RA Lea Hungerbühler & Joanna Freiermuth
AsyLex
Gotthardstrasse 52
8002 Zürich
info@asylex.ch
+41 79 746 71 82

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

Zürich, 29.01.2021

Stellungnahme bezüglich der Teilrevision des FINMA Rundschreibens zur Video- und Online-Identifizierung

Sehr geehrte Frau Grüninger

Im Namen des Vereins AsyLex bedanken wir uns für die Möglichkeit zur Stellungnahme zu der vorgesehenen Teilrevision des FINMA Rundschreibens zur Video- und Online Identifizierung.

Nachfolgend finden Sie unsere detaillierte Stellungnahme. Wir bedanken uns für die Kenntnisnahme und bitten Sie, unsere Anliegen zu berücksichtigen.

Mit freundlichen Grüssen

RA Lea Hungerbühler
CEO AsyLex

Joanna Freiermuth
Projektleiterin "Financial Inclusion"

1. Das Wichtigste in Kürze

- Asylsuchende und vorläufig Aufgenommene haben nur begrenzt Zugang zu einem eigenen Bankkonto und somit zum Zahlungsverkehr.
- Vorliegende Änderung berücksichtigt die Interessen jener Personen zu wenig. Insbesondere die Erleichterungen für Personen mit biometrischen Ausweisen wirken sich nicht zugunsten der Asylsuchenden und den vorläufig Aufgenommenen aus, denn diese verfügen über keinen biometrischen Ausweis.
- Bereits durch kleine wegweisende Schritte seitens der FINMA könnte diese Problematik erheblich entschärft werden.

2. Financial Inclusion von geflüchteten Menschen in der Schweiz

AsyLex ist ein Schweizer Verein, welcher geflüchteten Menschen Rechtsberatung im Asylrecht anbietet. Seit mehreren Jahren macht AsyLex – basierend auf einer Harvard Studie von Lea Hungerbühler – auf die *Financial Exclusion* von geflüchteten Menschen in der Schweiz aufmerksam und hat diesbezüglich regelmässig sowohl mit der FINMA als auch mit der Industrie Gespräche geführt. Ziel des Financial Inclusion Projekts ist es, auch geflüchteten Menschen in der Schweiz den Zugang zu einem Basisbankkonto zu ermöglichen. Auch das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) anerkennt die Wichtigkeit vom Zugang zu Bankdienstleistungen und hat soeben erst dazu aufgerufen, die Möglichkeiten für internationalen Zahlungen aus Industrieländern offen zu halten (vgl. https://www.eda.admin.ch/eda/de/home/das-eda/aktuell/newsuebersicht/2020/05/remittance-call-to-action.html):

> *Konkret soll der Zugang der Migrantinnen und Migranten zu Transferdienstleistungen verbessert werden, indem zusätzliche digitale Zahlungsmöglichkeiten zur Verfügung gestellt werden. Der Appell will politische Entscheidungsträger, Regulierungsbehörden und Dienstleistungsanbieter weltweit ermuntern, Geldüberweisungen zu erleichtern, indem sie die Regeln lockern, etwa durch Lizenzvergaben, indem sie finanzielle Anreize schaffen, beispielsweise durch die temporäre Senkung der Überweisungsgebühren, und indem sie die Anbieter in diesem Bereich als wichtige Dienstleister anerkennen. Schliesslich sollen die Migrantinnen und Migranten durch Informationskampagnen auf die neuen Möglichkeiten einschliesslich der digitalen Transferkanäle hingewiesen werden. Die Schweiz verpflichtet sich ihrerseits, Geldüberweisungen zu erleichtern, indem sie die Entwicklung von Finanzdienstleistungen unterstützt, die auf die Bedürfnisse von Migrantinnen und Migranten ausgerichtet sind.*

In diesem Zusammenhang ist auch die vorliegende Teilrevision des Rundschreibens der Video- und Online-Identifizierung von zentraler Bedeutung.

3. Hürden bei der Bankkontoeröffnung für Menschen mit Flüchtlingshintergrund

Wie die erwähnte Studie offenbarte, ist es heute für Personen mit N- und F-Ausweis sowie für sog. *Sans Papiers* kaum bis überhaupt nicht möglich, ein einfaches Bankkonto zu eröffnen. Ausschlaggebend für die Verweigerung eines Bankkontos ist regelmässig die Tatsache, dass die Identitätsdokumente (N- bzw. F-Ausweis, Ausgangsschein) von Finanzintermediären nicht als ausreichendes Identifikationsdokument angesehen wird bzw. werden darf. Oftmals verlangen die Banken sodann einen heimatlichen Ausweis, um die Identität zu überprüfen – was faktisch unmöglich ist, da die Betroffenen ihre heimatlichen Ausweisdokumente dem Staatssekretariat für Migration abgeben müssen, wo sie bis zur allfälligen Ausreise eines Tages hinterlegt bleiben. Teils verlangen die Banken auch das Vorlegen eines Arbeitsvertrags, was aufgrund des Arbeitsverbots gerade bei Asylsuchenden ebenfalls nicht zielführend ist.

Einzig die Postfinance sowie vereinzelte kantonal tätige Banken bieten gemäss der Studie grundsätzlich Konti für Personen mit N- und F-Status an, wobei es nach unserer Praxiserfahrung auch dort oft zu Problemen kommt und regelmässig die Kontoeröffnung erst nach unserer Intervention ermöglicht wird. Der Grundversorgungsauftrag der Postfinance dürfte Grund dafür sein, weshalb dieser Finanzintermediär offener ist für geflüchtete Menschen (Art. 32 Abs. 1 PG (SR 783.0)). Dabei ist zu erwähnen, dass Asylsuchende heute über längere Zeit keinen N-Ausweis mehr ausgestellt bekommen, stattdessen erhalten sie für eine lange Zeit bloss einen Ausgangsschein als Identifikationsdokument. Dieses wird aber selbst von der Postfinance nicht als Basis für die Errichtung eines Bankkontos zugelassen. Der Ausschluss vom Zugang zu Basis-Finanzdienstleistungen betrifft eine grosse Bevölkerungsgruppe: Über 50‘000 Menschen haben einen N- oder F-Ausweis, und eine geschätzte Zahl von 100‘000 bis 200‘000 Menschen sind Sans Papiers.[1]

Wie essentiell ein Bankkonto jedoch für solche Personen ist, erklärt sich von selbst. Es ermöglicht nicht nur den einfachen Online-Einkauf und die Bezahlung von Abonnementen,

[1] Ausländer- und Asylstatistik 2019, S. 79 f., https://www.sem.admin.ch/sem/de/home/publiservice/statistik/auslaenderstatistik/bestellung_statistiken.html, zuletzt besucht am 21.12.2020.

sondern auch die Zahlung von Mieten sowie das Auszahlen von Lohn. Die Signifikanz wird unter den vergangenen Geschehnissen im Rahmen der Corona-Pandemie noch verstärkt: Die Läden waren geschlossen. Viele Menschen waren angewiesen auf Online-Shopping und in den wenigen noch offenen Läden wurde sogar teilweise das Benutzen von Kreditkarten als Zahlungsmethode empfohlen. Beim Online-Shopping ist jedoch die Bezahlung auf Rechnung keine Selbstverständlichkeit mehr, denn viele Unternehmen setzen heute auf die Nutzung von Online-Zahlung, welche ohne Bankkonto quasi unmöglich ist. Zudem verlangen einige davon einen Aufpreis für die Einzahlung mit Bargeld an einem Postschalter. Durch diese besonderen Umstände sind Asylsuchende sowie vorläufig Aufgenommene noch mehr von den hiesigen Finanzdienstleistungen ausgeschlossen.[2]

4. Stellungnahme zu den Änderungen

Wie einleitend erwähnt, hat sich die Schweiz verpflichtet, Überweisungen für Migrantinnen und Migranten zu erleichtern, insbesondere durch digitale Zahlungsmöglichkeiten. Ohne Zugang zu Basisfinanzdienstleistungen ist dies aber schlicht nicht möglich. Es wäre erfreulich, wenn auch die FINMA dieses begrüssenswerte Committment der Schweiz mittragen würde und insbesondere im Rahmen der Anpassungen des Rundschreibens zur Online-Identifizierung aufgreifen würde.

Es ist grundsätzlich zu begrüssen, dass das neue Rundschreiben eine Alternative zur Online-Identifizierung Überweisung von einem bestehenden Bankkonto bietet. Dies insbesondere vor dem Hintergrund, dass geflüchtete Menschen eben i.d.R. noch kein Bankkonto in der Schweiz haben. Allerdings werden jegliche Erleichterungen für geflüchtete Menschen von keinem Nutzen sein, solange die ihnen ausgestellten Ausweisarten bei der Online-Identifizierung nicht zugelassen sind:

Das Rundschreiben konkretisiert Sorgfaltspflichten aus dem Geldwäschereigesetz, wobei es als nachvollziehbar erscheint, dass gerade im digitalen Umfeld ein gewisser Mindeststandard an die Sicherheit gestellt wird. In diesem Zusammenhang ist allerdings zu beachten, dass das geplante Erfordernis (Einlesen eines biometrischen Passes) für Personen mit N- und F-Ausweisen ein drastisches Zugangserschwernis darstellt. Bis Mitte 2021 werden diese Ausweise mindestens teilweise noch in Papierform ausgestellt und weisen daher in keiner Weise die Eigenschaften eines biometrischen Ausweises auf. Zwar wurden ab dem 1. November 2019 die neuen Ausweise gestaffelt nach Kantonen in Kreditkartenformat

[2] Eine ähnliche Problematik zeigte sich während der Covid-19 Pandemie beispielsweise in Irland: Asylum seekers excluded from financial system by bankers, Euronews, https://www.euronews.com/2020/11/29/asylum-seekers-excluded-from-financial-system-by-banks-in-ireland, zuletzt besucht am 9.1.2020.

ausgestellt, jedoch sind diese immer noch keine biometrischen Ausweise.[3] Somit bleibt diesen Personen auch durch die neue Alternatividentifizierungsform die Eröffnung eines Bankkontos – insbesondere online – verunmöglicht. Dies ist zu bedauern, da gerade das neue Format der N- und F-Ausweise Vorteile wie erhöhte Fälschungssicherheit mit sich bringt und Unterschrift sowie Foto der Person enthält. Das neue Format genügt somit durchaus den heutigen Anforderungen betreffend Fälschungsbekämpfung und Sicherheit.

Die FINMA hat bereits grundsätzlich bestätigt, dass ihrer Ansicht nach sowohl N- als auch F-Ausweise für die (nicht-digitale) Eröffnung eines Bankkotos ausreichend sind. Dennoch scheinen die Banken bei der Eröffnung von Bankkonten für die Betroffenen zurückhaltend zu sein, wohl auch wegen der unklaren Gesetzeslage und der damit verbundenen Rechtsunsicherheit. Es wäre daher zu begrüssen, dass die FINMA einen ähnlichen Ansatz wie die deutsche Aufsichtsbehörde (BaFin) verfolgen würde und explizit sowie öffentlich erklären würde, dass die Kontoeröffnung mit N- und F-Ausweis (idealerweise auch mit Ausgangsschein) als Identifikationsdokument zulässig ist (z.B. in einem Rundschreiben, Wegleitung oder Positionspapier).[4] Durch die so vermittelte Rechtssicherheit im Markt müssten die Banken nicht mehr das Risiko der regulatorischen Ungewissheit tragen und dürften offener sein für Geflüchtete als Klientschaft.

Neben der ordentlichen Eröffnung von Bankkonti – welche an sich bereits eine enorme Hürde ist für Geflüchtete – sollte heute eigentlich der Zugang zu digitalen Finanzdienstleistungen im Vordergrund stehen. Dort ist der Zugang für geflüchtete Menschen vollends versperrt, was gerade angesichts des einleitend erwähnten Aufrufs der Schweiz zur Erleichterung von online Finanzdienstleistungen für Migrantinnen und Migranten besonders stossend ist.

Neben der obenerwähnten Klarstellung der Zulässigkeit der Kontoeröffnung für Menschen mit N- oder F-Ausweis auf traditionelle Art und Weise wäre es demnach geboten, auch Möglichkeiten zu schaffen, welche es geflüchteten Menschen ermöglichen, online ein Bankkonto zu eröffnen – was mit der heutigen Regulierung vollends ausgeschlossen ist. So wäre beispielsweise denkbar, dass geflüchtete Menschen zusätzlich zum N- bzw. F-Ausweis oder dem Ausgangssschein eine Bestätigung der zuständigen Migrationsbehörde (entweder Staatssekretariat SEM oder kantonales Migrationsamt, je nach Verfahrensstand) einscannen / fotografieren könnten, welches die einmalige und unveränderliche Identifikationsnummer („N

[3] Ausländerausweise im Kreditkartenformat, 20.09.2020, https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2019/2019-09-20.html, zuletzt besucht am 13.12.2020.

[4] Ein ähnlicher Ansatz wurde mit Blick auf andere europäische Länder vorgeschlagen: Vgl. z.B. The challenge of fostering financial inclusion of refugees, Bruegel, Zsolt Darvas, 13.12.2017, https://www.bruegel.org/2017/12/the-challenge-of-fostering-financial-inclusion-of-refugees, zuletzt besucht am 28.01.2021.

Nummer“) enthält. Alternativ könnte eine Asylsozialhilfebestätigung eingereicht werden, oder ein anderes Schreiben der zuständigen Migrationsbehörden, welches die eindeutige Identifizierung der betroffenen Person sicherstellt. Ein individuell zugeschnittener QR-Code, welcher bei Einscannen die notwendigen Informationen zur abschliessenden Identifikation einer Person offenbart, könnte den administrativen Aufwand hierbei vereinfachen. Schliesslich wäre eine fortschrittlichere Art der Identifizierung denkbar, z.B. mittels Iris-Scan oder Fingerabdrücken, welche auch für Menschen, welche keine Identifikationspapiere haben, möglich sind.

In jedem Fall ist es u.E. unumgänglich, dass die gegenwärtige Diskriminierung von geflüchteten Menschen bei der Kontoeröffnung ein Ende nimmt. Dies entspricht nicht nur dem vom EDA geäusserten Aufruf, vielmehr ist der heutige Status der „Financial Exclusion“ einem weltweit führenden Finanzplatz in einem für seine humanitären Werte gelobten Land unwürdig. Es wäre folglich sehr zu begrüssen, wenn die FINMA diesbezüglich einen vorausschauenden, inklusiven und fortschrittlichen Ansatz verfolgen und den Einbezug von geflüchteten Menschen bei online Finanzdienstleistungen ermöglichen würde.

5. Erläuterungen zu Praktiken im Ausland

An dieser Stelle sei noch kurz auf alternative Handhabungsmöglichkeiten bezüglich der Problematik *Financial Inclusion* von geflüchteten Menschen einzugehen. Hierzu wurde insbesondere einen Blick auf die Praxis im Ausland geworfen:

Das finnische Blockchain-Startup MONI hat ein System entwickelt, welches allen Flüchtlingen ermöglicht, eine Prepaid-Debitkarte und ein mobiles Zahlungskonto zu eröffnen, ohne dass diese dafür Ausweispapiere benötigen. Im Rahmen einer Initiative mit der finnischen Einwanderungsbehörde hat MONI ein System entwickelt, das den Asylausweis eines Migranten, der mit einem eindeutigen biometrischen Polizeidatensatz verknüpft ist, nutzt, um Asylbewerbern eine offizielle Identität zu geben. Dies ermöglicht, dass sie Zugang zu Finanzdienstleistungen erhalten können, während sie auf eine Entscheidung über ihren Flüchtlingsstatus warten.[5] Prepaid Debitkarten erscheinen dabei als besonders vorteilhaft, weil dadurch die Bank kein Risiko einer allfälligen Überbelastung der Karte trägt.

[5] Vgl. O. Smith, Moni gives ‘financial inclusion and dignity’ to European migrants, The Memo, 3 Oktober 2016, https://www.forbes.com/sites/oliversmith/2016/10/03/moni-offers-financial-inclusion-and-dignity-for-6000-european-migrants/, zuletzt besucht am 28.01.2021; Hungerbühler/Westerwinter, S. 11; MONI, https://startup100.net/company/moni, zuletzt besucht am 28.01.2021.

