präzisierungsbedarf. Unter dem Aspekt der Technologieneutralität scheint uns im Übrigen wichtig, dass die Formulierung dergestalt gewählt wird, dass die Lebenderkennung mittels unterschiedlichen Methoden erfolgen kann.

Wie bereits zuvor erwähnt bezweifeln wir, dass holografisch-kinematische Merkmale oder Druckelemente mit Kippeffekt auf Standbildern überprüft werden können. Es wird dem Finanzintermediär somit auch nicht möglich sein, wie in Rz. 32 gefordert die Echtheit des Identifizierungsdokuments anhand von mindestens drei zufällig ausgewählten optischen Sicherheitsmerkmalen zu beurteilen. Der Einschub, wonach dies nur notwendig ist, soweit sich diese Sicherheitsmerkmale auf einem Standbild überprüfen lassen, führt unseres Erachtens lediglich zu Rechtsunsicherheit, z.B. bei der Formulierung von Anforderungen in Outsourcingverhältnissen oder im Rahmen der Einhalteprüfung durch die Prüfgesellschaft. Wir empfehlen deshalb, den ganzen Satz ersatzlos zu streichen.

d) Rz. 33 des teilrevidierten Entwurfs des Rundschreibens

Wir begrüssen die vorgesehene Öffnung, dass Geldüberweisungen neu nicht mehr zwingend von einer Bank mit Sitz in der Schweiz aus verlangt werden, sondern auch Überweisungen von Banken in Liechtenstein sowie – unter bestimmten Voraussetzungen – von Banken eines FATF-Mitgliedstaates ausreichend sind. U.E. stellt die vorgesehene Öffnung die Grundvoraussetzung für die gewünschte Verbreitung des Online-Identifizierungsverfahrens dar.

Um der Verbreitung des Online-Identifizierungsverfahrens noch weiter Auftrieb zu verleihen, regen wir an, die Öffnung nicht nur in geografischer Hinsicht voranzutreiben, sondern auch weitere Zahlungsdienstleister, die nicht zwingend als Bank qualifizieren, jedoch einer in Geldwäschereibekämpfungsbelangen gleichwertigen Regulierung und Aufsicht unterstehen, mit zu erfassen. U.E. sollte es im Rahmen der Online-Identifizierung möglich sein, die verlangte Geldüberweisung auch via Kreditkarten- und *Paypal*konto durchzuführen.

4. Video- und Online-Identifizierung im Kontext von ICOs

Im Kontext der von der FINMA am 16. Februar 2018 veröffentlichten "Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs)" ergeben sich im Lichte der beiden Verfahrensarten der Video- und der Online-Identifizierung interessante Frage- und Problemstellungen. Aus der Wegleitung resultiert, dass ein ICO-Organisator je nach Qualifikation und Maturität der im Rahmen des ICOs herauszugebenden Tokens als Finanzintermediär qualifiziert und grundsätzlich die sich aus der Geldwäschereigesetzgebung resultierenden Sorgfaltspflichten einzuhalten hat; insbesondere also die Pflicht zur Identifizierung der Vertragspartei, zur Feststellung der wirtschaftlich berechtigten Person sowie zur Abklärung der Herkunft der eingebrachten Vermögenswerte und den Hintergründen einer Transaktion.

Für die Identifizierung der Token-Zeichner kann der ICO-Organisator grundsätzlich auf die Verfahrensart der Video-Identifizierung zurückgreifen. Bei den bestehenden Anbietern von Video-Identifizierungslösungen sind zumeist mehrere Dutzend ausländische Identifizierungsdokumente hinterlegt, womit auch eine Vielzahl an Zeichner aus dem Ausland rechtsgültig identifiziert werden können. Die Identifizierung von Token-Zeichner mittels Video-Identifizierung weist in der Praxis allerdings aber auch erhebliche Nachteile auf. Dies ergibt sich aus dem Zeitfenster, das im Rahmen

eines ICOs für die Identifizierung von Token-Zeichner zur Verfügung steht (i.d.R. zwischen 1 bis 3 Wochen), und der mitunter grossen Zahl von Token-Zeichner, die innerhalb dieser Frist identifiziert werden müssen. Vor dem Hintergrund, dass bei einem grösseren ICO schnell mehrere Hundert bis mehrere Tausend Zeichner identifiziert werden müssen, stösst die personenabhängige und damit zeitintensive Video-Identifizierungsmethode naturgemäss schnell an ihre Grenzen. Die dadurch entstehenden Wartezeiten würden letzten Endes zu einer Vereitelung der Identifizierung aller Token-Zeichner führen und somit auch die Durchführung von ICOs bzw. die Etablierung der Schweiz als ICO-Standort gefährden.

Hinzu kommt, dass die Kosten für die Video-Identifizierung (insbesondere im Vergleich zur Online-Identifizierung) relativ hoch sind, insbesondere im Verhältnis zu den oftmals von einzelnen Token-Zeichnern gezeichneten geringen Token-Beträgen (im Gegenwert von zumeist wenigen hundert Schweizer Franken). Der Skalierbarkeit der Video-Identifizierungslösung sind folglich enge Grenzen gesetzt.