Im Juli 2014 hat die EU die Zahlungskontenrichtlinie erlassen, die jedem, der sich rechtmässig in der Europäischen Union aufhält, das Recht auf ein sogenanntes Basiszahlungskonto ("Basiskonto") gibt.[6]

- Auf der Grundlage dieser Richtlinie hat der italienische Bankenverband (ABI) am 16. April 2019 ein Rundschreiben an alle Banken betreffend die Eröffnung von Bankkonten durch Asylsuchende versandt. ABI hat dabei hervorgehoben, dass Banken in Italien verpflichtet sind, ihre Kunden anhand von Identitätsdokumenten oder anderen als gleichwertig erachtete Identifikationsdokumenten oder anhand von Dokumenten, Daten oder Informationen, die aus einer zuverlässigen und unabhängigen Quelle stammen, zu identifizieren. ABI betonte, dass für den Zugang zu Dienstleistungen von Banken nicht die Vorlage einer Aufenthaltsbewilligung (oder eines Passes) verlangt wird, sondern ein einfaches Identifikationsdokument genüge.[7]
- Dementsprechend können auch in Deutschland alle Personen ein Bankkonto direkt mittels ihres Asylausweises eröffnen.[8] Zudem dürfen selbst Menschen ohne jeglichen Ausweis durch eine Bescheinigung der Behörden ein Konto errichten. Die Bescheinigung beinhalten neben weiteren Angaben ein Lichtbild des Antragstellers.[9]
- In Frankreich kann ein Bankkonto grundsätzlich mithilfe einer Wohnsitzbescheinigung eröffnet werden. Des Weiteren besteht, im Rahmen des durch den Gesetzgeber initiierten Projekts “Recht auf ein Bankkonto”, die Möglichkeit, im Falle einer verweigerten Kontoeröffnung an die Banque de France zu gelangen. Diese überprüft den Fall und veranlasst gegebenenfalls weitere Schritte.[10]

Sowohl in Deutschland als auch in Frankreich ist die Nachfrage nach solchen Konti immens.[11] Hierdurch zeigt sich, dass im Ausland die Problematik von Hürden bei der Bankkontoeröffnung

---

[6] Directive 2014/92/EU of the European Parliament and of the Council, 23.07.2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0214.01.ENG, zuletzt besucht am 28.01.2021.

[7] Asylum Seeker: Residency is not required to open a bank account, 20.05.2019, http://www.integrazionemigranti.gov.it/en/latest-news/news/Pages/Asylum-seeker-residency-is-not-required-to-open-a-bank-account.aspx, zuletzt besucht am 28.01.2021.

[8] § 12 Absatz 1 Satz 1 Nummer 1 des Geldwäschegesetzes

[9] § 2 Ziff. 1 Verordnung über die Bestimmung von Dokumenten, die zur Überprüfung der Identität einer nach dem Geldwäschegesetz zu identifizierenden Person zum Zwecke des Abschlusses eines Zahlungskontovertrags zugelassen werden (Zahlungskonto-Identitätsprüfungsverordnung - ZIdPrüfV)

[10] Beispielhaft: Denis Beau, Banque de France - Financial inclusion in the digital age: how to make a difference?, https://www.banque-france.fr/en/intervention/financial-inclusion-digital-age-how-make-difference, zuletzt besucht am 28.01.2021

[11] Ouverture d’un compte bancaire, https://www.infomigrants.net/fr/post/8550/ouverture-d-un-compte-bancaire-la-poste-met-en-place-un-guichet-special-pour-les-demandeurs-d-asile#:~:text=La%20Poste%20et%20la%20Mairie%20de%20Paris%20ont%20lanc%C3%A9%20mi,le%2011e%20arrondissement%20de%20Paris*, zuletzt besucht am 09.01.2021; Tipps für Flüchtlinge, Kontoeröffnung leicht gemacht, https://www.financescout24.de/wissen/ratgeber/kontoeroeffnung-fuer-fluechtlinge, zuletzt besucht am 09.01.2021.

für geflüchtete Menschen erkannt wurde und entsprechende Anpassungen vorgenommen wurden. Das Thema wurde als derart signifikant eingestuft, dass sogar die EU durch obgenannte Richtlinie aktiv wurde. Ähnliche Lösungsansätze könnten auch in der Schweiz angestrebt werden.

6. Abschliessende Bemerkungen

Aufgrund der für asylsuchende und vorläufig aufgenommene Personen bestehenden drastischen Schwierigkeiten bei der Inanspruchnahme von Dienstleistungen einer Bank, wäre es aus der Sicht von AsyLex angebracht, den Interessen dieser Personengruppen mehr Rechnung zu tragen. Dies nicht nur bei vorliegendem Rundschreiben bezüglich der Video- und Online-Identifizierung, sondern auch in sämtlichen anderen Belangen, in welchen sie durch Finanzintermediäre im Vergleich zu nicht-geflüchteten Menschen schlechter gestellt sind. Kleine wegweisende Schritte der FINMA könnte den Zugang zu Bankdienstleistungen für geflüchtete Menschen erheblich verbessern und somit einen enormen Beitrag gegen Diskriminierung und zur Integration leisten.

Baloise Bank SoBa AG
Amthausplatz 4, 4502 Solothurn
T +41 (0)58 285 33 33
www.baloise.ch
BIC: KBSOCH22
CHE-116.301.152 MWSt

Baloise Bank SoBa

Ihr Kontakt
Thomas Maurer
Leiter Kundenservice
T +41 58 285 37 42
thomas.maurer@baloise.ch

E-Mail

isabel.grueninger@finma.ch

Eidgenössische
Finanzmarktaufsicht FINMA
Isabel Grüninger
Laupenstrasse 27
CH-3003 Bern

29. Januar 2021 / tma

Stellungnahme zum Erläuterungsbericht der Teilrevision des Rundschreibens 2016/7 «Video- und Online-Identifizierung»

Sehr geehrte Frau Grüninger
Sehr geehrte Damen und Herren

Mit diesem Schreiben folgen wir Ihrer Einladung zur Stellungnahme bezüglich der Medienmitteilung vom 16. November 2020.

1. Teilrevision des Rundschreibens 2016/7 «Video- und Online-Identifizierung»

Die in der Teilrevision des Rundschreibens 2016/7 «Video- und Online-Identifizierung» präsentierten Änderungsvorschläge erfüllen unsere Anforderungen nicht.

Rz 33 - Banküberweisung

Folgende Herausforderungen haben wir bei der Banküberweisung beobachtet:

- Kunden halten die Frist von 30 Tagen (VSB 2020) nicht ein.
- Die Überweisung erfolgt von einem Konto, welches nicht auf den Namen der Vertragspartei lautet. Beispiele:
  - Eltern zahlen für ihre Kinder (junge Erwachsene) ein
  - Lohnzahlung des Arbeitgebers
  - Überweisung einer Versicherungsleistung
  - etc.

Solche Fälle entsprechen einer zu grossen Anzahl von Eröffnungen und führen zu häufig zu Abbrüchen.

Rz 33.1 Auslesen des Chips

Bei Schweizer Bürgern kommt hierfür nur der Schweizer Pass in Frage. Bemühungen, die Schweizer Identitätskarte mit einem Chip zu versehen, wurden im Dezember 2017 durch den Bundesrat verworfen. Die Variante «Chip» bedient in der heutigen Zeit deshalb lediglich einen Nischenmarkt.

Im Weiteren ist anzufügen, dass mit der Online-Identifizierung – egal ob mit Pass oder Banküberweisung – keine Dokumente mit einer qualifizierten elektronischen Signatur (Art. 14 Abs. 2bis OR) unterzeichnet werden können.

2. Vorschlag: Video-Aufzeichnung in Echtzeit mit asynchroner Verifikation

Die Banken benötigen eine Lösung, welche durch den Kunden 7x24x365 bedienbar ist und den europäischen Normen (AML5, eIDAS, EU-Verordnung Nr. 910/2014) entspricht.

Die Identifizierung selbst muss folgende Elemente enthalten:

- Video- und Audioaufzeichnung in Echtzeit
  - mit allen relevanten Seiten des Ausweisdokumentes und
  - mit der zu identifizierenden Person selbst,
- Face Biometrics Scoring,
- Liveness Detection und
- (je nach gefordertem Sicherheitslevel) die asynchrone Verifikation durch ausgebildete Mitarbeitende.

Eingliederung in das Rundschreiben

Die «Video-Identifizierung in Echtzeit mit asynchroner Verifikation» soll der persönlichen Vorsprache gleichgestellt sein und in einem neuen Abschnitt definiert werden. Textvorschlag im Anhang.

3. Weitere Anliegen

Da sich die Technologie rasant weiterentwickelt, begrüssen wir einen kürzeren Aktualisierungsrhythmus des Rundschreibens. Dies gibt die Möglichkeit, zeitnah auf eventuelle Entwicklungen im EU-Raum reagieren zu können und etwaige Wettbewerbsnachteile rasch wettzumachen.

Freundliche Grüsse

Baloise Bank SoBa AG

Thomas Maurer
Leiter Kundenservice Bank

Jürg Ritz
CEO

>28.01.2021>B025181>d>3109

Anhang 1 – Eingliederung in das Rundschreiben (Vorschlag)

xy. Video-Identifizierung in Echtzeit mit asynchroner Verifikation

Der Identifizierung einer natürlichen Person bei persönlicher Vorsprache gleichgestellt ist die Identifizierung mittels asynchroner Verifikation, soweit sie die folgenden Grundsätze erfüllt:

a) Technisches und Organisatorisches

Die Identifizierung erfolgt mittels Datenübertragung zwischen der Vertragspartei und dem Finanzintermediär. Der Finanzintermediär setzt dafür geeignete technische Hilfsmittel ein, die eine

- sichere Übertragung,
- das Auslesen der MRZ auf dem Identifizierungsdokument,
- das Auslesen der optisch erkennbaren Textinformationen (Visual Inspektion Zone, VIZ) auf dem Identifizierungsdokument,
- die Aufnahme einer Videosequenz der Gesichtspartie der Vertragspartei,
- die Aufnahme einer Videosequenz und Lichtbilder der Vorderseite des Identifizierungsdokuments und
- die Aufnahme einer Videosequenz und Lichtbilder der Rückseite des Identifizierungsdokuments

sicherstellen.

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

Bild- und Tonqualität müssen geeignet sein, um eine einwandfreie Identifizierung zu ermöglichen.

b) Identitätsprüfung

Der Finanzintermediär gestaltet den Prozess zur Aufnahme der Geschäftsbeziehung über Internet-Kanäle so, dass die Vertragspartei die Angaben nach Art. 44 und 60 GwV-FINMA vorgängig zur Erstellung der Videosequenzen und dem Auslesen der VIZ und der MRZ elektronisch erfasst und dem Finanzintermediär übermittelt.

Der Finanzintermediär holt vor der Aufzeichnung und Übermittlung der Videosequenz das ausdrückliche Einverständnis der Vertragspartei zur Durchführung der Identifizierung und Speicherung der Videosequenzen und Lichtbilder ein.

Der Finanzintermediär setzt geeignete technische Hilfsmittel für die folgenden Prüfungen ein:

- Die Übereinstimmung der übermittelten Daten mit den Informationen aus der MRZ und der VIZ des Identifizierungsdokuments der Vertragspartei.
- Die Übereinstimmung der Vertragspartei in der Videosequenz mit dem Lichtbild auf dem Identifizierungsbild der Vertragspartei.

- Die Echtheit des Identifizierungsdokuments durch maschinelle Überprüfung von mindestens zwei Sicherheitsmerkmalen.
- Die Lebendigkeit der Vertragspartei anhand der Videosequenz, insbesondere die Echtheit der Videosequenz und die persönliche Präsenz der Vertragspartei im Zeitpunkt der Aufnahme der Videosequenz, um eine gefälschte oder manipulierte Videosequenz erkennen zu können.

Jeder Identifizierungsvorgang ist zu dokumentieren. Die Videosequenzen oder Lichtbilder des Identifizierungsdokuments und der Vertragspartei inkl. der einzelnen Prüfungsergebnisse sind zu den Akten zu nehmen und zu archivieren.

c) Ergänzende manuelle Prüfung

Einzig die Übereinstimmung der übermittelten Daten der Vertragspartei mit den Informationen aus der MRZ und der VIZ des Identifikationsdokuments kann zusätzlich manuell durch den Finanzintermediär beurteilt werden, wenn die Schreibweise der übermittelten Daten von MRZ und VIZ abweicht (z.B. Sonderzeichen). In den übrigen Fällen erfolgt der Abbruch des Identifizierungsvorgangs.

d) Abbruch des Identifizierungsvorgangs

Der Finanzintermediär bricht den Identifizierungsvorgang ab,

- wenn die Bild- und/oder Tonqualität eine einwandfreie Identifizierung der Vertragspartei nicht erlauben; oder
- wenn Zweifel an der Echtheit des Ausweisdokuments, der Videosequenz oder der Identität der Vertragspartei aufkommen.

Der Abbruch des Identifizierungsvorgangs kann auch darin bestehen, dass der Kunde für die fraglichen Identifizierungsschritte auf herkömmliche Kanäle (persönliche Vorsprache, Korrespondenzweg) verwiesen wird.

EXPERT suisse
Wirtschaftsprüfung
Steuern
Treuhand

Per E-Mail: isabel.grueninger@finma.ch

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

Zürich, 3. Februar 2021

Stellungnahme zur Anpassung des FINMA-Rundschreibens 2016/7 „Video- und Online-Identifizierung“

Sehr geehrte Frau Grüninger

Für die Zustellung der Unterlagen zu den eingangs erwähnten Anpassungen danken wir Ihnen bestens. Die zuständigen Kommissionen von EXPERTsuisse haben die Entwürfe und Anpassungen intensiv studiert.

Wir sind mit den meisten Anpassungen einverstanden. Unsere Verbesserungsvorschläge haben wir in beiliegendem Dokument festgehalten und sind Ihnen für die wohlwollende Prüfung unserer Empfehlungen dankbar.

Für Rückfragen stehen Ihnen die Unterzeichnenden gerne zur Verfügung.

Freundliche Grüsse
EXPERTsuisse

Thomas Romer
Präsident Fachbereich Finanzmarkt

Dr. Thorsten Kleibold
Mitglied der Geschäftsleitung

EXPERTsuisse AG – Schweizer Expertenverband für Wirtschaftsprüfung, Steuern und Treuhand
Stauffacherstrasse 1, CH-8004 Zürich, Tel. +41 58 206 05 05, Fax +41 58 206 05 09
info@expertsuisse.ch, www.expertsuisse.ch

<table>
<tr><th colspan="2">FINMA-Rundschreiben 2016/7 „Video- und Online-Identifizierung “</th><th></th></tr>
<tr><th>Rz</th><th>Geänderte Texte
Neue = blau unterstrichen, gelöscht = ~~blau und durchgestrichen~~</th><th>Verbesserungsvorschlag / Kommentar / Bemerkung</th></tr>
<tr><td>2</td><td>-</td><td>Anpassungsvorschlag:
Dieses Rundschreiben findet direkte Anwendung auf Finanzintermediäre nach Art. 2 Abs. 2 GwG ~~und solche nach Art. 2 Abs. 3 GwG, die der Aufsicht der FINMA gemäss Art. 14 GwG direkt unterstellt sind (DUFI)~~.</td></tr>
<tr><td>53</td><td>Die in den nachfolgenden Artikeln der GwV-FINMA gewählte Formulierung beinhaltet in einem digitalen Kontext auch folgende Formen:

<table><tr><td>Verordnungsartikel und -Wortlaut</td><td>Erläuterungen und Anwendungsbeispiele zur digitalen Form</td></tr><tr><td>[…]</td><td>[…]</td></tr><tr><td>Art. 28 Abs. 3 GwV-FINMA:

Beigezogene Dritte dürfen ihrerseits keine weiteren Personen oder Unternehmen beiziehen.</td><td>Zieht ein Finanzintermediär einen anderen Finanzintermediär bei, und nimmt dieser die Video- und Online-Identifizierung durch direkt beauftragte Dienstleister vor, so gelten letztere nicht als weitere Personen oder Unternehmen und es liegt keine untersagte Weiterdelegation vor.</td></tr><tr><td>[…]</td><td>[…]</td></tr></table></td><td>Referenz auf DUFI ersetzen, da nicht mehr aktuell.

<table><tr><td>Art. 45 Abs. 2 GwV-FINMA: Wird die Geschäftsbeziehung ohne persönliche Vorsprache aufgenommen, so prüft der ~~DUFI~~ Finanzintermediär zusätzlich die Wohnsitzadresse durch Postzustellung oder auf andere gleichwertige Weise […]</td><td>[…]</td></tr></table></td></tr>
</table>

fidentity

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

fidentity GmbH
Thorsten Hau
Alpenstrasse 62
3126 Kaufdorf
thorsten@fidentity.ch

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

Sehr geehrte Frau Grüninger

Gerne nutze ich die Gelegenheit, Möglichkeiten aufzuzeigen, Innovation und Technologieneutralität zu fördern und so ein höheres Sicherheitsniveau ohne höhere Kosten zu erreichen.

Ich bin Geschäftsführer der Firma fidentity. Wir betreiben ein Identifikationsverfahren, das die Vorgaben zur Online-Identifikation komplett automatisiert erfüllt. Unser Fokus liegt darauf die Identifikation für die Anwender mittels künstlicher Intelligenz möglichst einfach zu machen. Einfachheit ist wesentlich. Jeder kognitiv aufwändige Prozessschritt, den der Nutzer erledigen muss, reduziert die Wahrscheinlichkeit, dass ein Angebot genutzt wird um 50% bis 90%.

Ich werde im Folgenden zuerst die von Ihnen vorgeschlagene Änderung einordnen, danach Verbesserungspotenzial aufzeigen und zuletzt Vorschläge machen, mit denen das Potenzial genutzt werden kann.

Einordnung:
Mit der Online- und der Videoidentifikation sind zwei Verfahren zugelassen, die sich im Sicherheitsniveau der Identifikation stark unterscheiden. Die Technologie, die Videoidentifikation skalierbar zu umgehen, wird gerade erst möglich. Damit ist die Videoidentifikation relativ sicher.

Im Gegensatz hierzu ist das Sicherheitsniveau der Onlineidentifikation sehr niedrig. Einfache Uploads durch den Nutzer lassen es zu, dass Kopien digital bearbeitet werden und ohne Umweg hochgeladen werden können. Daher ist hier der starke Faktor der Banküberweisung ergänzend notwendig.

Mit der Möglichkeit mittels NFC den Chip des Passes zu nutzen, lassen Sie neu ein Verfahren zu, das kryptografisch sicher ist. Eine Umgehung ist beinahe unmöglich.

Aus unserer Sicht bleiben mit der vorliegenden Revision wesentliche Aspekte unberücksichtigt. Wir sehen vor Allem folgende **Verbesserungspotenziale:**

- **Technologieneutralität:** Effektive Methoden ergeben sich meist aus der Praxis durch Kombination und Optimierung. Durch die Vorgabe bestimmter Technologien wird verhindert, dass sich unterschiedliche Methoden im Wettbewerb beweisen. Unser Verfahren ist z.B. deutlich sicherer als der Massstab, der bei der Onlineidentifikation gefordert wird. Regulatorisch liefert dies keinen Mehrwert, da sich diese Massnahmen nicht in die vorgedachten Kategorien einsortieren lassen.
- **Risikoorientiertes Vorgehen:** Die GWV-Finma sieht diverse Ausnahmen und Erleichterungen der Sorgfaltspflichten vor, wenn das Risikoprofil es zulässt. Z.B. ist es gemäss Art. 12 möglich, eine Zahlkarte auf dem Korrespondenzweg mittels ID-Kopie per Post zu eröffnen und monatlich bis zu CHF 25'00 zu bezahlen oder Bargeld zu beziehen. Im Gegensatz hierzu muss für die Eröffnung jedes einfachen Gehaltskontos eine Identifikation gemäss Rundschreiben erfolgen.
- **Praktikabilität / Relevanz in der Praxis**
  Der Ansatz via NFC ist theoretisch attraktiv, aber praktisch stellen sich diverse Hürden dar:
  a. In der Praxis sehen wir praktisch keine Nutzer, die sich mittels Pass identifizieren. Die ID hat auf absehbare Zeit keinen NFC Chip. In der Schweiz dominiert die ID mit ca. 99% der Identifizierungsvorgänge.
  b. Der Nutzer muss einen weiteren «Arbeitsgang» machen, bis er identifiziert ist.
  Der Scan des Chips erfordert das visuelle Auslesen der MRZ des Dokuments, da sonst kein Zugriff zum Chip gewährt wird.
  c. Das Auslesen des Chips selbst ist anfällig für Fehler durch den Nutzer. Z.B. positioniert er/sie das Dokument falsch (einige cm reichen).
  d. Der in Pässen genutzte NFC-Standard erfordert die Verwendung einer nativen App, was bei optischen Verfahren nicht der Fall ist.

  Ähnlich verhält es sich mit der Banküberweisung.
  a. Oft sind IT-Systeme nicht ohne Weiteres in der Lage den Geldeingang zu melden und die Identifikation abzuschliessen.
  b. Der Prozess für den Kunden ist komplex (z.B. Wechsel ins e-banking, Überweisung an neue IBAN).
  c. Zeitliches Auseinanderfallen von Identifikation, Überweisung und Aufnahme der Geschäftsbeziehung macht die Prozess-Steuerung komplex.
  d. Oft treten regulatorische Unsicherheiten auf («Dürfen wir eine neue IBAN kommunizieren, bevor wir den Geldeingang auf dieser IBAN verzeichnet haben?»)

Vorschläge zur Ausgestaltung der Online Identifikation

a. Technologieneutrale Formulierung der flankierenden Sicherheitsanforderungen
Neben den vorgeschlagenen Massnahmen (Banküberweisung, NFC) ist eine Vielzahl weiterer Massnahmen denkbar, die das Sicherheitsniveau v.A. in Kombination massiv erhöhen. Z.B.:
- Videomitschnitte der Identifikation und deren manuelle Prüfung während oder nach der Identifikation
- Stichprobenmässige Videoidentifikation der identifizierten Personen
- Ergänzendes Videogespräch mit der Person
- Einbezug weiterer Datenquellen (IP-Adressen, Mobilnetz-Anbieter, Browser-Fingerprint, Verhalten des Anwenders während der Identifikation, …)
- Technische Massnahmen zur Validierung der Echtheit der Dokumente, Z.B. Prüfung optisch veränderlichen Merkmale, Prüfung der Mikroschrift, …

Vorschlag analog Art. 50 GWV-FINMA: «Der Finanzintermediär kann auf die Banküberweisung verzichten, wenn er andere technische, organisatorische oder prozessuale Massnahmen ergreift, die es ihm ermöglichen, die Identität der Vertragspartei zu überprüfen.»

b. Risikoorientierte Ausgestaltung der flankierenden Sicherheitsanforderungen

Explizit vorsehen, dass sich der Umfang der flankierenden Sicherheitsanforderungen am Geldwäscherei-Risiko zu orientieren hat. Ein Konto z.B., das nur zur Abzahlung eines Kredits, als Sparprodukt ohne Zahlungsverkehr oder als Gehaltskonto mit Rückzugslimiten betrieben wird, hat ein massiv geringeres Risikoprofil als das Geschäftskonto einer neu gegründeten Gesellschaft.

Explizit vorsehen, dass die Qualität der Identifikation im Zeitverlauf angepasst werden muss, wenn sich das Risikoprofil ändert, oder Verdachtsmomente auftauchen.

Vorschlag analog Art. 69 GWV-FINMA: «Flankierende Massnahmen müssen risikoadäquat sein. Der Finanzintermediär legt hierzu Kriterien fest. Die Identifizierung muss im Laufe der Geschäftsbeziehung wiederholt oder ergänzt werden, wenn sich das Risikoprofil ändert.»

c. Ergebnisorientierung

Mit einer Flexibilisierung des Vorgehens geht die Notwendigkeit einher nachzuweisen, dass das gewählte Vorgehen die Geldwäscherei wirksam verhindert. Hierzu sollten statistisch belastbare Formulierungen gewählt werden. Z.B.:
«Wählt der Finanzintermediär andere, als die im Rundschreiben aufgezählten, flankierende Massnahmen, so überprüft er 1% der identifizierten Kunden mittels Vor-Ort oder Video-Identifikation. Treten in mehr als 1% der geprüften Fälle Zweifel an der Identifikation auf, so ist das Identifikationsverfahren zu überprüfen.»

Besten Dank für die Prüfung unserer Vorschläge. Wir sind der Überzeugung, dass mit unseren Vorschlägen eine effizientere Regulierung möglich wird und der Finanzplatz noch stärker von technischen Innovationen profitiert. Gerne stehen wir für eine weitergehende Abklärungen zur Verfügung.

Mit freundlichen Grüssen

Dr. Thorsten Hau

PXL Vision AG, Mühlebachstrasse 164, CH – 8008 Zurich
Phone: +41 44 295 10 40 | info@pxl-vision.com | www.pxl-vision.com

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

Kontaktperson

Karim Nemr
karim.nemr@pxl-vision.com
+41 76 432 49 11

31. Januar, 2021

Stellungnahme zum Änderungsentwurf des Rundschreibens 2016/7 "Video- und Online-Identifizierung" der FINMA

Sehr geehrte Damen und Herren,

Die PXL Vision AG bedankt sich für die Möglichkeit, nachfolgend zum Änderungsentwurf des FINMA Rundschreibens 2016/7 Stellung nehmen zu dürfen. Wir begrüssen ausdrücklich die angedachte Liberalisierung, möchten aber darauf hinweisen, dass sie unseres Erachtens angesichts der fortgeschrittenen Technik der Bilderkennung noch weitere Verfahren der Identifizierung auch ohne Referenzüberweisung in Betracht ziehen sollte.

Wir möchten darlegen, dass die derzeit verfügbaren innovativen elektronischen Identifikationsverfahren, die sich bei ihrer Risikobewertung an einer menschlichen Face-to-Face Kontrolle unter Anwesenden messen lassen müssen, ebenso geeignet sind, das erforderliche Sicherheitsniveau für die Online-Identifizierung zu erfüllen.

Die Techniken der digitalen Bilderkennung zusammen mit der Gesichtserkennung auf biometrischer Basis stellen ein hoch zuverlässiges Verfahren zur Durchführung von Online-Identitätsprüfungen dar.

Im Zusammenspiel mit den Banken und deren Interesse an einem rechtssicheren aber auch für den Kunden praktikablen Prozess, wird daher unsererseits angeregt, in der Schweiz einem technologieneutralen, und der Selbstverantwortung der Banken verpflichteten Ansatz zu folgen. Zuverlässige Sicherheitsmerkmale, wie Hologramm- oder Kippbilderkennung als Kriterium sollten als ebenso sicher wie die NFC Überprüfung anerkannt werden. Wir regen daher eine Erweiterung des Änderungsvorschlags, insbesondere in den folgenden Bereichen an:

- Verzicht der Referenzüberweisung und Wohnsitzprüfung, nicht nur unter Anwendung der Chip Prüfung, sondern auch unter Anwendung einer hochentwickelter Echtheitserkennung von Hologrammen /Kippbildern
- Verzicht der Referenzüberweisung und Wohnsitzprüfung in Kombination mit einer menschlichen Nachkontrolle

Wir danken für die wohlwollende Berücksichtigung unserer Position und stehen für Fragen, Erläuterungen und Diskussionen gerne zur Verfügung.

Mit freundlichen Grüssen

Michael Born

Chief Executive Officer

Karim Nemr

Chief Business Officer

Beilagen:

- Stellungnahme im Detail

Stellungnahme im Detail

Detaillierte Stellungnahme und Herleitung zur Anhörung im Bezug auf die Teilrevision des FINMA-Rundschreibens: 2016/7 „Video- und Online-Identifizierung“

Autoren: Karim Nemr, Mitinhaber und Chief Business Office PXL Vision AG

Rechtsanwalt Thomas Börner, Legal Counsel bei PXL Vision AG

I. PXL Vision AG

Die PXL Vision AG ist ein Technologiedienstleister für die Erfüllung von Sorgfaltspflichten bei der Aufnahme von Geschäftsbeziehungen über digitale Kanäle.

Mit ihren zuverlässigen Lösungen zur Identitätsprüfung unterstützt PXL Vision bereits zahlreiche namhafte Schweizer Unternehmen (darunter SwissID, alle Mobilfunkanbieter, namhafte Schweizer Banken) bei der Erfassung von Endkunden durch sichere Überprüfung von deren Identität durch ein automatisiertes maschinelles Verfahren (Auto-Ident) in Echtzeit und ohne physische Präsenz.

PXL Vision begrüsst die Bereitschaft der FINMA in dem vorgeschlagenen Änderungsentwurf den Anwendungsbereich der Online-Identifikation zu erweitern ausdrücklich. Da die Verwendung des biometrischen NFC-Dokumentenchips ein ausgesprochen sicheres Verfahren ist, ist deren Zulassung im Rahmen der Identifizierung zielführend und folgerichtig.

Allerdings ist sie aus unserer Sicht nicht das einzige wirksame Verfahren, weswegen wir mit dieser Stellungnahme die Berücksichtigung noch weiterer Verfahren anregen möchten.

II. Die Anpassung der Sorgfaltspflichten

Mit unserer Stellungnahme beziehen wir uns konkret auf die geplante zusätzliche Möglichkeit zur Online-Identifikation durch das Auslesen und Prüfen von Daten auf dem Chip des biometrischen Passes ohne das Erfordernis einer zusätzlichen Referenzüberweisung.

Im Ergebnis möchten wir nachfolgend darlegen, dass die automatisierte Bilderkennung von Ausweisdokumenten, die aufgrund hochentwickelter und KI-unterstützter Technik als Mindestanforderung in der Lage ist, neben den reinen Ausweisdaten auch zahlreiche Sicherheitsmerkmale des gescannten Dokumentes (wie kinematische Effekte und Hologramme) zu erkennen, im Zusammenspiel mit biometrischer Gesichtserkennung und optionaler, menschlicher Nachkontrolle im Falle von Uneindeutigkeiten, der Chiperkennung kaum nachsteht. Der Sicherheitsmassstab sollte zudem an der Erkennung durch einen Menschen bei physischer Präsenz gemessen werden. Dies wollen wir nachfolgend im Rahmen einer Verhältnismässigkeitsprüfung darlegen (s. im Detail unten zu maschinellen Erkennungsmöglichkeiten des Hologramms).

1. Anzulegender Sicherheitsmassstab

Die Bankinstitute sind schon qua eigenen wirtschaftlichen Interesses in höchstem Masse daran interessiert, die mit einer Transaktion verbundenen Risiken zu evaluieren und entsprechende ggf. im Einzelfall auch über die regulatorischen Anforderungen hinausgehende Massnahmen zur Verhinderung von Missbrauch zu ergreifen. Es stehen ihnen hierzu neben der Dokumentenbasierten Identitätsprüfung auch zahlreiche Datenbasen zur Verfügung, mittels derer sie die

Seriosität eines Kunden, aber auch die Rechtskonformität von Transaktionen beurteilen können.

Für den überwiegenden Teil der Kundengeschäfte dürften die Banken zu dem Ergebnis kommen, dass gesteigerte Missbrauchs- und damit Schadensrisiken nicht bestehen. Sie werden daher einen zwar sicheren, aber dennoch auch im Verhältnis zum Interesse des Kunden an einem nutzerfreundlichen Verfahren orientierten Sicherheitsmassstab anlegen, den es mit der Regulierung abzudecken gilt.

2. Geeignetheit des Autoidentverfahrens

Es ist unbestritten, dass die Identifizierung über den Chip eine höchst sichere und damit geeignete Verfahrensweise darstellt und dass weitere Verifikationsvorgänge wie eine Referenzüberweisung bei diesem Verfahren nicht erforderlich sind.

Ein Auto-Ident Verfahren, auch ohne NFC Überprüfung, ist jedoch gleichfalls geeignet, die notwendige Sicherheit zu erzielen, auch ohne dass es weiteren flankierenden Massnahmen wie einer Referenzüberweisung bedürfte.

Bei der Beurteilung der anzuwendenden Massnahmen ist zu berücksichtigten, ob das gewählte Verfahren auch das mildeste einsetzbare Mittel ist, um den Zweck der Erreichung des Sicherheitsmassstabes zu erfüllen.

Die alleinige Berücksichtigung der Verfahren NFC (ohne Referenzüberweisung) oder Dokumentenscan mit Referenzüberweisung wäre nur dann erforderlich, wenn die Sicherheitsanforderung nicht durch weitere Möglichkeiten der Sicherheitsüberprüfung ebenso gut befriedigt werden könnte.