Demgegenüber ist die Verfahrensart der Online-Identifizierung in ihrer technologieneutralen und somit automatisierbaren Form für die Identifizierung von Token-Zeichner grundsätzlich geradezu prädestiniert. Die Online-Identifizierung kann relativ kostengünstig erfolgen und lässt sich unter der Voraussetzung der automatischen Durchführung gemäss obiger Erläuterungen beliebig skalieren.

Hauptgrund, weshalb sich die Online-Identifizierung bislang im Zusammenhang mit ICOs nicht durchsetzen konnte, ist in der Teilanforderung der Überweisung eines Geldbetrages ab einem Schweizer Bankkonto zu erblicken. Mit der beabsichtigten Erweiterung des Kriteriums der Bankkontoüberweisung in geografischer Hinsicht dürfte die Online-Identifizierung im ICO-Kontext jedoch kaum an Attraktivität gewinnen. In der Praxis stellt die Fallkonstellation, wo Token-Zeichner den Zeichnungsbetrag in Fiat-Währung via Bankkonto an den ICO-Organisator überweisen, eine Ausnahme dar. Zumeist erfolgt die Überweisung des Zeichnungsbetrages in Kryptowährung (Bitcoin oder Ether).

Um die Online-Identifizierung auch für ICOs praktikabel auszugestalten regen wir bei Token-Zeichnungen mit geringem Geldwäschereirisiko bzw. bei solchen mit niedrigen Beträgen eine Erleichterung hinsichtlich des Online-Identifizierungsprozesses an: Konkret soll eine Alternative zum Teilkriterium der Überweisung eines Geldbetrages ab einem Bankkonto geschaffen werden. Anstelle der Geldüberweisung ab einem Bankkonto soll eine Hintergrundprüfung der Blockchain-Wallet vorgenommen werden, ab welcher die Bezahlung für die im Rahmen des ICOs neu geschaffenen Token erfolgt.

Die Wallet-Analyse soll Aufschluss über die Historie und die Finanzierung der einzelnen Wallets der Token-Zeichner geben und eine Risikoaussage aus Geldwäschereisicht enthalten. Die dadurch gewonnenen Informationen und Erkenntnisse erlauben einem ICO-Organisator, sich eine Risikoeinschätzung über jeden einzelnen Token-Zeichner zu machen und entsprechende Massnahmen zu treffen. Sollte die Wallet-Analyse z.B. Hinweise dafür ergeben, dass die dem Wallet zugrundeliegenden Kryptowährungen aus verbrecherischer oder betrügerischer Handlung stammen, müsste der Identifizierungsvorgang entsprechend abgebrochen werden.

Wir sind der Überzeugung, dass die Blockchain-basierte Wallet-Analyse eine verlässliche Risikoaussage über die Herkunft der für die Token-Zeichnung aufgebrachten Vermögenswerte ergibt. Nichtsdestotrotz wird eine vollständige Gleichwertigkeit zum Kriterium der Banküberweisung schwierig zu erzielen sein. Entsprechend regen wir unter Herbeiziehung eines risikobasierten Ansatzes an, die Transaktionsanalyse zumindest bis zu einem Schwellenwert von CHF 5'000.- als Alternative zur Banküberweisung gelten zu lassen. Übersteigt der Betrag, der ein Token-Zeichner im Rahmen eines

ICOs zeichnet, den Schwellenwert von CHF 5'000.-, so hat der Token-Zeichner – nebst den übrigen Elementen des Online-Identifizierungsverfahren – entweder eine Banküberweisung zu tätigen oder aber eine Video-Identifizierung gemäss den geltenden bzw. neuen Anforderungen durchzuführen.

Wir regen deshalb eine neue Rz. 33.1 an, welche bspw. wie folgt lauten könnte:

> *"Wird anstelle einer Geldüberweisung gemäss Rz. 33 eine Transaktion auf der Blockchain von bis zu CHF 5'000.- Gegenwert in Kryptowährungen vorgenommen, führt der Sorgfaltspflichtige eine Hintergrundanalyse derjenigen Blockchain Wallet durch, ab der die Transaktion durchgeführt wurde."*

*****

Zusammengefasst begrüsst Swisscom die Teilrevision des FINMA-RS 2016/7 grundsätzlich. Gleichzeitig sehen wir in auserwählten Punkten Änderungsbedarf.

Gerne stehen wir Ihnen zur Erläuterung unserer Sichtweise zur Verfügung. Für die Prüfung unserer Anliegen danken wir Ihnen im Voraus bestens.

Freundliche Grüsse

Swisscom (Schweiz) AG

Dominik Witz

Head Banking Compliance

Luciano Donati

Senior Manager Banking Compliance

Swisscom (Schweiz) AG
Enterprise Customers
Pfingstweidstrasse 51
8005 Zürich

Swissquote

Swissquote Bank SA
Head Office

Chemin de la Crétaux 33
Case postale 391
CH - 1196 Gland

T. +41 22 999 94 11
F. +41 22 999 94 12

Par courriel

Autorité fédérale de surveillance des marchés financiers FINMA
Laupenstrasse 27
3003 Berne

A l'att. de Madame Isabel Grüninger

Gland, le 27 mars 2018

Circulaire FINMA 2016/7 « Identification par vidéo et en ligne » – Projet de révision partielle du 13 février 2018

Madame,

Par ces lignes, nous saisissons l'occasion offerte par votre Autorité de participer à l'audition relative à la révision partielle de la Circulaire FINMA 2016/7 « Identification par vidéo et en ligne ». Nous saluons cette démarche tendant à faire évoluer la réglementation pour garantir la capacité d'innovation de la place financière suisse tout en assurant une gestion adéquate du risque de blanchiment. Nous apprécions aussi le fait que le principe de neutralité technologique soit un élément clé des considérations de votre Autorité.

A. Commentaires généraux

Avant de commenter une partie des modifications proposées, nous souhaitons revenir sur le contexte de la digitalisation du secteur financier et en particulier sur l'importance que prend l'entrée en relation d'affaires par vidéo ou en ligne.

Sans contester la présentation faite dans le Rapport explicatif[1] concernant le taux de pénétration de l'entrée en relation par vidéo ou en ligne auprès des banques, nous souhaitons apporter un regard plus nuancé. Pour notre établissement, les entrées en relation d'affaires « digitales » ont représenté – pour les 6 derniers mois – plus de 55% du total des nouvelles relations d'affaires ; env. 30% des entrées en relation d'affaires digitales se sont faites par vidéo et env. 70% en ligne, celles-ci ayant souvent la

[1] *« Environ une douzaine de banques en Suisse utilisent la vérification d'identité par vidéo avec succès. La plupart en limitent l'usage à la clientèle suisse. Le nombre de contrats conclus est encore faible (approximativement 6 % au plus des nouvelles ouvertures). A quelques exceptions près, les banques s'appuient sur des prestataires externes qui proposent la vérification d'identité par vidéo et/ou en ligne en guise de modèle d'affaires. La vérification d'identité en ligne ne s'est pas imposée jusqu'à présent auprès des banques comme alternative à la vérification d'identité par vidéo. L'onboarding numérique des clients est généralement très important pour les prestataires de services financiers transfrontières et plus particulièrement pour les prestataires en matière des Fintech. »*, p. 6 du Rapport.

faveur des clients car perçues comme plus *user-friendly*. Par ailleurs, le fait que, pour certaines banques, ces entrées en relation d'affaires digitales soient actuellement principalement offertes à la clientèle suisse peut sans doute s'expliquer par le modèles d'affaires desdites banques, ainsi que par l'effet de l'actuel cm. 33 de la Circulaire FINMA 2016/7 qui, en limitant le caractère probant du transfert initial à ceux qui proviennent de banques suisses, ont certainement eu une incidence importante sur les statistiques. Pour ce qui concerne notre établissement, la situation est plus contrastée au sujet de l'entrée en relation par vidéo, qui est utilisée par des clients potentiels provenant de nombreux pays différents. Nous notons également que la solution vidéo de notre établissement a été développée à l'interne et ne repose donc pas sur des prestataires externes.

Parallèlement au fort développement des ouvertures par vidéo et en ligne, nous n'avons pas constaté d'augmentation des tentatives de fraude. D'une manière générale, un renforcement des mesures de lutte contre la fraude ne nous semble donc ni nécessaire, ni opportun.

Pour compléter ces commentaires généraux, nous soulignons l'importance d'atteindre le but fixé par votre Autorité elle-même en matière de neutralité technologique. La technologie évolue de façon importante et rapide. C'est pourquoi il est primordial que les règles émises se concentrent sur la définition de principes généraux permettant de réduire les risques en évitant d'être par trop influencées par les solutions informatiques existant au moment de l'adoption desdites règles.

B. Commentaires spécifiques

Concernant les modifications proposées, nous avons identifié quatre sujets que nous commentons ci-après.

1. Identification par vidéo – Renforcement des mesures de contrôle (cm. 14)

En général

Le cm. 14 exige désormais le contrôle de trois éléments de sécurité optiques (au lieu d'un jusqu'à présent) ainsi qu'une mesure de contrôle nouvelle (la comparaison avec une base de données). Cela traduit un renforcement marqué des mesures de contrôle sans qu'il ne soit allégué ni démontré que le niveau de fraudes ou de tentatives de fraudes en matière d'entrée en relation par vidéo aurait atteint un niveau tel que les exigences actuelles devraient être renforcées.

Eléments de sécurité optiques

Notre expérience (étude empirique sur une vingtaine de pays) montre que les passeports des pays suivants ne permettent pas de vérifier à l'œil nu trois éléments de sécurité optiques dans le cadre d'une vidéo-conférence, ce même si la qualité de la vidéo-conférence est très bonne : France, Israël, Italie, Malaisie, Mexique, Norvège, Royaume-Uni, Taiwan et Turquie. Si on considère les cartes d'identité émises par cette vingtaine de pays, la situation est encore plus nette : seuls l'Allemagne, l'Espagne et l'Ukraine émettent des cartes d'identité contenant trois éléments de sécurité optiques pouvant être vérifiés à l'œil nu dans le cadre d'une vidéo-conférence et les cartes d'identité suisses, par exemple, ne seraient pas utilisables.

Par conséquent, l'augmentation de l'examen des éléments de sécurité optiques d'un à trois ne nous apparaît ni justifiée (cf. les développements ci-dessus), ni praticable. En effet, même pour les documents contenant suffisamment d'éléments de sécurité optiques, le contrôle ne sera souvent pas possible sans recours à des outils techniques actuellement disponibles de façon limitée. Or, la Circulaire FINMA 2016/7 autorise un examen visuel de ces éléments et l'obligation de recourir à de tels outils semble difficilement compatible avec le principe de neutralité technologique qui devrait prévaloir[2].