Es sind also andere vergleichbare Verfahren zur Beurteilung heranzuziehen, die bereits jetzt als gleich geeignet ohne Referenzüberweisung für die Eröffnung eines Bankkontos angesehen werden können und somit als den Anforderungen entsprechendes Mittel zur Erreichung des Sicherheitsinteresses gelten können.

Als Vergleichsmassstab ist die Prüfung durch einen Menschen unter physischer Anwesenheit oder die anerkannte Video-Identifizierung heranzuziehen, bei der es ebenfalls keines NFC Scans und keiner Referenzüberweisung bedarf. Ein Autoidentverfahren nach neuestem Stand der Technik kommt es dieser gleich oder übertrifft sie sogar in seiner Zuverlässigkeit, so sollte also auch das Auto-Ident Verfahren ohne Referenzüberweisung als gleich geeignet akzeptiert werden.

III. Verfahrensvergleich

Als Experten im Bereich der Identitätsprüfung haben wir die derzeit bereits von der FINMA anerkannten Methoden im Detail analysiert. Hierzu gehören die rein menschliche Kontrolle unter Anwesenden sowie die derzeit akzeptierte Form der Onlineidentifikation.

Das online Verfahren nach neuestem Stand der Technik übertrifft die Möglichkeiten der persönlichen Vorsprache auch ohne das Auslesen des Chips und ohne Referenzüberweisung und sollte daher ebenso in einer Ergänzung der Online-Identifizierung Berücksichtigung finden.

1. Bei der Identitätsprüfung zu berücksichtigende Kriterien

Um einen Vergleich der verschiedenen Verfahren auf ihre Geeignetheit vornehmen zu können, ist zunächst wichtig zu verstehen, welche Kriterien ein menschliches oder automatisches Verfahren zu bestehen hat, um die Identität eines Menschen anhand seines Personaldokuments zu verifizieren:

a) Sicherheitsmerkmale des Identitätsdokuments

Ein modernes Identitätsdokument weist zahlreiche Sicherheitsmerkmale auf, die die zu überprüfende Stelle zu kontrollieren hat. Dabei handelt es sich insbesondere um:

- Haptik des Dokuments (Plastik- oder Papierart, Beschädigungen oder Abnutzungen)
- Umfang des Dokumentes (Seitenanzahl)
- Optik des Dokuments (Farben, Kontraste, VIZ[1])
- Machine Readable Zone (MRZ[2]), die nach bestimmten Vorgaben gestaltet ist, einschliesslich Prüfziffer
- Sicherheitsmerkmale (Hologramme, Kippbilder, Kinematische Effekte, Farbgebung, Mikroschriften etc.)
- Lichtbild

b) Erscheinungsbild der zu überprüfenden Person

Personen zu erkennen, zu erkennen, ob es sich bei einer auf einem Lichtbild abgebildeten Person um dieselbe Person handelt und ob diese Person lebendig und tatsächlich anwesend ist, muss ebenfalls von den Überprüfungsverfahren kontrolliert werden können. Hierbei sind insbesondere folgende Aspekte zu berücksichtigen. Eine Person kann sich in vielerlei Hinsicht vom Bild unterscheiden:

- Alter
- Hautfarbe
- Haartracht
- Barttracht
- Brille

1 VIZ =”visual inspection Zone”

2 MRZ = “Machine readable Zone”

c) Missbrauchsszenarien

Sowohl beim Dokument wie auch bei Personen sind diverse Missbrauchsszenarien denkbar, die im Rahmen einer Identifizierung bestmöglich erkannt werden sollten.

In Bezug auf das Dokument:

- Verfälschung von bestimmten Informationen auf dem echten Dokument (z.B. Retuschen an Textelementen)
- Einfügen von echten Seiten eines anderen Dokumentes
- Entfernen von Seiten oder bestimmten Informationen
- Auftragen von falschen Sicherheitsmerkmalen
- Digitale Veränderungen auf einem Lichtbild eines echten Dokumentes
- Austausch des Lichtbildes
- Gestohlene Dokumentenrohlinge
- Illegal erworbene echte Dokumente
- Fantasiedokumente von erfundenen Ausstellungsbehörden

In Bezug auf die Person:

- Nutzung von Fotos, Videos oder digital animierten Gesichtern einer anderen Person durch einen Unbefugten
- Täuschend echte kosmetische Anpassungen (z.B. von Silikonmasken)
- Zwangsausübung gegenüber einer Person

d) Gefährdungsstufen

Nicht alle oben dargestellten Missbrauchsszenarien sind gleich häufig und gleich komplex. Auch dies ist bei der Beurteilung der geeigneten Massnahmen zu berücksichtigen.

Level 1 – extrem anspruchsvolle und hochentwickelte Betrugsversuche. (Erwerb von Dokumentenrohlingen, echte Dokumente mit Falschinformationen durch Täuschung und sozialer Manipulation.)

Level 2 – anspruchsvolle aber durch hochqualifizierte Experten oder mit technischen Mitteln erkennbare Dokumentenfälschungen oder Verfälschungen

Level 3 - einfache oder mangelhafte Dokumentenfälschungen oder Verfälschungen die z.B. durch Checksummenprüfung oder MRZ / VIZ Abgleich auffallen können

Level 4 – einfache, schlichte Amateurversuche (Fantasiedokumente oder einfache Verfälschungen wie aufgeklebte Elemente)

2. Manipulationsmöglichkeiten

Möglichkeiten der einzelnen zu vergleichenden Identifizierungsverfahren, Manipulationen auf Ebene der verschiedenen Gefährdungsstufen zu erkennen:

a) Mensch

Vorteile des Menschen

Der Mensch hat den Vorteil der direkten Begegnung mit dem Gegenüber und bei physischer Anwesenheit im Vergleich zu online Verfahren die Möglichkeit, das Dokument selbst in die Hand zu nehmen, sowie mit dem anderen Menschen zu sprechen und ihn anzusehen. Die Liste der Vorteile ist aber im Vergleich zur nachfolgenden Liste der Defizite eher kurz. Ausserdem dürften die Vorteile des Menschen schon bei der Videoidentifikation, wo sich Kunde und Agent nur per Videochat begegnen, weitaus geringer ausfallen.

Bessere Fähigkeit haptischer Prüfung

Im Vorteil ist der Mensch daher allenfalls bei haptisch erkennbaren Fälschungen unter Anwesenden also allenfalls bei den Gefährdungen des Levels 3 und 4.

Bessere Fähigkeit zur Erkennung eines lebenden und nicht kosmetisch veränderten Menschen

Sollte ein Mensch sich durch kosmetische Massnahmen (Schminken, Silikonmasken) versuchen einem anderen anzugleichen, mag dies aufgrund der Mimik eher auffallen. Wobei man erwähnen muss, dass es hier bereits ausgesprochen ausgefeilte Techniken in der Maskenbildnerei gibt, die selbst einem Menschen kaum noch auffallen können. Biometrische Merkmale, die ein technisches System erkennen kann, können zudem auch kosmetisch nicht verändert werden.

Bessere Fähigkeit zur Erkennung von Drucksituationen

Ferner ist ein Mensch vermutlich empathischer bei der Beurteilung ob ein Mensch unter Druck ggf. eines Dritten stand, eine Transaktion vorzunehmen.

Defizite des Menschen

Den genannten Vorteilen stehen eine Reihe von Defiziten gegenüber.

Wie schwierig es für einen Menschen ist, eine vor ihm stehende Person mit einem Foto derselben Person abzugleichen, dürfte schon jedem einmal bewusst geworden sein, wenn er z.B. jemanden auf einem Gruppenfoto heraussuchen sollte oder ihm ein Jugendfoto eines anderen gezeigt wird. Darüber hinaus ergeben sich nachfolgende Defizite:

Umfassendes Schulungserfordernis und Erfahrung bei der Gesichtserkennung

Es bedarf umfassender Schulungen und Erfahrung bei der Erkennung charakteristischer Merkmale, wie Augenabstand, Haaransatz, Ohrenform etc., um einen Menschen wirklich genau erkennen zu können. Nicht umsonst besteht z.T. in einigen Ländern die Pflicht, Mitarbeiter in Callcentern, die eine Videoidentifizierung durchführen sollen, durch polizeiliche Stellen zu schulen.

Folgend einige Beispiele für Personenvergleiche, die ein maschinelles System zuverlässig erkennt - bei den Beispielen, markiert mit “X”, handelt es sich nicht um dieselbe Person:

Menschliche Schwächen, Stresssituationen

Menschen sind je nach Arbeitssituation und Arbeitsleistung nicht immer gleichermassen konzentriert und leistungsfähig. Hinzu kommt die mögliche Stresssituation beim persönlichen Kontakt mit einem anderen Menschen, wo es unter Umständen auch aus zeitlichen Gesichtspunkten nicht immer möglich ist, genauestens hinzusehen. Auch können Menschen je nach zu erwartendem Geschäftsabschluss geneigt sein, bei der Genauigkeit “ein Auge zuzudrücken”.

Keine aktive Kenntnis aller verfügbaren Dokumente und angewandter Sicherheitsmerkmale

Kein Mensch kann die Vielzahl offizieller (auch ausländischer, aus 195 Ländern) Dokumente alle bereits gesehen haben, kennen und deren Echtheit zweifelsfrei beurteilen. Auch die komplexen Sicherheitsmerkmale, die teilweise selbst bei Dokumenten derselben Art oder desselben Landes nicht immer einheitlich sind, sind Menschen nicht immer alle bekannt und von ihnen beurteilbar, insbesondere nicht innerhalb eines wirtschaftlich abbildbaren Zeitrahmens. Ferner kann ein Mensch nicht die Checksumme der MRZ prüfen.

Keine Nachbearbeitung möglich

Ein Kunde der weg ist, kann nicht mehr überprüft werden.

Kostenfaktor

Menschliche Arbeitskraft ist überdies wesentlich teurer als automatisierte Verfahren.

b) Maschine

Während sich die menschlichen Fähigkeiten qua eigener Erfahrung leicht beurteilen lassen, ist zur Beurteilung der Fähigkeiten automatisierter Verfahren zunächst eine Erläuterung des gegenwärtigen Stands der Technik erforderlich. Diese gehen aufgrund weitentwickelter Bildanalysetechniken weit über die Möglichkeiten herkömmlicher Foto-Identverfahren, bei denen nur ein Einzelbild abfotografiert wurde, hinaus.

Vorteile nach dem Stand der Technik bei KI-basierten Identifizierungsverfahren

Mit dem Einsatz der höchsten Standards der maschinellen Identitätsprüfung, kombiniert mit manuellen Unterstützungsprozessen und unter Anwendung von differenzierten Logiken zur Beurteilung der Resultate, sind wir überzeugt, dass das Auto-Ident Verfahren der Sicherheit und Zuverlässigkeit einer Videoidentifikation oder physischen Präsenz mindestens gleichkommt.

Dokumentenprüfung:

Um Betrugsversuche bei Identitätsdokumenten zu erkennen und zu unterbinden, bestehen folgende Massnahmen bei aktuell eingesetzten Auto-Ident Verfahren:

Erfassung Lichtbild:

- Das Lichtbild wird als Videosequenz, und nicht als einzelnes Lichtbild erfasst. Somit können die folgenden Analysen basierend auf mehreren Bildern (Frames) durchgeführt werden, und Sicherheitsmerkmale geprüft werden. Solche Sicherheits-Checks sind basierend auf einem einzelnen Bild nicht verlässlich.
- Es wird sichergestellt, dass die Lichtbildaufnahme live während des Prozesses der Identitätsprüfung aufgenommen wird. Früher aufgenommene Bilder/Videos sind nicht zulässig.
- Es wird sichergestellt, dass während der Videoaufnahme das Dokument nicht aus der Kamerasicht entfernt wird und möglicherweise mit einem anderen Dokument ausgetauscht wird.

Qualitätsprüfung Lichtbild:

- Das Lichtbild muss in möglichst hoher Auflösung aufgenommen werden, und es wird sichergestellt, dass alles nötigen Prüfungen durchgeführt werden können.
- Das Bild darf nicht verschwommen sein und das gesamte Dokument muss ersichtlich sein, Dokumentenränder dürfen nicht abgeschnitten sein.
- Das Nutzerinterface weist den Nutzer entsprechend auf Verbesserungsmöglichkeiten von Auflösung und Beleuchtung hin.

Überprüfung Datenintegrität:

- Die Informationen des Dokumentes werden sowohl aus der MRZ, als auch aus der VIZ extrahiert
- Die MRZ wird automatisch auf Ihre Checksumme geprüft
- Die MRZ kann zusätzlich auf Syntax und Logik überprüft werden
- Bestimmte Informationen aus der MRZ (z.B. Dokumentennummer, Geburtstag, Ablaufjahr) werden mit den Informationen aus der VIZ verglichen
- Wenn vorhanden, wird der biometrische Chip zusätzlich ausgelesen und die Informationen können mit denjenigen aus dem Lichtbild automatisiert und aufgrund zuverlässiger Algorithmen verglichen werden

Visuelle Echtheitsprüfung:

- Das Lichtbild des Dokuments wird mit einer Referenz, einem sogenannten Template verglichen. Hierbei werden zahlreiche visuelle Merkmale (z.B .Ecken, Kanten, Datenfelder, Hintergrundmuster, Flaggen etc.) identifiziert und abgeglichen, um eine möglichst hohe Übereinstimmung zu erhalten
- Physische Sicherheitsmerkmale, insbesondere Hologramme/Kinegramme und Kippbilder, werden erkannt und auf ihre Integrität geprüft. Hierbei wird sichergestellt, dass z.B. die Struktur, der Farbverlauf und das Reflektionsverhalten unter verschiedenen Winkeln, der Referenz entspricht. Bei Kippbildern werden zudem, sofern vorhanden, hinterlegte Informationen (z.B. Dokumentennummer und Ablaufjahr bei der Schweizer ID ausgelesen und gegen die Informationen der MRZ verglichen. Ein maschinelles System kann Sicherheitsmerkmale wie Hologramme und Kippbilder zuverlässig auf Echtheit prüfen, indem eine Mehrzahl von erfassten Lichtbildern aus verschiedenen Winkeln in Echtzeit erfasst und analysiert werden. Hierzu bewegt der Nutzer das Smartphone oder das Dokument in verschiedene Richtungen, um Lichtbilder von den relevanten Winkeln zu erfassen. Um zu bestimmen, welche Lichtbilder für eine zuverlässige Analyse des Sicherheitsmerkmals erforderlich sind, muss die Lösung die erkannten Kernmerkmale des Dokumentes verfolgen (Tracking) und in Echtzeit die richtigen Winkel errechnen. Basierend auf dem

vorliegenden Dokumententyp, unterscheidet die Lösung, welche Hologramm-Druckmuster abgeglichen werden muss.

- Andere Prüfungen, wie z.B. die Feststellung von Anomalien der Schriftart und Schriftgrösse, die korrekte Rundung der Ecken des Dokuments, die Druckfarben etc. sind gemäss unserer Tests und unserer Erfahrung mit hunderttausenden von Dokumenten nicht genügend zuverlässig.

Echtheitsbestimmung einer realen Person:

Um im nächsten Schritt die Zugehörigkeit des Dokumentes und des Nutzers zu gewährleisten, muss das maschinelle Verfahren in der Lage sein zu bestimmen, dass das Lichtbild des Nutzers eine echte, reale Person zeigt und nicht ein Fälschungsversuch vorliegt. Dieser Vorgang wird als Liveness Detection bezeichnet. Eine Fälschung liegt vor, wenn der Nutzer z.B. einen Fotodruck oder eine Videoaufnahme einer anderen Person aufnimmt, ein digital animiertes Gesicht abspielt (Deep Fake) oder 2D oder 3D Masken trägt.

Nach dem aktuellen Stand der Technik verfügen Auto-Ident Verfahren in dieser Hinsicht über folgende Funktionalitäten:

Erfassung Lichtbild:

- Das Lichtbild wird als Videosequenz, und nicht als einzelnes Lichtbild erfasst. Somit können die folgenden Analysen basierend auf mehreren Bildern durchgeführt werden, und die Liveness geprüft werden. Dies ist basierend auf einem einzelnen Bild nicht verlässlich.
- Es wird sichergestellt, dass die Lichtbildaufnahme live während des Prozesses der Identitätsprüfung aufgenommen wird. Früher aufgenommene Bilder/Videos sind nicht zulässig.
- Es wird sichergestellt, dass während der Videoaufnahme das Gesicht nicht aus der Kamerasicht entfernt wird und möglicherweise mit einem anderen Gesicht ausgetauscht wird.

Liveness Detection:

- Das maschinelle Verfahren prüft basierend auf dem erfassten Lichtbild, ob es sich um ein Fälschungsversuch handelt und errechnet den Konfidenzwert.

Zugehörigkeitsbestimmung:

Wenn festgestellt ist, dass es sich um ein echtes Dokument und eine echte Person handelt, wird die Zugehörigkeit des Dokuments zum Nutzer bestimmt. Hierzu werden Algorithmen zur Gesichtserkennung angewendet, um das Gesicht des Dokumentenlichtbilds mit dem Gesicht des Nutzers automatisiert und zuverlässig zu vergleichen:

Erfassung Lichtbild:

- Für den Vergleich wird das Gesicht des vorgängig erfassten Lichtbilds genutzt. Andernfalls können Betrüger für die Liveness Detection das eigene Gesicht hernehmen und für die Gesichtserkennung dann ein Foto vorhalten.

Gesichtserkennung:

- Der Algorithmus vergleicht das Gesicht des Dokumentenfotos mit dem Gesicht des erfassten Videos und errechnet den Konfidenzwert.

Nachkontrollmöglichkeit

Selbst im Fall uneindeutiger Identifizierungen bietet das Auto-Ident Verfahren, gemäss unserem Vorschlag, eine Möglichkeit der Überprüfung des Ergebnisses durch einen Mitarbeiter des Finanzdienstleisters, mit Unterstützung von zusätzlichen technischen Hilfsmitteln, wie Referenzdatenbanken zugreifen kann.

Diese Nachkontrollmöglichkeit hat zudem den weiteren Vorteil, dass auch im Falle späterer Probleme der Kontrollprozess anhand gespeicherter Bilddaten nachvollzogen werden kann, dokumentiert ist und ggf. auch Ermittlungen unterstützt werden können.

Nachteile der maschinellen Identifikation

Die Nachteile der maschinellen Identifikation beschränken sich auf folgende Punkte:

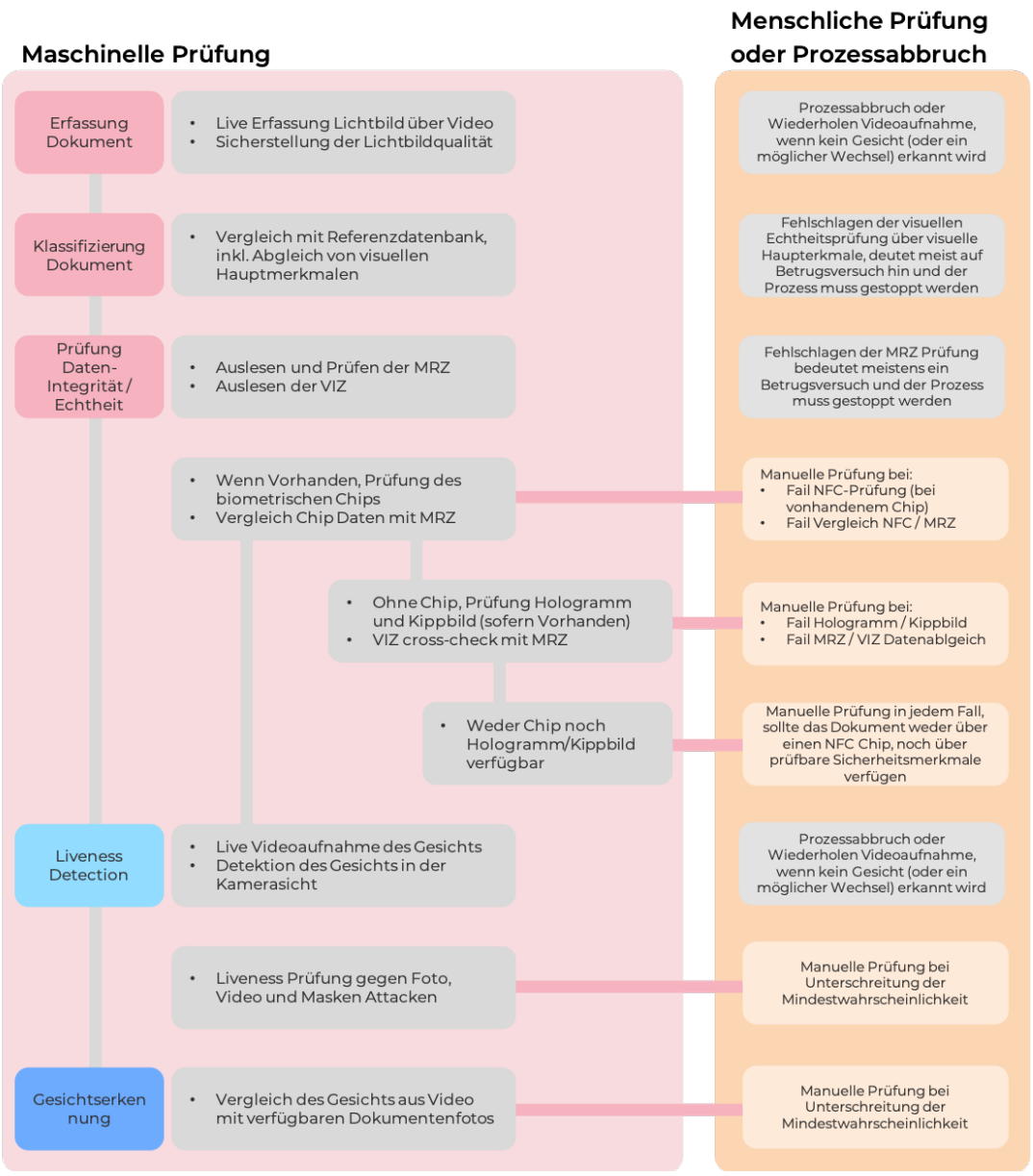
- erhöhter Trainingsaufwand der selbstlernenden Systeme
- fehlender Zugang zu haptischen Prüfungsmethoden
- Kein verfügbarer Standard, wie Resultate angegeben und interpretiert werden sollten

Unser Vorschlag eines hybriden, automationsunterstützenden Verfahrens, mit Einbezug einer menschlichen Nachbearbeitung schliesst unser Erachten die Lücken der Videoidentifikation aber auch der heutigen Onlineidentifikation und bieten einen skalierbaren, praktikablen Ansatz für die gesamte Branche. Wir sind überzeugt, dass eine automationsunterstützende Prüfung, in Kombination mit der menschlichen Beurteilung, und unter Einbezug heuristischer Regelungen, das zuverlässigste Verfahren der Identitätsprüfung ist. Folgend zeigen wir unseren Vorschlag eines Verfahrens zur Anerkennung von der FINMA. Dieser nutzt eine grundsätzliche maschinelle Prüfung, gemäss den unten beschriebenen Verfahren, als Basis, bezieht aber die menschliche Beurteilung mit ein, sollten Unsicherheiten auftreten oder gewisse Prozessschritte fehlschlagen.

3. Vorschlag für eine Erweiterung des Änderungsentwurfs der Online Identifikation

In Anbetracht der individuellen Vor- und Nachteile der jeweiligen Methoden sind wir der Auffassung, dass ein automationsunterstütztes Verfahren unter Einbezug einer menschlichen Nachkontrolle – diese allerdings ausschliesslich im Fall von Unsicherheiten oder bei Betrugsverdacht – und unter Einbeziehung heuristischer Regelungen, die Nachteile der zuvor genannten Verfahren auch ohne Zusatzerfordernis der Referenzüberweisung und Wohnsitzprüfung ausgleicht und einen praktikablen Ansatz für die gesamte Branche bietet.

Folgend erläutern wir unseren Vorschlag für die Erweiterung der Onlineidentifikation zur Anerkennung von der FINMA im Detail. Dieser Vorschlag erlaubt den weitergehenden Verzicht auf eine Referenzüberweisung und die Wohnsitzprüfung, und zwar nicht nur bei Anwendung der Chip-Prüfung, sondern auch dann, wenn die Echtheitsprüfung unter Zuhilfenahme optisch variabler Sicherheitsmerkmale, wie z.B. Hologramme und Kippbilder durchgeführt wird. Der Vorschlag enthält im Vergleich zu den heute beschriebenen Bestimmungen der Onlineidentifikation etwas klarere und teilweise strengere Regeln für die anzuwendenden Prüfungsmethoden. Es handelt sich bei dem unten beschriebenen Prozess grundsätzlich um ein maschinelles Verfahren, bezieht aber in kritischen Einzelfällen die menschliche Beurteilung mit ein, sollten Unsicherheiten auftreten oder gewisse Prozessschritte fehlschlagen.



4. Abgleich der Geeignetheit der Verfahren zur sicheren Identifizierung von Personen

Der folgende Vergleich wurde basierend auf den zu interpretierenden Mindestmassnahmen aus den entsprechenden FINMA Richtlinien erstellt. Die anerkannte Onlineidentifikation, auch in der Ausführung des FINMA Änderungsvorschlags, bietet unseres Erachtens bereits heute eine zumindest gleichwertige Zuverlässigkeit wie die Videoidentifikation oder die Identifikation bei physischer Präsenz. Sogar bietet der heutige Stand der Technik Möglichkeiten, dieses Verfahren auszubauen, um eine erhöhte Sicherheit und Zuverlässigkeit der Online-Identifikation zu erlangen und Interpretationsspielräume zu minimieren. Hierzu verweisen wir auf das oben beschriebene Verfahren gemäss unserem Vorschlag einer anzuerkennenden Erweiterung der Onlineidentifikation. Diese beinhaltet insbesondere - sollte kein Dokumentenchip zur Prüfung vorhanden sein - eine Prüfung der optisch variablen Sicherheitsmerkmale sowie eine menschliche Nachkontrolle bei Unsicherheiten.

Folgende Übersicht stellt nochmals tabellarisch die wesentlichen Unterschiede dar und zeigt klar an, dass maschinelle Verfahren auf dem derzeitigen Stand der Technik die Möglichkeiten menschlicher Kontrolle überwiegen.

	Phyische Präsenz	Video Identifikation	Online Identifikation heute	Online Identifikation gem. PXL Vorschlag
Verfälschungen der MRZ				
Verfälschungen der VIZ				
Einfügen von echten Seiten eines Anderen Dokumentes				
Auftragen von falschen Sicherheitsmerkmalen				
Digitale Veränderungen auf einem Lichtbild				
Gefälschte Dokumente				
Gestohlene Rohlinge				
Illegal erworbene echte Dokumente				
Ungültige Dokumente und Spezimen				
Betrüger hält ein Foto oder Video einer anderen Person vor				
Betrüger spielt ein digital animiertes Gesicht vor				
Betrüger trägt eine Maske				
Betrüger wechselt das Gesicht zwischen der Liveness Detection und der Gesichtserkennung				
Betrüger nutzt ein gestohlenes Dokument				

Selbst die noch erkennbaren Vorteile einer physischen Präsenz dürften angesichts der zahlreichen Zusatzmöglichkeiten der elektronischen Verfahren kaum noch ins Gewicht fallen.

Haptischer Kontakt mit Dokumenten, der grösste Vorteil der menschlichen Kontrolle, ist letztlich im Grunde nur bei sehr plumpen Fälschungen von Vorteil. Wenn also z.B., wenn ein Fälscher Papier statt eine Plastikkarte nutzt, er ein Foto überklebt oder sonstige physikalische Veränderungen an einem Dokument vornimmt.

Für die Erkennung solcher Fälschungen gibt es ebenfalls technische Lösungen, die z.B. durch das Erkennen von Schatteneffekten oder Auflösungsanalysen der Bildränder Fälschungen erkennbar machen.

Ansonsten bieten die maschinellen Prozesse weitaus mehr Möglichkeiten als sie ein Mensch je hätte, so kann z.B. kein Mensch die Prüfziffern aus der MRZ nachrechnen oder die Echtheit eines Hologramms erkennen.

Auch ist es, wie gesagt, von Bedeutung, dass die Kontrolle durch einen Menschen ein flüchtiger und später nicht mehr nachvollziehbarer Vorgang ist. Elektronische Verfahren bieten selbst in einem nicht erkannten Missbrauchsfall noch zahlreiche Daten für Ermittlungen.

Neben dem Verfahrensvergleich sei aber noch auf weitere Kriterien hingewiesen, die Vorteil einer erweiterten Anwendbarkeit von Identifizierungsverfahren wären:

Prozesse, z.B. die Eröffnung eines Kontos, für den Verbraucher so einfach und zeitnah wie möglich gestaltet werden. Wenn dieser nur vor die Alternative des Einsatzes eines NFC Chips oder einer Referenzüberweisung gestellt wird, werden unverhältnismässige Hürden sowohl für ihn als auch für die Bankinstitute aufgestellt:

- Die Schweizer Identitätskarte enthält bis heute keinen Chip
- Nicht alle Schweizer haben einen Pass, geschweige denn einen mit einem NFC Chip.
- Viele Nutzer sind mit dem Einsatz des Chips und der Auslesemöglichkeit über ein Lesegerät oder Smartphone überfordert, so dass es zu Transaktionsabbrüchen kommen wird
- Endkunden, die nicht bereits über ein den Anforderungen genügendes Bankkonto verfügen (Ausländer oder Minderjährige), können auch keine Referenzüberweisung veranlassen
- Für Banken bedeutet die Prüfung der Referenzüberweisung den Zugriff auf ein Konto eines wettbewerbenden Instituts, und der Kunde könnte es als störend empfinden, wenn er offenlegen muss, mit welcher Bank er sonst noch eine Geschäftsbeziehung hat.
- Neben den o.g. zeitlichen und prozessualen Umständen sind selbstverständlich auch noch die höheren Transaktionskosten zu beachten. je einfacher ein Verfahren ist, desto weniger Kosten entstehen dem Kunden und dem Finanzdienstleister

5. Sonstige Aspekte

Dieses Dokument konzentriert sich hauptsächlich auf die Beurteilung und Anerkennung von Methoden und deren Sicherheit zur Identitätsprüfung.

Bei der Ausarbeitung von anerkannten, für die Branche praktikablen Ansätzen der Identitätsprüfung ist die Sicherheit der Lösung sicherlich zentral, allerdings sollten auch gesamtheitlich die folgenden Faktoren beachtet werden, um die Branche zu unterstützen:

Kosten:

Bei der Beurteilung von anerkannten Methoden sind die Kosten mit zu berücksichtigen. Manuelle, durch Menschen durchgeführte Prüfungen führen zu hohen Prozesskosten. Maschinelle Unterstützung des Prozesses kann diese Kosten senken und eine weitere Verbreitung der Methode begünstigen. Zudem helfen geringe Prozesskosten, z.B. bei einer Kontoeröffnung, neue digitale Geschäftsmodelle zu entwickeln und sie können somit als Innovationstreiber, z.B. für Neobanken und FinTechs dienen.

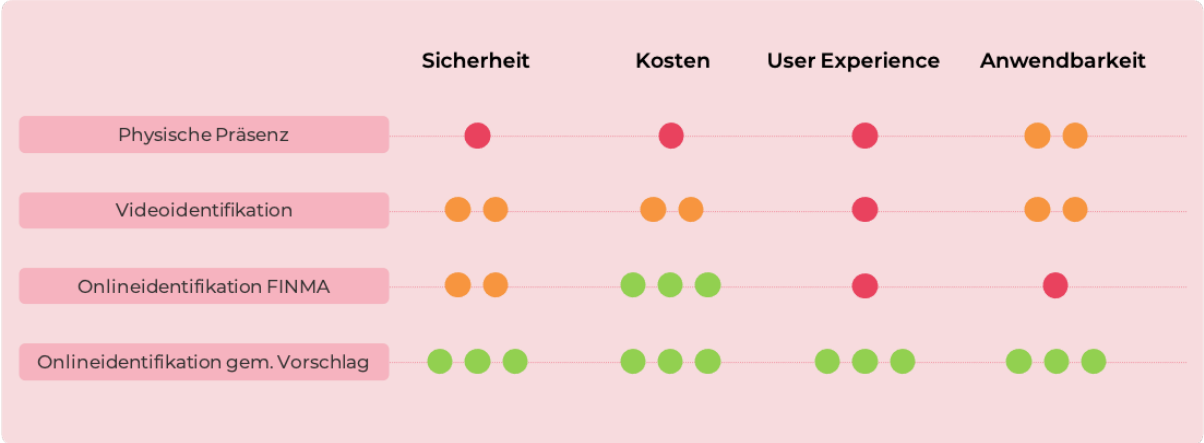
Benutzerfreundlichkeit:

Eine Methode zur Identitätsprüfung sollte möglichst einfach und schnell durchgeführt werden können. Komplizierte und mühselige Methoden können zu Prozessabbrüchen führen. Benutzerfreundliche Lösungen können der Branche helfen, einfacheren und schnelleren Zugang zu Finanzdienstleistungen zu bieten.