[2] Des fournisseurs semblent proposer des outils informatiques permettant de faire certains contrôles en la matière. Voir en particulier ID Now qui, sur son site, se prévaut de sa collaboration avec la FINMA : https://www.idnow.eu/press/finma-increases-security-for-online-identification/

Comparaison systématique avec une base de données

Concernant le contrôle systématique avec une base de données relative aux documents d'identification qui est introduite à la fin du cm. 14, on peut s'interroger quant à la compatibilité de cette exigence avec le principe de neutralité technologique, dès lors que les règles applicables à la vérification d'identité en cas d'entrée en relation d'affaires par pourparlers ou par correspondance, pas plus que celles applicables à l'émission d'attestation d'authenticité, n'ont jamais imposé des exigences de contrôle aussi détaillées.

D'un point de vue opérationnel, la comparaison systématique avec une base de données constitue un alourdissement important de la procédure, dès lors que ce contrôle devrait pouvoir être effectué manuellement afin d'en assurer sa neutralité technologique. Or, les collaborateurs en charge du contrôle des entrées en relation d'affaires par vidéo ont une bonne connaissance des structures, types et particularités des documents d'identification usuels et cela leur permet d'identifier d'éventuels cas douteux sans recourir systématiquement à une base de données. Ce n'est que pour ces cas douteux qu'ils vont effectuer une comparaison avec une base de données.

Le recours à une telle comparaison devrait donc être réservé aux contrôles supplémentaires en cas de doute et non imposé de façon systématique.

La remarque faite à propos du manque de neutralité technologique formulée à propos des éléments de sécurité optiques vaut également ici. Afin d'avoir un texte pérenne et conforme au principe de neutralité technologique, il conviendrait de faire de la comparaison avec une base de données relative aux documents d'identification un moyen de contrôle parmi d'autres.

C'est pourquoi nous proposons que le cm. 14 soit reformulé ainsi :

> Par ailleurs, l'intermédiaire financier contrôle l'authenticité ~~des pièces d'identité~~ des documents d'identification, d'une part au moyen de la lecture et du déchiffrage des informations contenues dans la MRZ et, d'autre part, à l'aide ~~de d'au moins trois~~ l'une des ~~marques~~ de l'un des éléments de sécurité optiques ~~variables~~ du document d'identification (par exemple kinégramme) ~~choisis de manière aléatoire~~. Ce dernier contrôle peut être réalisé au moyen d'un support technique ou de manière visuelle (par exemple en inclinant la pièce d'identité). L'intermédiaire financier vérifie que les informations décryptées concordent avec les autres données figurant sur ~~la pièce d'identité~~ le document d'identification et avec celles fournies par le cocontractant lors de l'ouverture de la relation d'affaires. ~~Il compare le document d'identification avec les références d'une banque de données relative aux documents d'identité concernant les éléments de sécurité, le type et la taille de caractères ainsi que la structure.~~
>
> Si l'intermédiaire financier a un doute quant au type, à la structure, aux éléments de mise en page ou aux éléments de sécurité du document d'identification présenté, il procède à un contrôle supplémentaire (par exemple en comparant le document d'identification avec les références d'une base de données relative aux documents d'identification).

2. Identification en ligne – Vérification du document d'identification (cm. 32)

Eléments de sécurité optiques

Par analogie à l'un des contrôles figurant au cm. 14 concernant l'identification par vidéo, le cm. 32 exige désormais que, pour l'identification en ligne, « L'intermédiaire financier évalue l'authenticité du document d'identification à l'aide d'au moins trois éléments de sécurité optiques choisis de manière aléatoire, pour autant qu'ils puissent être contrôlés sur une image fixe. »

Outre le fait que l'augmentation des exigences n'est pas justifiée (cf. commentaire au ch. 1 ci-dessus), cette nouvelle exigence, importée de l'identification par vidéo, pose un problème pratique dans le sens que la plupart des éléments de sécurité optiques ne peuvent précisément pas être contrôlés sur une image fixe. Par principe, appliquer le même contrôle reposant sur des éléments optiques dynamiques à l'examen d'une image fixe ne semble pas pertinent.

Nous avons fait une étude empirique sur les documents d'identification – passeports et cartes d'identité – des pays du GAFI et somme arrivés à la conclusion qu'aucun d'entre eux ne permet de vérifier visuellement trois éléments de sécurité optiques sur une image fixe.

Par conséquent, cette exigence devrait être abandonnée pour être remplacée par un examen des éléments visuels qui peuvent être contrôlés sur une image fixe (par exemple type, structure, éléments de mise en page, éléments de sécurité du document d'identification).

Comparaison systématique avec une base de données

Cf. nos développements au ch. 1. ci-dessus.

Exigence relative à la qualité de la photo (selfie with liveness detection)

Comme développé au ch. 1. ci-dessus, il n'est ni allégué ni démontré que le niveau de fraudes ou de tentatives de fraudes en matière d'entrée en relation par vidéo ou en ligne aurait atteint un niveau tel que les exigences actuelles devraient être renforcées. Il conviendrait de laisser le choix des mesures de contrôle aux intermédiaires financiers.