Anwendbarkeit:

Anerkannte Methoden sollten breit anwendbar und skalierbar sein und die Branche profitiert nicht, wenn eine Identitätsprüfung nur durch ein kleines Zielsegment oder nur zu limitierten Zeiten durchführbar ist. Die Banküberweisung, welche die heutige Wegweisung zur Onlineidentifikation vorgibt, ist nur von Personen mit existierendem Bankkonto innerhalb der FATF möglich, und schliesst auch u.A. alle Schweizer ohne Konto (z.B. alle im Alter unter 18 Jahren) aus. Auch der Revisionsvorschlag der FINMA unterbindet eine breite Anwendung der Onlineidentifikation, da gerade einmal die Hälfte der Schweizer Bevölkerung im Besitz eines Passes mit biometrischem Chip ist. Für alle Bewohner mit Identitätskarte ist der Prozess somit nicht anwendbar. Insbesondere in heutigen Zeiten der COVID Pandemie hat ein ortsunabhängiger Zugang zu Finanzdienstleistungen eine noch höhere Relevanz.

Sicherlich verdient der Aspekt der Sicherheit und Zuverlässigkeit eines Verfahrens die höchste Gewichtung, allerdings sind die damit verbundenen Kosten, die Benutzerfreundlichkeit und die Anwendbarkeit nicht ausser Acht zu lassen. Die folgende Grafik stellt diese Faktoren in Bezug auf die verschiedenen Verfahren im heutigen Stand in den Vergleich:



IV. Folgerungen für die Umsetzung in der Schweiz

Ein Blick über die Schweizer Grenzen hinaus zeigt, dass Länder wie Grossbritannien, Belgien, Irland und Liechtenstein, eine grössere Flexibilität bei der Anwendung von Identifizierungsprozessen erlauben, sofern hinreichende Sicherheit im Rahmen einer Risikobetrachtung gewährleistet ist.

Es sollte daher auch in der Schweiz den Finanzintermediären ermöglicht werden, einen einfachen, schnellen, medienbruchfreien und damit verhältnismässigen Onboarding Prozess durchführen zu können.

Raiffeisen Schweiz

Raiffeisenplatz 4
Postfach
9001 St.Gallen
Telefon 071 225 49 98
www.raiffeisen.ch
finma-office@raiffeisen.ch

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

Für Sie zuständig:
Gabriela Glaus, RA – 071 225 49 98

St. Gallen, 21. Januar 2021

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

Sehr geehrte Frau Grüninger

Wir beziehen uns auf die Eröffnung der Anhörung zum eingangs erwähnten FINMA-Rundschreiben (nachfolgend „RS") vom 16. November 2020 und bedanken uns für die Möglichkeit der Stellungnahme. Eingangs verweisen wir auf die Stellungnahme der Bankiervereinigung, die wir mittragen und in welcher die nachfolgend erwähnten Punkte ebenfalls berücksichtigt werden.

RZ 51

Die Präzisierung, wonach bei einem Beizug eines anderen Finanzintermediärs, welcher die Video- und Online Identifizierung durch direkt beauftragte Dienstleister vornimmt, letztere nicht als weitere Personen oder Unternehmen gelten und somit keine untersagte Weiterdelegation vorliegt, ist zu begrüssen.

Es stellt sich aber weiterhin die Frage, wie sich die Bestimmung von Rz. 51 mit Art. 43 Abs. 3 VSB 20 vereinbaren lässt. Es ist ausdrücklich zulässig, dass ein Finanzintermediär Personen und Unternehmen mit der Durchführung der Identifizierung der Vertragspartei gemäss Kapitel III und IV beauftragen kann. Gemäss Erläuterungsbericht der FINMA zum Rundschreiben 2016/7 "Video- und Onlineidentifizierung" vom 21.12.2015 steht die Möglichkeit des Beizugs Dritter gemäss Art. 28 und 29 GwV-FINMA einem Finanzintermediär für die gesamten Prozess- bzw. Verfahrensschritte der Abschnitte III, IV und V offen, oder aber nur für einzelne, ausgewählte Schritte davon.

Es ist somit zulässig, eine Person oder ein Unternehmen mit der Online-Identifizierung zu beauftragen, welche gemäss Art. 10 Abs. 2 VSB 20 der Identifizierung bei Aufnahme der Geschäftsbeziehung auf dem Korrespondenzweg gleichgestellt ist. In Art. 43 Abs. 3 VSB 20 ist jedoch ausdrücklich vorgesehen, dass im Rahmen der Delegation der Identifizierung des Vertragspartners eine Weiterdelegation sowie eine *Korrespondenzeröffnung* durch den Beauftragten ausgeschlossen sind. Somit steht Rz. 51 des RS insofern im Widerspruch zu Art. 43 Abs. 3 VSB 20, als dass das Rundschreiben eine Delegation der Online-Identifizierung an einen Dritten ausdrücklich zulässt, während die VSB untersagt, dass ein beauftragter Dritter seinerseits den Vertragspartner auf dem Korrespondenzweg identifiziert, was wie erwähnt der Online-Identifizierung entspricht.

Es wäre deshalb der Klarheit halber und im Sinne der Rechtssicherheit zu begrüssen, wenn unter Ziff. VIII. Technologieneutralität dieser Widerspruch wie unten dargestellt klargestellt bzw. präzisiert würde. Diese Präzisierung ist umso notwendiger, als dass gemäss Rz. 33.1 des revidierten RS der Finanzintermediär auf eine Banküberweisung gemäss Rz. 33 verzichten kann, falls er (bzw. der beauftragte Dritte) den Chip der biometrischen Identifizierungsdokumente mit geeignetem Hilfsmittel ausliest und die auf ihre Authentizität und Integrität geprüften Daten mit den Angaben und dem erstellten Lichtbild der Vertragspartei übereinstimmen. Somit kann der Online-Identifizierungsprozess völlig losgelöst vom delegierenden Finanzintermediär durchgeführt und abgeschlossen werden.

Verordnungsartikel und Wortlaut	Erläuterungen und Anwendungsbeispiele zur digitalen Form
Art. 35 GwV-FINMA: Für die Identifizierung der Vertragsparteien und die Feststellung der Kontrollinhaberin oder des Kontrollinhabers und der an Vermögenswerten wirtschaftlich berechtigten Person gelten für Banken und Effektenhändler die Bestimmungen der Vereinbarung vom 13. Juni 2018 über die Standesregeln zur Sorgfaltspflicht der Banken (VSB 20). *Via Art. 35 GwV-FINMA sind für Banken und Wertpapierhäuser[1] in diesem Zusammenhang u.a. folgende Artikel in der VSB relevant:* Art. 10 Abs. 3 VSB: Der Identifizierung bei Aufnahme der Geschäftsbeziehung auf dem Korrespondenzweg gleichgestellt ist die Online-Identifizierung gemäss den jeweils geltenden FINMA-Vorschriften. Art. 43 Abs. 3 VSB: Eine Weiterdelegation sowie eine Korrespondenzeröffnung durch den Beauftragten sind ausgeschlossen.	Zieht ein Finanzintermediär einen Dritten zwecks Durchführung der Online-Identifizierung gemäss Ziff. IV. Lit. B. bei, kann dieser im Rahmen der Delegation sämtliche Prozess- und Verfahrensschritte durchführen. Eine Identifizierung auf dem Korrespondenzweg mittels Durchführung der Online-Identifizierung durch den beauftragten Dritten ist somit zulässig.

Eröffnung von Geschäftsbeziehungen für Minderjährige durch eine mündige Drittperson

Die Eröffnung einer Geschäftsbeziehung, lautend auf einen Minderjährigen, kann entweder durch eine mündige Drittperson oder durch den Minderjährigen selbst erfolgen, wobei Vertragspartner in beiden Fällen der Minderjährige ist. Wenn der Minderjährige die Geschäftsbeziehung selbst eröffnet, identifiziert die Bank den Minderjährigen, während bei Eröffnung durch die mündige Drittperson die Bank hingegen diese Person identifizieren muss (Art. 18 lit. a VSB).

Gemäss dem Wortlaut im RS beziehen sich die Identifikationsschritte ausschliesslich auf den *Vertragspartner*. Das würde unserem Verständnis nach in der Konsequenz bedeuten, dass im Rahmen der Kontoeröffnung für einen Minderjährigen durch eine mündige Drittperson von der Möglichkeit der Video- und Online-Identifizierung nicht Gebrauch gemacht werden kann, da es sich bei der zu identifizierenden Person nicht um den Vertragspartner handelt.

Es wäre deshalb auch hier der Klarheit halber und im Sinne der Rechtssicherheit zu begrüssen, wenn unter Ziff. VIII. Technologieneutralität klargestellt wird, dass auch einer mündigen Drittperson in der oben erwähnten Konstellation die Möglichkeit der Video- und der Online-Identifizierung offen steht und das RS entsprechend präzisiert bzw. angepasst wird.

Im Übrigen sind wir mit den geplanten Änderungen einverstanden.

Wir hoffen Ihnen mit unseren Ausführungen gedient zu haben und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Raiffeisen Schweiz

Alexandra Klingler-Härtsch
Leiterin Compliance

Gabriela Glaus
FINMA-Office

[1] Terminologie in der GwV-FINMA sollte entsprechend Art. 2 Abs. 2 lit. d GwG generell angepasst werden (Substitution „Effektenhändler" durch „Wertpapierhäuser").

Kopie an:

- PricewaterhouseCoopers (CH_Raiffeisen_Coordination@pwc.ch)
- Ernst & Young (eych.raiffeisen.audit@ch.ey.com)

Elektronisch

Eidgenössische Finanzmarktaufsicht FINMA
z.H. Frau Isabel Grüninger
Laupenstrasse 27
3003 Bern
Schweiz

Zürich, 01. Februar 2021

Betreff: Stellungnahme zum Entwurf der Teilrevision des FINMA-Rundschreibens 2016/7 „Video- und Online-Identifizierung"

Sehr geehrte Frau Grüninger,

bezugnehmend auf Ihre Einladung zur Stellungnahme zum Entwurf der Teilrevision des RS 2016/7, lassen wir Ihnen in der Beilage unsere konstruktiven Bemerkungen und Anregungen zukommen.

Freundliche Grüsse
ROCKON Digital Evolution AG

Roland Rüttimann	Adriana Bogdanova
CEO	Legal & Compliance

BEILAGE:

a) Stellungnahme

STELLUNGNAHME

1. ALLGEMEIN

Wir begrüssen, dass sich die FINMA wiederkehrend mit dem technologischen Wandel auseinandersetzt und diese in den verschiedensten Rundschreiben miteinfliessen lässt. Dies sichert eine stetige Weiterentwicklung des Schweizer Finanzmarktes und die Wettbewerbsfähigkeit gegenüber anderen Europäischen Ländern.

2. STELLUNGNAHME ZUR RANDZIFFER 33.1

«Der Finanzintermediär kann auf eine Banküberweisung gemäss Rz 33 verzichten, falls er den Chip der biometrischen Identifizierungsdokumente mit geeignetem Hilfsmittel ausliest und die auf ihre Authentizität und Integrität geprüften Daten mit den Angaben und dem erstellten Lichtbild der Vertragspartei übereinstimmen.»

Das beschriebene Verfahren der Chip-Auslesung anstelle der Banküberweisung in Rz33.1 stellt sicher eine gute Alternative dar und hebt das Sicherheitsniveau der Online-Identifizierung gleichzeitig an. Die Formulierung *«geprüfte Daten»* lässt unserer Meinung nach jedoch sehr viel Spielraum für Interpretationen, da sich die auf einem Chip enthaltenen Daten eines biometrischen Identifizierungsdokuments, je nach Herausgeberland deutlich unterscheiden können. Zum besseren Verständnis wäre es sinnvoll eine Auflistung der Daten, welche ausgelesen werden dürfen, in der Rz33.1 miteinfliessen zu lassen.

Des Weiteren bringt der Wortlaut «Authentizität und Integrität» und die dazugehörige Erklärung im Erläuterungsbericht (vgl. S.8), die Verifizierung der eSignatur auf dem Chip der biometrischen Identifizierungsdokumente mit sich. Dies stellt abhängig der zu unterstützenden Ausweisen, ein nicht zu unterschätzendes Erschwernis dar, da eine Public-Key-Authentifizierung mit dem jeweiligen Herausgeberland vorzunehmen wäre. Hier wäre zu erwägen, ob diese Überprüfung nicht gänzlich zu streichen ist, da durch die anderen begleitenden Sicherheitsüberprüfungen, genügend Daten vorliegen, um die Identität einer Person zu bestätigen.

SwissBanking

Eidgenössische Finanzmarktaufsicht FINMA
Isabel Grüninger
Laupenstrasse 27
CH-3003 Bern

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

Basel, 01.02.2021
EGY | +41 58 330 62 64

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

Sehr geehrte Frau Grüninger
Sehr geehrte Damen und Herren

Wir beziehen uns auf die oberwähnte, am 16. November 2020 eröffnete Anhörung.

Wir bedanken uns bestens für die Konsultation in dieser für die Finanzbranche wichtigen Angelegenheit. Gerne nehmen wir die Gelegenheit zur Stellungnahme wahr und unterbreiten Ihnen nachfolgend unsere Anliegen.

I. Allgemeines

Wir begrüssen, dass die FINMA dem technologischen Wandel Rechnung trägt und neue Möglichkeiten für die Online-Identifizierung vorsieht. Auch unterstützen wir das Ziel, mit der Online-Identifizierung einen vollautomatisierten und dennoch sicheren Eröffnungsprozess zu gewährleisten. Entgegen der Einschätzung der FINMA ist dies unseres Erachtens mit den vorgesehenen Anpassungen aber noch nicht vollständig möglich. Aus unserer Sicht bieten neue Technologien, künstliche Intelligenz bzw. *Machine Learning* aber auch Kameraspezifikationen moderner Smartphones bereits mehr Möglichkeiten als der *Chip Scan*.

II. Zur Online-Identifizierung

II.1 Zur Prozessvariante «Auslesen des Chips» Rz. 31 ff.

Im *Chip Scan* sehen wir eine sinnvolle Alternative zur Banküberweisung. Tatsächlich ist die Banküberweisung und somit die Freigabe des Kontos vor dem eigentlichen Abschluss der

Identifikation ein risikoerhöhender Faktor, der viele Banken von einer Online-Identifizierung bisher abgehalten hat. Leider ist der *Chip Scan* in der Praxis aufgrund der tatsächlichen Verbreitung der NFC Chips limitiert. In der Schweiz sind Pässe und gewisse Ausländerausweise mit den entsprechenden Chips ausgestattet. Schweizer Identitätskarten verfügen jedoch über keinen NFC Chip und es ist derzeit nicht absehbar, dass ein solcher für Identitätskarten vorgesehen ist. Gerade im wenig risikoreichen Schweizer Retail Segment sind Identitätskarten sehr beliebt und häufig eingesetzt. Um diesem Umstand Rechnung zu tragen, sollten Ausweisdokumente, die nicht biometrische Identifizierungsmerkmale enthalten, trotzdem ohne das zusätzliche Erfordernis einer Banküberweisung verwendet werden können. Anstatt des *Chip Scans* oder anderen Mitteln zur Auswertung der biometrischen Daten müsste folglich eine oder mehrere alternative Sicherheitsmassnahmen (siehe Vorschläge in Ziff. III) zur Anwendung gelangen.