Le recours à la reconnaissance du caractère vivant de la photo (*selfie with liveness detection*) devrait être un moyen de contrôle parmi d'autres, qui serait réservé en cas de doute et non imposé de façon systématique. Comme pour la base de données relative aux documents d'identification, une formulation générale permettrait d'avoir un texte pérenne et conforme au principe de neutralité technologique.

C'est pourquoi nous proposons que le cm. 32 soit reformulé ainsi :

> L'intermédiaire financier se procure auprès du cocontractant des photographies de toutes les pages importantes de son document d'identification et de la personne même. Il vérifie que la photographie établie concorde avec la photographie du document d'identification. ~~et compare le document d'identification avec des références d'une banque de données relatives aux documents d'identité concernant les éléments de sécurité, le type et la taille de caractères ainsi que la structure. L'intermédiaire financier se procure auprès du cocontractant des photographies de sa pièce d'identité et de la personne même.~~ A l'aide de supports techniques appropriés qui permettent au minimum la lecture et du déchiffrage des informations contenues dans la MRZ et de les comparer avec les autres informations figurant sur la pièce d'identité, l'intermédiaire financier vérifie que les informations décryptées concordent avec les autres données figurant sur la pièce d'identité et avec celles fournies par le cocontractant lors de l'ouverture de la relation d'affaires. L'intermédiaire financier évalue l'authenticité du document d'identification en examinant son type, sa structure, les éléments de mise en page ou les éléments de sécurité. S'il a un doute, il procède à un contrôle supplémentaire (par exemple en comparant le document d'identification avec les références d'une base de données relative aux documents d'identification).
>
> Si l'intermédiaire financier a un doute concernant la photographie, il demande à en recevoir une nouvelle, dans une qualité qui lui permette de s'assurer de son actualité (par exemple *selfie with liveness detection*).~~à l'aide d'au moins trois éléments de sécurité optiques choisis de manière aléatoire, pour autant qu'ils puissent être contrôlés sur une image fixe. L'intermédiaire financier s'assure en outre que la photographie du cocontractant a été prise dans le cadre de la procédure de vérification d'identité, par exemple par une reconnaissance du caractère vivant (*selfie with liveness detection*).~~

3. Identification en ligne – Premier virement comme moyen de contrôle – Elargissement à d'autres pays (cm. 33)

En général

L'élargissement de la condition du contrôle par le premier virement à d'autres pays que la Suisse est bienvenu. Ce d'autant plus qu'il s'agit d'une mesure de contrôle courante en matière d'entrée en relation en ligne, efficiente et facile à mettre en œuvre pour les clients ainsi que pour les intermédiaires financiers.

Conditions mises à l'élargissement

De façon générale, la référence directe dans une circulaire de la FINMA à des résultats de travaux du GAFI ne nous semble pas opportune. La situation est en effet différente des cas où des notions (pays membre par exemple), des définitions, voire des extraits des Recommandations du GAFI, sont inclus, dès lors qu'il s'agit de standards réglementaires[3]. Comme indiqué en introduction, il faudrait préférer des formulations plus générales, permettant une mise en œuvre adaptée en fonction du type d'intermédiaire financier et de son profil de risque.

Le texte proposé élargit certes le cercle qui était jusqu'à présent limité à la Suisse, mais il continue d'être particulièrement restrictif en cumulant diverses conditions :

- pays membre du GAFI,
- n'ayant pas de cotation NC aux Recommandations relatives à la *customer due diligence* et aux *wire transfers*,
- qui, s'il a été évalué selon la dernière méthodologie (4ème round d'évaluations mutuelles), n'a pas de cotation *low* en ce qui concerne les *immediate outcomes* 3 (*supervision*) et 4 (*preventive measures*) dans le cadre de l'évaluation mutuelle du GAFI.

Il ressort des informations publiées par le GAFI que seul un tiers des pays membres du GAFI ont été évalués selon la dernière méthodologie et ont vu leur rapport d'évaluation mutuelle publié. La formulation du cm. 33 laisse un doute quant à la façon de traiter les deux tiers restants, même si elle laisse entendre que l'absence d'une évaluation mutuelle selon la dernière méthodologie n'entraîne pas la disqualification du pays en question pour le besoin du premier virement comme moyen de contrôle. Par ailleurs, nous notons que, par exemple, l'Islande, le Japon et la Nouvelle-Zélande ont été jugés non-compliant sur l'une ou l'autre des recommandations pertinentes lors de la 3ème évaluation (parfois il y a de nombreuses années) et n'ont pas encore eu d'évaluation mutuelle selon la dernière méthodologie ; l'exclusion du Japon montre que la référence directe à des résultats de travaux du GAFI n'aboutit pas nécessairement à des résultats probants. Les considérations *cross-border* sont évidemment réservées.

L'approche proposée dans la circulaire révisée exclut par ailleurs d'autres juridictions non-membres du GAFI, alors même que celles-ci auraient passé avec succès des évaluations faites selon la méthodologie GAFI, ce qui pourrait être vérifié de façon ciblée, dès lors que cela concerne la vérification de l'identité du cocontractant et l'indication du donneur d'ordre.