Im Hinblick auf die Berücksichtigung von Schweizer Identitätskarten sowie den technologischen Entwicklungen befürworten wir eine offenere Formulierung der neuen Rz. 31.1:

FINMA-RS 2016/7, Rz. 31.1

«Der Finanzintermediär kann auf eine Banküberweisung gemäss Rz 33 verzichten, falls er die im Ausweisdokument enthaltenen biometrischen Identifizierungsmerkmale bspw. mittels Chips Scan oder mit anderen geeignetem Hilfsmittel ausliest und die auf ihre Authentizität und Integrität geprüften Daten mit den Angaben und dem erstellten Lichtbild der Vertragspartei übereinstimmen. Bei Ausweisdokumenten ohne biometrische Identifizierungsmerkmale kann auf eine Banküberweisung gem. Rz. 33 verzichtet werden, wenn andere geeignete Sicherheitsmassnahmen zur Anwendung gelangen, welche eine Überprüfung der Authentizität und Integrität der geprüften Daten mit den Angaben und dem erstellten Lichtbild der Vertragspartei erlauben.»

II.2 Zur Wohnsitzüberprüfung, Rz. 34-37

Die Gleichstellung der Online-Identifikation mit der Korrespondenzeröffnung nach VSB, vor allem die Adressprüfung gemäss den Randziffern 34 bis 37 ist nicht mehr zeitgemäss und unterbricht unnötigerweise den Online-Identifizierungsprozess. So bringt bspw. die Überprüfung der Wohnsitzadresse mittels *Utility Bill* keinen Mehrwert, da die Echtheit einer elektronisch übermittelten *Utility Bill* kaum überprüfbar ist; weder durch Menschen noch durch IT-gestützte Hilfsmittel. Die Dokumente können durch Software nicht zuverlässig als Rechnung erkannt werden und ein automatischer Datenabgleich ist aufgrund fehlenden Zugriffes auf Datenbanken für zugelassene *Utility Bill*-Aussteller derzeit nicht möglich. Es bleibt im Hinblick auf eine Vollautomatisierung des Prozesses nur die Anbindung an ein öffentliches Register oder eine durch einen vertrauenswürdigen Privaten geführte Datenbank (mit den entsprechenden datenschutzrechtlichen Herausforderungen), welche aber derzeit nicht gegeben sind. Aus diesem Grund schlagen wir vor, dass zusätzlich zu den bereits bestehenden Alternativen zur Wohnsitzüberprüfung (Utility Bill,

Postzustellung, Registerprüfung) den Finanzintermediären eine weitere Möglichkeit, nämlich diejenige der Geolokalisierung, zur Verfügung stehen soll. Geolokalisierung bedeutet, dass Informationen zum Aufenthaltsort ermittelt und im Rahmen der Echtzeitübermittlung zur Plausibilisierung der Angaben der Interessenten zum Aufenthalts- oder Wohnort hinzugezogen werden können.

Demnach wäre zwischen Rz. 37 und 38 eine neue Ziffer einzufügen:

FINMA-RS 2016/7, neue Rz. nach Rz. 37

«Ferner überprüft er die Wohnsitzadresse die Vertragspartei anhand:

[…]

- eines öffentlichen Registers, der durch einen vertrauenswürdigen Privaten geführte Datenbank oder eines solchen Verzeichnisses; oder
- einer Geolokalisierung.»

III. Zu weiteren Sicherheitselementen

Die aktuellen technologischen Möglichkeiten bieten zusätzliche, im Rundschreiben noch nicht enthaltene, flankierende Sicherheitsvorkehrungen, die unseres Erachtens die bisherigen ergänzen bzw. ohne Nachteil ersetzen können. Es wäre wünschenswert, wenn die Online-Identifizierung zukünftig ohne Systembruch, d.h. ohne Adressverifikation (ausgenommen, es besteht die Alternative zur Prüfung mittels Geolokalisierung, siehe obenstehend II.2) und Referenzüberweisung, möglich ist. Die Kombination von verschiedenen Technologien zur Gesichtserkennung, Lebenderkennung und dem Auslesen der *Visual Inspection Zone* (VIZ) und *Machine Readable Zone* (MRZ) der Ausweisdokumente ermöglichen eine sichere Online-Identifizierung ohne unnötigen Unterbruch des Prozesses.

Zu beachten gilt in diesem Zusammenhang auch die Entwicklungen im Bereich der digitalen Zertifikate. Derzeit besteht noch eine Pflicht zur persönlichen Vorsprache zwecks Identifikation, wenn ein digitales Zertifikat, z.B. eine qualifizierte elektronische Signatur, verwendet werden möchte. In der EU läuft derzeit eine Vernehmlassung des European Telecommunications Standards Institute (ETSI), nach der das Identifikationsverfahren bei digitalen Zertifikaten neu regelt wird. Insbesondere wird dort die automatisierte Identifikation mit biometrischen Daten näher definiert.[1] Sollte sich dieser Standard in der EU durchsetzen, so ist zu erwarten, dass in einem ersten Schritt dieses Verfahren von der Konformitätsbewertungsstelle der persönlichen Vorsprache gleichwertig anerkannt wird (vgl. Art. 7 Abs. 1 VZertES). In einem zweiten Schritt werden wohl dann auch die Schweizer Regeln (ZertES und VZertES) angepasst. Es ist folglich damit zu rechnen, dass in naher Zukunft die Identifikation mittels audiovisueller Kommunikation bei digitalen Zertifikaten

[1] https://docbox.etsi.org/esi/Open/Latest_Drafts/Draft%20ETSI-TS-119-461-v0.0.5.pdf.

entfallen wird. Im Sinne der Harmonisierung und Technologieneutralität sollte auch im Bereich der Geldwäscherei diese Entwicklung mitgetragen werden.

Nachfolgend finden Sie eine Auswahl von Sicherheitsvorkehrungen, die zusammen mit dem Auslesen der Ausweisdokumente zur Anwendung gelangen könnten:

- **Videosequenzen in Echtzeit:** Eine Videosequenz in Echtzeit anstelle von blossen Bildern bietet die Möglichkeit, die zu identifizierende Person mittels Lebendigkeitscheck aber auch die Sicherheitsmerkmale der häufig eingesetzten Schweizer Identitätskarte sicher und vollautomatisch zu prüfen. An Videosequenzen können technisch hohe Anforderungen gestellt werden (Auflösung, Lichtverhältnisse etc.). Im europäischen Raum wird diese Möglichkeit bereits durch Spanien[2] genutzt und weitere EU-Länder folgen diesem Beispiel. Möglich macht dies die in der eIDAS[3] verankerte – und in der Geldwäschereirichtlinie referenzierte – Generalklausel, nach der Identifizierungsmethoden, die auf nationaler Ebene anerkannt sind und gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten (vgl. Art. 24 Abs. 1 lit. d eIDAS), zugelassen sind. Wenn sich Schweizer Finanzintermediäre dieser Entwicklung nicht anschliessen können, bedeutet dies letztlich ein Wettbewerbsnachteil.
- **Gesichtserkennung:** Verbesserte Technologien bei der Gesichtserkennung kombiniert mit Softwarekomponenten zur Abwehr von *Deepfakes* bringen zuverlässige Resultate, die über eine hohe Erkennungsschwelle abgesichert werden und bei ungenügender *Convenience* einer manuellen Überprüfung/Abklärung durch geschulte Mitarbeitende zugeführt werden können. Im Sinne einer hohen Sicherheit sind *false negative* oder auch der automatische Abbruch des Verfahrens aufgrund schlechter Lichtverhältnisse für die Erkennung von Gesicht oder Ausweisdokument etc. in Kauf zu nehmen. Insgesamt sichert dieses Vorgehen Finanzintermediären die Wettbewerbsfähigkeit im europäischen und internationalen Markt. Im Übrigen stehen die verschiedenen Algorithmen zur Gesichtserkennung und zur Lebendigkeitsprüfung in ständigem Wettbewerb, werden regelmässig von unabhängigen Stellen überprüft und aufgrund neuer Erkenntnisse von den Herstellern weiterentwickelt. Es haben sich für Test- und Zertifizierungsverfahren[4] hohe Branchenstandards entwickelt.
- Eine Lebendigkeitsprüfung kann durch sinnvolle und zufällig ausgewählte ***Challenge-Response* Elemente** in Ton, Video oder am *User Interface* angereichert werden.

---

[2] Die *Servicio Ejecutivo de la Comisión de Prevenicón de Blanqueo de Capitales e Infracciones Monetarias SEPBLAC* hat bereits ein Identifikationsverfahren basierend auf einer live Videosequenz ohne direkte Beteiligung einer Person seitens des Finanzintermediärs implementiert.

[3] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG; Richtlinie (EU) 2018/843 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU.

[4] Vgl. FVRT 1:1 VERIFICATION, FVRT MORPH, aber auch NIST- und ISO Standards (30107-3).

IV. Zum Beizug Dritter, Rz. 51

Die Präzisierung, dass keine untersagte Weiterdelegation besteht, wenn ein Finanzintermediär einen anderen mit der Identifizierung beauftragt und dieser wiederum einen Dienstleister beizieht, begrüssen wir.

Es stellt sich die Frage, wie sich Rz. 51 im Verhältnis zu Art. 43 Abs. 3 VSB 20 verhält. Gemäss Rundschreiben und Art. 28 und 29 GwV-FINMA ist ein Beizug Dritter für die Identifizierung erlaubt. Die VSB 20 schränkt diese Erlaubnis aber in Art. 43 Abs. 3 VSB in Bezug auf die Korrespondenzeröffnung ein, obwohl die Korrespondenzeröffnung gem. Art. 10 Abs. 2 VSB 20 der Online-Identifizierung gleichstellt ist. Nach unserer Auffassung kann die Online-Identifizierung trotz Einschränkung in der VSB vollumfänglich an einen Dritten delegiert werden. Im Sinne der Klarheit und Rechtssicherheit würden wir es begrüssen, wenn die FINMA unsere diesbezügliche Haltung zumindest im Ergebnisbericht zur Vernehmlassung bestätigen könnte.

V. Weitere Anliegen

V.1 Begriff «Vertragspartner»

Das gesamte Rundschreiben bezieht sich bzgl. Online- und Video-Identifizierung jeweils auf den «Vertragspartner». Es gibt einige Konstellationen, in denen nicht der Vertragspartner selbst, sondern eine andere Person eine Geschäftsbeziehung eröffnen kann (oder gar muss) oder in denen nicht nur der Vertragspartner selbst identifiziert werden muss. Zu denken sei bspw. an die Eröffnung einer Geschäftsbeziehung durch eine mündige Drittperson für eine minderjährige Person oder eines Kapitaleinzahlungskontos. Laut Wortlaut des Rundschreibens können diese Parteien nicht von der Online- und Video-Identifizierung Gebrauch machen, da sie selbst nicht Vertragspartei sind. Es wäre zu begrüssen, dass auch für diese Konstellationen der Weg der Online- und Video-Identifizierung offenstehen und die Terminologie entsprechend angepasst würde.

V.2 Beachtung des technologischen Fortschrittes

Die Technologie entwickeln sich schnell weiter. Wir würden daher einen kürzeren Aktualisierungszyklus des Rundschreibens begrüssen, auch um die Entwicklungen ausländischer Regularien und damit mögliche Vorteile der Mitbewerber im Ausland rasch zu kompensieren. Zudem würden wir es sehr begrüssen, wenn die FINMA den aktuellen Stand der Technik bereits in der vorliegenden Revision berücksichtigt (siehe obenstehende Ausführungen in Ziff. III).

V.3 Knappe Anhörungsfrist und Zeitpunkt

Die Anhörung als auch die durchgeführten Vorkonsultationen werden grundsätzlich geschätzt. Jedoch ist die lediglich auf zweieinhalb Monate bemessene Anhörungsfrist sehr knapp, insbesondere weil der Anhörungszeitraum über die Festtage läuft. Dieser Umstand hätte zumindest mit einer grosszügigen Frist kompensiert werden können.

SwissBanking

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

Andreas Barfuss
Leiter Legal und Compliance

Eleonor Gyr
Senior Advisor Compliance

OAR–ASA | SRO–SVV

Selbstregulierungsorganisation des SVV
Organisme d'autorégulation de l'ASA
Organismo di autodisciplina dell'ASA
Self-regulatory organisation of the SIA

Eidgenössische Finanzmarktaufsicht FINMA
Isabel Grüninger
Laupenstrasse 27
3003 Bern

Zürich, 28. Januar 2021

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

Sehr geehrte Frau Grüninger

Wir danken Ihnen für die Möglichkeit, an der Anhörung zur Teilrevision des FINMA-Rundschreibens 2016/7 «Video- und Online-Identifizierung» teilnehmen zu können. Gerne nehmen wir die Gelegenheit wahr, Ihnen nachfolgend die Stellungnahme der Selbstregulierungsorganisation des SVV (SRO-SVV) zu unterbreiten. Diese Sichtweise deckt sich mit der Haltung des Schweizerischen Versicherungsverbands SVV.

Wir begrüssen die Revision des FINMA-Rundschreibens 2016/7 «Video- und Online-Identifizierung» in der vorgeschlagenen Stossrichtung ausdrücklich.

Wir regen an, die neue Formulierung in Ziffer 53 im Sinne der im Erläuterungsbericht ausgeführten Zielsetzung der Technologieneutralität offener zu formulieren.

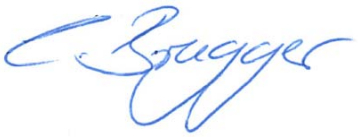
Formulierungsvorschlag
«Zieht ein Finanzintermediär einen ~~anderen Finanzintermediär~~ Dritten bei und nimmt dieser die Video- und Online-Identifizierung durch direkt beauftragte Dienstleister vor, so gelten letztere nicht als weitere Personen oder Unternehmen und es liegt keine untersagte Weiterdelegation vor.»

Erwägungen
In der Praxis bieten auch Unternehmen Video- und Online-Identifizierungslösungen an, die selbst nicht über einen Regulierungsstatus als Finanzintermediär verfügen. Es handelt sich dabei um Unternehmen, die ihre Tätigkeit auf die Bereitstellung von technischen Lösungen fokussieren. Dabei gibt es auch Konstellationen, in denen diese Technologiespezialisten weitere Dienstleister beiziehen (analog zu den im Erläuterungsbericht aufgeführten Finanzintermediären, die in Zusammenarbeit mit weiteren Unternehmen eine Video- und Online-

Identifizierung zur Verfügung stellen). In beiden Konstellationen wird in arbeitsteiliger Zusammenarbeit eine Gesamtlösung angeboten. Die Klarstellung in der neuen Formulierung in Ziffer 53, nach der die beigezogenen Unternehmen nicht als weitere Personen oder Unternehmen im Sinne der Delegationsvorgaben von Art. 28 GwV-FINMA gelten, sollte deshalb auf alle Konstellationen erweitert werden. Dies entspricht auch der Regelung in Art. 28 GwV-FINMA, wonach die Sorgfaltspflichten nicht nur an Finanzintermediäre, sondern generell an Dritte delegiert werden können (sofern die Voraussetzungen betreffend die sorgfältige Auswahl, Instruktion und Überwachung erfüllt sind, vgl. Formulierung in Art. 28 Abs. 1 GwV-FINMA).

Wir danken Ihnen für die Berücksichtigung unseres Anpassungsvorschlags und unserer Erwägungen bei der weiteren Behandlung des Entwurfs. Gerne stehen wir Ihnen für Rückfragen zur Verfügung

Freundliche Grüsse
SRO-SVV



Dr. Markus Hess
Präsident

Dr. Christina Brugger
RAin, Leiterin der Geschäftsstelle

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

Eidgenössische Finanzmarktaufsicht FINMA
Laupenstrasse 27
CH-3003 Bern

Zürich, 25. Januar 2021

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

Sehr geehrte Frau Grüninger

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

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

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

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

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

Konkret fordert SFTI folgende Alternativen für digitale Kunden-Onboardings:

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

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

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

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

1 Grundsatz: Beibehaltung Sicherheitsniveau

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

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

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

2 Auto-Identifizierung der persönlichen Vorsprache gleichgestellt

2.1 Technisch möglich

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

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

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

2.2 Keine Einbussen bei Sicherheit und Qualität

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

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

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

2.3 eIDAS-Verordnung

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

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

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

2.4 Fazit

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

3 Online-Identifizierung ohne Banküberweisung oder Alternativen dazu

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

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

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

4 Eventualiter: Chipscan ohne Zertifikatsprüfung

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

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

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

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

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

5 Geolokalisation zur Plausibilisierung der Adressangaben

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

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

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

6 Keine handschriftliche Unterschriften für Feststellung wB

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

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

Freundliche Grüsse

Sig. Werner W. Wyss
Leiter der AG Regulations

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

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

SwissSign Group

SwissSign Group AG
Sägereistrasse 25
Postfach
CH-8152 Glattbrugg
+41 848 77 66 55
info@swisssign.com
www.swisssign-group.com

Ihr Ansprechpartner:
Attila Fekete
+41 79 445 35 33

Eidgenössische Finanzmarktaufsicht FINMA
Isabel Grüninger
Laupenstrasse 27
CH-3003 Bern

Per E-Mail: isabel.grueninger@finma.ch

1. Februar 2021

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

Sehr geehrte Frau Grüninger

Obschon SwissSign Group AG (SwSG) nicht explizit zur Stellungnahme im Rahmen obengenannter Anhörung eingeladen wurde, erlauben wir uns, Ihnen hinsichtlich «Video- und Online-Identifizierung» unsere Einschätzung, insbesondere auch unter Einbezug möglicher künftiger Entwicklungen, darzulegen.