La réglementation anti-blanchiment connaît déjà la notion de « surveillance prudentielle et réglementation adéquates en matière de lutte contre le blanchiment d'argent et le financement du terrorisme » pour justifier l'application de certaines exceptions. On pourrait s'appuyer sur cette pratique pour déterminer le cercle des pays éligibles au titre du cm. 33. L'enjeu est de déterminer si la banque étrangère est assujettie à une surveillance prudentielle et à une réglementation adéquate en matière de lutte contre le blanchiment d'argent et le financement du terrorisme, en particulier sous l'angle de la vérification de l'identité du cocontractant et de l'indication du donneur d'ordre. Le fait d'être membre du GAFI et la référence aux travaux du GAFI (évaluations mutuelles) et à leurs résultats (cotation) restent évidemment des outils utiles pour pouvoir répondre à cette question. Si un

[3] Cf. aussi les problèmes de pérennité de terminologie avec l'exemple du projet de révision de l'OBA-FINMA qui se réfère aux « pays à haut risque ou non-coopératif », terminologie remplacée par celle de « Juridictions à hauts risques et juridictions sous surveillance ».

intermédiaire financier souhaite élargir l'application de cette condition à d'autres juridictions (non-membres du GAFI par exemple), il lui reviendrait de démontrer sur quelle base il s'appuie pour le faire.

Une telle approche se justifierait d'autant plus que, dans le cadre de l'évolution réglementaire et du développement des technologies dans le secteur financier, les principes d'égalité de traitement et de neutralité technologique sont fréquemment évoqués et appliqués. Or, pour l'entrée en relation d'affaire par correspondance, qui présente de grandes similitudes avec l'entrée en relation d'affaires en ligne, l'OBA-FINMA (art. 49) et la CDB (art. 11 et son Commentaire) indiquent que l'attestation d'authenticité du document d'identification – sur laquelle l'intermédiaire financier basera son contrôle – peut être émise par un intermédiaire financier « assujetti à une surveillance et à une réglementation équivalentes en matière de lutte contre le blanchiment d'argent et le financement du terrorisme ».

Cette notion d'équivalence est notamment présente dans les textes correspondants de la JMLSG Guidance, revue en profondeur en 2017, pour le Royaume-Uni[4] et de la Guideline on Anti-Money Laundering and Counter-Terrorist Financing (For Authorized Institutions), dans sa dernière version qui date de mars 2015, pour Hong Kong[5].

C'est pourquoi nous proposons que le cm. 33 soit reformulé ainsi :

> En outre, l'intermédiaire financier demande au cocontractant d'effectuer un virement d'argent en sa faveur ou en faveur de la banque dépositaire à partir d'un compte libellé au nom du cocontractant auprès d'une banque en Suisse ou au Liechtenstein. Au lieu d'un compte dans une banque en Suisse ou au Liechtenstein, un compte auprès d'une banque assujettie à une surveillance prudentielle et à une réglementation adéquates en matière de lutte contre le blanchiment d'argent et le financement du terrorisme est également suffisant. ~~dans un Etat membre du Groupe d'action financière (GAFI) est également suffisant, pour autant que cet Etat n'ait pas été noté not compliant en ce qui concerne les recommandations relatives à la customer due diligence et aux wire transfers ni low en ce qui concerne les immediate outcomes 3 (supervision) et 4 (preventive measures) dans le cadre de l'évaluation mutuelle du GAFI.~~

4 *"The additional verification check may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures, or may include:*
- requiring the first payment to be carried out through an account in the customer's name with a UK or EU regulated credit institution, or an assessed low risk jurisdiction."
(The Joint Money-Laundering Steering Group: Prevention of money laundering/combating terrorist financing, Guidance for the UK Financial Sector, 2017 Revised Version (Part I, Customer Due Diligence/ Private Individuals/ Obtain standard evidence/ Mitigation of impersonation Risk / para. 5.3.90)
La notion de *Assessed Low Risk Jurisdiction* figure quasi-systématiquement au côté des mentions UK, EU (voire EEA) pour les exceptions en matière d'application des règles de due diligence dans la JMLSG Guidance. Cela constitue une forme d'équivalent de la notion suisse de *« réglementation en matière de lutte contre le blanchiment d'argent et le financement du terrorisme et à une surveillance prudentielle adéquates »* (OBA-FINMA) ou *« surveillance prudentielle et à une réglementation en matière de lutte contre le blanchiment d'argent et le financement du terrorisme adéquates »* (CDB).

5 *"The AMLO requires an FI to take additional measures to compensate for any risk associated with customers not physically present for identification purposes. If a customer has not been physically present for identification purposes, the FI must carry out at least one of the following measures to mitigate the risks posed: (...)*
(c) ensuring that the first payment made into the customer's account is received from an account in the customer's name with an authorized institution or a bank operating in an equivalent jurisdiction that has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 and is supervised for compliance with those requirements by a banking regulator in that jurisdiction."
(Guideline on Anti-Money Laundering and Counter-Terrorist Financing (For Authorized Institutions), Hong Kong Monetary Authority, mars 2015, para. 4.12.2)

4. Identification par vidéo et en ligne – En présence d'éléments de risque accru (cm. 22 et 31.2)

Nous saluons le fait qu'à l'obligation de suspendre la procédure d'entrée en relation par vidéo en cas d'élément de risque accru, se substitue une exigence déjà connue de la réglementation anti-blanchiment, à savoir celle de l'art. 18 OBA-FINMA, ce qui va dans le sens de la neutralité technologique.

En vous remerciant par avance de l'attention que vous porterez à la présente, nous vous adressons, Madame, nos salutations distinguées.

Swissquote Bank SA

Paolo Buzzi
Chief Technology Officer

Morgan Lavanchy
Chief Legal Officer

Verband Schweizerischer Kantonalbanken
Union des Banques Cantonales Suisses
Unione delle Banche Cantonali Svizzere

Geschäftsstelle

Wallstrasse 8
Postfach
CH-4002 Basel

Telefon 061 206 66 66
Telefax 061 206 66 67
E-Mail vskb@vskb.ch

Eidgenössische Finanzmarktaufsicht FINMA
Isabel Grüninger
Laupenstrasse 27
CH-3003 Bern
isabel.grueninger@finma.ch

Datum 27. März 2018
Kontaktperson Marilena Corti
Direktwahl 061 206 66 21
E-Mail m.corti@vskb.ch

Teilrevision des FINMA-Rundschreibens Anhörung: 2016/7 «Video- und Online-Identifizierung»

Sehr geehrte Frau Grüninger

Am 13. Februar 2018 hat die Eidgenössische Finanzmarktaufsicht (FINMA) die Anhörung zur Teilrevision des FINMA-Rundschreibens Anhörung: 2016/7 «Video- und Online-Identifizierung» eröffnet. Wir danken Ihnen bestens für die Gelegenheit zur Stellungnahme. Die Kantonalbanken haben sich mit der Vernehmlassung befasst und ihre Anliegen in die Schweizerische Bankiervereinigung (SBVg) eingebracht. Wir werden somit die Stellungnahme der SBVg unterstützen.

Ergänzend gilt es zu bedenken, dass das Rundschreiben «Video- und Online-Identifizierung» bereits sehr kurze Zeit nach Inkrafttreten revidiert wird. Dies führt dazu, dass kürzlich implementierte Prozesse insbesondere bei den vorgesehenen zusätzlichen Anforderungen (Überprüfung von mindestens drei zufällig ausgewählten optischen Sicherheitsmerkmalen im Rahmen der Video-Identifizierung), bereits wieder angepasst werden müssen, ohne dass eine zwingende Notwendigkeit besteht. Sollte auf die obengenannten, zusätzlichen Anforderungen nicht verzichtet werden, müssten zumindest grosszügige Übergangsfristen gewährt werden. Eine Übergangsfrist von sechs Monaten für die Anpassung der IT-Prozesse, die teilweise erst seit wenigen Monaten operativ sind, würde nicht genügen.

Wir danken Ihnen bestens für die Kenntnisnahme.

Freundliche Grüsse

Verband Schweizerischer Kantonalbanken

Hanspeter Hess
Direktor

Dr. Adrian Steiner
Leiter Public Affairs

Verband Schweizerischer Vermögensverwalter I VSV
Association Suisse des Gérants de Fortune I ASG
Associazione Svizzera di Gestori di Patrimoni I ASG
Swiss Association of Asset Managers I SAAM

Eidgenössische Finanzmarktaufsicht
FINMA
Isabel Grüninger
Laupenstrasse 27
3003 Bern

Zürich, 27. März 2018

Per Email: isabel.grueninger@finma.ch

Anhörung: FINMA-Rundschreiben 2016/7 «Video- und Online-Identifizierung» - Teilrevision

Sehr geehrte Frau Grüninger, sehr geehrte Damen und Herren

Wir nehmen Bezug auf Ihre Einladung vom 13. Februar 2018 zur Anhörung betreffend Teilrevision des FINMA-Rundschreibens 2016/7 «Video- und Online-Identifizierung» und möchten uns für diese Gelegenheit bedanken.

Zur Vorlage nimmt der VSV als führender nationaler Branchenverband der unabhängigen Vermögensverwalter («UVV») wie folgt Stellung:

I. Zum Inhalt der vorliegenden Stellungnahme

Die vorliegende Stellungnahme beschränkt sich auf diejenigen Themenbereiche, welche die Tätigkeit der UVV in der Schweiz direkt betreffen.

Wichtig ist dem VSV dabei vor allem auch, dass die Möglichkeiten der Anwendung zugelassener technologie-basierter Verfahren und Methoden auch den Kleinst- und Kleinunternehmen im Finanzsektor offensteht und die Beschreibung des Zugelassenen und dessen Grenzen hinreichend klar dargestellt sind.

Bahnhofstrasse 35
CH-8001 Zürich
Tel. 044 228 70 10
Fax 044 228 70 11
info@vsv-asg.ch
www.vsv-asg.ch

Chantepoulet 12
CH-1201 Genève
Tél. 022 347 62 40
Fax 022 347 62 39
info@vsv-asg.ch
www.vsv-asg.ch

Via Landriani 3
CH-6900 Lugano
Tel. 091 922 51 50
Fax 091 922 51 49
info@vsv-asg.ch
www.vsv-asg.ch

II. Zur Anhörungsvorlage im Einzelnen

1. Identitätsprüfung Videoidentifizierung

Die Ergänzung in Rz. 14 betreffend Überprüfung der Identifizierungsdokumente mittels mindestens drei zufällig ausgewählten optischen Sicherheitsmerkmalen zur Gewährleistung einer sicheren Identifizierung und zur Erschwerung der Verwendung gefälschter Ausweise erachten wir grundsätzlich als sinnvoll. Allerdings weisen wir darauf hin, dass nicht unnötig hohe Anforderungen zur Überprüfung der Identifizierungsdokumente vorgeschrieben werden sollen, so dass faktisch gesehen eine Videoidentifizierung insbesondere für Kleinst- und Kleinunternehmen im Finanzsektor, insbesondere auch für neue Fintech-Anbieter, finanziell und ressourcenmässig kaum mehr zu bewältigen wäre.

Der Vergleich des Identifizierungsdokuments mit Referenzen aus einer Ausweisdatenbank bezüglich Sicherheitsmerkmalen, Zeichenart sowie -grösse und Layout (Rz. 14) stellt eine taugliche Variante zur Erhöhung der Sicherheit bei der Überprüfung dieser Merkmale dar. Das Erfordernis darf aber nicht dazu führen, zusätzlich unverhältnismässig hohe Kosten für einen Zugang zu privaten Datenbanken zu generieren. Öffentlich zugängliche und kostenlose Online-Register müssen als Prüfstandard genügen.

Aufgrund des geringen Nutzens einer Verifizierung der Identität der Vertragspartei mittels einer TAN bei der Videoidentifikation kann die Rz. 16 gestrichen werden.

Für die Verifikation der Vertragspartei im Identifizierungsprozess bei der Onlineidentifikation jedoch soll das bestehende Verfahren der TAN weiterhin möglich sein (vgl. dazu nachfolgend Ziff. 3 lit. b).

2. Abbruch des Identifizierungsvorgangs

Die Aufhebung von Rz. 20 und die entsprechende Anpassung in Rz. 22 begrüssen wir. Dadurch erfährt die Videoidentifizierung eine Angleichung an die Identifizierung bei persönlicher Vorsprache.

3. Online-Identifizierung mittels elektronischer Ausweiskopie

a. Allgemein

Die formelle Konkretisierung und Vervollständigung der Vorgaben durch das Einfügen der Rz. 31.1 bis 31.4 begrüssen wir.

b. Elektronische Ausweiskopie mit Echtheitsprüfung durch den Finanzintermediär

Die Beurteilung der Echtheit des Identifizierungsdokuments anhand von mindestens drei zufällig ausgewählten optischen Sicherheitsmerkmalen bei der Onlineidentifizierung ist nicht zielführend, die Übereinstimmung des erstellten Lichtbilds der Vertragspartei mit dem Lichtbild des Identifizierungsdokuments und der Abgleich mit Referenzen aus einer Ausweisdatenbank bezüglich Sicherheitsmerkmalen reicht völlig aus.

Die zusätzliche, neue Pflicht sicherzustellen, dass das Lichtbild der Vertragspartei im Rahmen des Identifizierungsvorgangs erstellt worden ist (beispielsweise durch eine Lebenderkennung) ist nicht praktikabel und wieder zu streichen.

Wie genau soll eine «Lebenderkennung» in der Praxis aussehen? Der Begriff ist nicht eindeutig und klar formuliert. Aus dem Rundschreiben geht auch nicht klar hervor, was mit einer «Lebenderkennung» effektiv gemeint ist. Neue in der nahen Vergangenheit aufgetauchte Techniken wie zum Beispiel das «Live-Foto» sind für die beabsichtigte Erhöhung der Sicherheit der Echtheitsprüfung untaugliche Mittel. Den Kunden vorgängig zu bitten, den kleinen Finger neben seinen Kopf zu halten und ein Foto zu schiessen, ist auch keine (kundenfreundliche) Option.

Der bisherige Prozess mit der Generierung einer TAN ist aus unserer Sicht genügend und hat sich über die letzten Jahre bewährt. Der Kontaktkanal kann damit eindeutig verifiziert werden.

Es soll entsprechend daran festgehalten werden.

Im Weiteren weisen wir darauf hin, dass sich die neue Technik des «Live-Fotos» in der Praxis gar noch nicht durchgesetzt hat. Werden solche kurzfristigen Trends ohne eigentliche Etablierung in der Praxis zu früh als Standards in die Regulierung eingebaut, wird dem prioritären Ansatz der Technologieneutralität nicht mehr entsprochen.

Es wird begrüsst, dass die Überweisung unter gewissen Voraussetzungen auch von einer Bank ausserhalb der Schweiz erfolgen kann. Allerdings erachten wir es als wichtig, dass die Qualitätsanforderungen klar festgehalten werden, um einen gewissen Minimum-Standard garantieren zu können.

c. Digitale Echtheitsbestätigung

Die in Rz. 40 vorgenommene Streichung begrüssen wir. Wie bereits in unserer Stellungnahme vom 18. Januar 2016 zum Entwurf für ein neues FINMA-Rundschreiben 2016/xx «Video- und Onlineidentifizierung» festgehalten, kann eine Datei nicht «zu den Akten» genommen werden.

Abschliessend möchten wir uns nochmals für die Möglichkeit bedanken, zur Teilrevision des FINMA-Rundschreibens 2016/7 «Video- und Online-Identifizierung» Stellung zu nehmen. Für Rückfragen stehen Ihnen die Unterzeichneten gerne zur Verfügung.

Freundliche Grüsse

Verband Schweizerischer Vermögensverwalter | VSV

RA lic. iur. Alexander Rabian
Vorsitzender der Geschäftsleitung SRO

lic. iur. Ralph Frey
Mitglied der Geschäftsleitung
Leiter der Hauptniederlassung