SwSG als Trust Service Provider (TSP) und als Herausgeberin der SwissID setzt sich täglich mit dem Thema «Überprüfung der Identität auf Distanz» auseinander. Unser hoher Anspruch an die Sicherheit gebietet, dass wir ausschliesslich Identifikations- und Verifikationsprozesse nutzen, die den höchsten regulatorischen Anforderungen gerecht werden. Aus diesem Grund sind wir auch vertraut mit den einschlägigen Normen und Standards, nicht nur hier in der Schweiz, sondern auch im internationalen Kontext. Durch den regelmässigen Austausch mit unseren Kunden, darunter auch viele Finanzdienstleister, kennen wir ebenfalls die Bedürfnisse am Markt hinsichtlich der Identitätsfeststellungsprozesse und deren Nutzung im Rahmen von weitergehenden, vertrauensbasierten Dienstleistungen (bspw. geregelte elektronische Signaturen und Zertifikate).

Vor diesem Hintergrund haben wir uns erlaubt, die o.g. Teilrevision des RS zur «Video- und Online-Identifizierung» näher zu beleuchten und sind dabei zu folgendem Schluss gelangt:

- Wir verstehen, dass der Bereich Online-Identifizierung um die «Auslesung mittels biometrischem Chip» erweitert wurde und erachten diese Erweiterung als sinnvoll und zielführend. Nichtsdestotrotz möchten wir darauf hinweisen, dass nur gerade 40% der Schweizer und Schweizerinnen von dieser Vereinfachung profitieren werden können. Aktuelle Schätzungen gehen von einer Verbreitung des biometrischen Passes von 40% bis 50% aus[1]. Das beliebtere Ausweisdokument, die schweizerische Identitätskarte (Verbreitung über 90%), verfügt nicht über einen auslesbaren Chip. Aktuell ist auch nicht absehbar, wann die schweizerische Identitätskarte mit einem biometrischen Chip ausgerüstet wird.

[1] Gemäss Aussage fedpol

- Wir bedauern, dass das revidierte Rundschreiben dem vorhandenen Potential der technischen Entwicklungen, welche in den letzten Jahren Einzug gehalten haben, zu wenig Rechnung trägt. Zudem scheint auch der sich in Erarbeitung befindliche internationale Standard des Identitiy Proofing (ETSI TS 119 461)[2] nur teilweise berücksichtigt worden zu sein. Dieser neue Standard hat zum primären Ziel, den Identitätsfeststellungsprozess nicht nur als integralen Bestandteil eines TSP zu sehen, sondern ihn zusätzlich als eigenständige Dienstleistungskomponente zu positionieren. Dies hat den Vorteil, dass letztere einerseits im Rahmen von vertrauensbasierten Dienstleistungen und zusätzlich auch für andere Zwecke, wie bspw. bei der Herausgabe von e-IDs oder im Rahmen des Onboarding-Prozesses bei Finanzdienstleistungen, eingesetzt werden kann. Damit spricht dieser neue Standard sowohl Anbieter von qualifizierten als auch von nicht qualifizierten Dienstleistungen an und die Spezifikationen sollen von unterschiedlichen Industrien angewendet werden (explizit wurde hier die Finanzdienstleistungsindustrie erwähnt). Auf politischer Ebene wurde im europäischen Raum damit erkannt, wie wichtig eine Harmonisierung des Identitätsfeststellungsprozesses zwischen den Industrien ist. Wir würden es daher begrüssen, wenn diese Harmonisierungsbestrebungen in der Schweiz von der FINMA ebenfalls vorangetrieben würden, nicht zuletzt aus dem Grund, dass das schweizerische Bankwesen internationalen Vorzeigecharakter aufweist und einen hervorragenden Ruf geniesst.

- Diesbezüglich hat das BAKOM uns gegenüber bestätigt, dass sie den neuen ETSI-Standard im Rahmen der ZertES Zertifizierung anwenden wird, sobald er in Kraft tritt (voraussichtlich Sommer 2021). Eine diesbezügliche Harmonisierung würde bedeuten, dass Identitäten, welche im Rahmen eines KYC-Prozesses festgestellt wurden und die Anforderungen des neuen Standards erfüllen, für die Ausstellung von geregelten Signaturzertifikaten genutzt werden können. Ein erneuter Identitätsfeststellungsprozess wäre somit nicht mehr notwendig. Dieser Umstand führt nachweislich zu einer höheren Convenience bei Bankkunden und die Prozesskosten können signifikant gesenkt werden.

Wir regen nach Rücksprache mit unseren Kunden aus dem Finanzdienstleistungsbereich daher gerne folgende Punkte an:

1. Angleichung der FINMA-Anforderungen an den neu entstehenden Standard für Identity Proofing (ETSI TS 119 461), insbesondere hinsichtlich Definition der Sicherheitsanforderungen, Gütequalität und bei der Berücksichtigung technischer Errungenschaften.

2. Nutzung der beim ETSI-Standard gegebenen breiten Vielfalt möglicher Identitätsfeststellungsprozesse, insbesondere im Prozessschritt Validierung (bspw. nicht nur digitale ID-Dokumente (Chip), sondern auch physische ID-Dokumente mit den gegebenen Sicherheitsmerkmalen).

3. Gleichstellung der FINMA-konformen Videoidentifizierung (audiovisuelle Kommunikation in Echtzeit) mit der automatisierten Online-Identifizierung, sofern die im Rahmen der ETSI geforderten Anforderungen erfüllt sind (insbesondere ETSI TS 119 461; Kapitel 8.2.4 Validation of Digital Identity Document sowie 8.2.5 Validation of Physical Identity Document). Die Erfahrung von SwSG mit Gesichtsverifikationen (SwSG nutzt hierzu die Lösung von PXL Vision), welche maschinell vorgenommen wurden, sind sehr positiv. Die im Rundschreiben erwähnten “False

[2] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects; Draft ETSI TS 119 461 V0.0.5

Rates” (positiv und negativ) konnten nicht nachgewiesen werden. Im Gegenteil – wir sehen in der automatisierten Online-Identifizierung eine viel sicherere Identifizierung im Vergleich zur Videoidentifizierung. Diesbezüglich verweisen wir auf das Schreiben von PXL Vision (Stellungnahme zum Änderungsentwurf des Rundschreibens 2016/7 "Video- und Online-Identifizierung" der FINMA») und begrüssen diese Empfehlung (siehe Beilage Befürwortungsschreiben).

Für eine wohlwollende Prüfung unseres Anliegens danken wir bestens und stehen für Rückfragen jederzeit gerne zur Verfügung.

Freundliche Grüsse
SwissSign Group AG

Markus Naef
CEO

Attila Fekete
Senior Digital Advisor

Beilage: erw.

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

Kontaktperson

Attila Fekete
+41 79 445 35 33

31. Januar, 2021

Befürwortungsschreiben zur Stellungnahme der PXL Vision AG in Bezug auf den Änderungsentwurf des Rundschreibens 2016/7 "Video-und Online-Identifizierung" der FINMA

Sehr geehrte Frau Grüninger

Diesem Befürwortungsschreiben dient als Bestätigung, dass [Firmenname] die Position von PXL Vision, in Bezug auf den Änderungsentwurf des Rundschreibens 2016/7 "Video-und Online-Identifizierung" der FINMA, vollumfänglich teilt.

Wir unterstützen den vor der PXL Vision AG unterbreiteten Vorschlag die Onlineidentifikation dahingehen zu erweitern, dass auch ohne Einsatz der Chip Prüfung auf eine zusätzliche Referenzüberweisung und Prüfung der Wohnsitzadresse verzichtet werden kann.

Das vorgeschlagene Verfahren einer automationsunterstützenden Identitätsprüfung mit menschlicher Nachkontrolle bei Unsicherheiten, wie von der PXL Vision AG im Detail vorgeschlagen, sehen wir als sichere, zuverlässige und praktikable Lösung für die Branche und würden eine Anerkennung der FINMA sehr begrüssen.

Mit freundlichen Grüssen

SwissSign Group AG

Markus Naef
CEO

Attila Fekete
Senior Digital Advisor

Ticino Blockchain Technologies Association
www.tbta.ch

Autorità federale di vigilanza sui mercati finanziari FINMA
Isabel Grüninger
Laupenstrasse 27
CH-3003 Berna
isabel.grueninger@finma.ch

Lugano, 29 gennaio 2021

Presa di posizione relativa alla modifica della Circolare FINMA 16/7

Gentile Signora Grüninger

Come previsto con comunicazione del 16 novembre 2020, ci permettiamo di inoltrare la presente presa di posizione per conto della Ticino Blockchain Technologies Association (di seguito TBTA) in merito ai lavori per la modifica della Circolare FINMA 16/7 sulla video identificazione e l'identificazione online.

1. Generalità sull'associazione e al suo interesse alla consultazione

TBTA è un'associazione che ha quale scopo quello di promuovere e sostenere le imprese innovative che fanno ricerca e sviluppo nel settore Blockchain e applicazioni decentralizzate, al fine di migliorare la loro competitività con impatto positivo sulla società in termini economici, di posti di lavoro qualificati, e di qualità della vita..

I soci di TBTA sono entità molto attive nell'ambito FinTech e che hanno avuto modo di implementare la Circolare FINMA 16/7 già per alcuni anni. Essi hanno pertanto un interesse importante affinché questa lodevole autorità comprenda le necessità non soltanto delle banche e altre grandi istituzione, ma anche delle piccole imprese, sovente start up, che devono confrontarsi con una concorrenza estera importante (si veda ad esempio Revolut, N26, coinbase, kraken, bitstamp) che hanno oggi norme sull'identificazione online molto più appropriate alle attività digitali rispetto alla Svizzera.

L'associazione ha pertanto un interesse a partecipare alla consultazione essendo l'attività dei loro membri direttamente collegate alle norme legali in discussione.

2. Presa di posizione

2.1. Considerazione generali

L'associazione approva con favore le modifiche che la FINMA intende adottare alla ORD-FINMA, che vanno nella giusta direzione. Tuttavia, vogliamo cogliere l'occasione della consultazione in corso per porre alla vostra attenzione le lacune riscontrate nella legislazione in relazione con la continua cresci-

ta delle attività digitali e FinTech in Svizzera. Siamo coscienti che non tutti gli argomenti che tratteremo in seguito sono direttamente legati alla consultazione da voi messa in atto, ma riteniamo, vista l'urgenza di alcune modifiche di seguito proposte, che questo sia il momento più opportuno per prendere in considerazione una modifica più ampia delle norme sul riciclaggio di denaro e più precisamente sugli obblighi di d'identificazione della controparte d'affari.

2.2. Adattamento dell'identificazione online alle procedure in uso in Europa

Con l'incremento della digitalizzazione delle attività commerciali sempre più attività non prevedranno la necessità di un incontro con i loro clienti. Tutti i rapporti con i clienti saranno svolti in modo digitale. In questo ambito, l'identificazione del cliente viene svolta esclusivamente in modo online o, in misura minore, per videoidentificazione. Un esempio è quello della società Revolut Ltd, la più grande società FinTech del mondo e presso la quale è possibile aprire e attivare un conto pronto per l'uso in qualsiasi momento nello spazio di 5 minuti. In Svizzera il tempo medio per svolgere un KYC online è di 20-25 minuti, con un'estrema difficoltà ad eseguire un'autorizzazione automatica del cliente. La Circolare FINMA 2016/17 che regola l'identificazione online è attualmente troppo rigida nei criteri di sicurezza richiesti e non permette di riconoscere una larga parte della popolazione mondiale tramite identificazione online. Requisiti come il Formulario A (che esiste solo in Svizzera) o l'obbligo di uso di documenti provvisti della Machine Readable Zone (MRZ) - laddove molti documenti di diversi paesi ne sono sprovvisti e quando le macchine ora sono in grado di leggere direttamente il testo del documento e non necessitano più di una MRZ - stanno convincendo sempre più società ad abbandonare la Svizzera. Prendiamo ad esempio la società Swissborg (swissborg.com) che ha delocalizzato la sua attività finanziaria in Estonia, perché le permette di identificare i clienti in modo più semplice ma comunque sicuro, e soprattutto senza la necessità di un bonifico bancario.

Riteniamo indispensabile che la Svizzera adegui la propria prassi a quella europea, onde evitare una escalation di società che abbandonino la Svizzera poiché impossibilitati di svolgere l'identificazione del cliente. Qui di seguito elenchiamo solo alcuni esempi del perché sia estremamente limitato eseguire un'identificazione online in Svizzera seguendo i criteri della Circolare FINMA 2016/07.

a) Richiesta MRZ

- United Kingdom: dal 2011 in Gran Bretagna le carte d'identità non sono più valide e non è più possibile usarle come prova d'identità. Le persone che necessitano di un documento probante la loro identità possono avvalersi di un passaporto o di una patente di guida (pochi elementi di sicurezza ottici, no MRZ) https://www.gov.uk/identitycards. In molti casi si è stabilito che la maggior parte dei cittadini della Gran Bretagna non intenzionati a viaggiare, sono possessori unicamente della licenza di condurre nel caso siano patentati (GBR-FO-09002). Il valore giuridico del documento e il suo principale obiettivo è atto a comprovare l'identità del titolare nel territorio di tale paese e il diritto a soggiornare legalmente in UK, ma non costituisce prova della sua cittadinanza. Di conseguenza, tutti i cittadini UK che non dispongono di un passaporto non possono aprire relazioni a distanza con società svizzere, mentre possono farlo nel resto d'Europa che non richiede requisiti simili a quelli elvetici.
- Italia: la carta d'identità della Repubblica Italiana in formato cartaceo (ITA-BO-03001) è uno dei documenti di riconoscimento più in uso previsti in Italia dalla legge. Tale documento è utilizzato per il riconoscimento personale e come documento per l'espatrio (in diversi paesi tra cui la Svizzera). Il documento non presenta alcun elemento di sicurezza ottico e non presenta il codice MRZ. Il valore giuridico del documento e il suo principale obiettivo è atto a comprovare

l'identità del cittadino, sia italiano sia straniero legalmente soggiornante in Italia, incluso l'indirizzo di residenza. Dalla nostra esperienza abbiamo rinvenuto diverse persone che non sono in possesso di un passaporto, ma solo della carta di identità. Tutte queste persone non possono aprire una relazione a distanza con società domiciliate in Svizzera, ma lo possono fare nel resto d'Europa.

- Francia: la carta d'identità francese (FRA-BO-02002), documento riconosciuto e valido per la verifica dell'identità e della cittadinanza, e altresì valido come documento di viaggio (soprattutto in Europa), non presenta particolari elementi di sicurezza ottici. Il valore giuridico del documento e il suo principale obiettivo è atto a comprovare l'identità del cittadino francese. Anche in questo caso un utente che detiene solo questo tipo di documento non potrà mai usufruire dei servizi di società svizzere, mentre non ha problemi di sorta ad utilizzare servizi offerti in Europa.

- Romania: la licenza di condurre rumena (ROU-FO-05001) è un documento privo del codice MRZ. Il valore giuridico del documento e il suo principale obiettivo è atto a comprovare che la patente di guida è stata rilasciata a una persona soggiornante legalmente in Romania, e atta a comprovare l'identità del titolare nel territorio di tale paese, ma non ne costituisce prova della sua cittadinanza.

- Australia: l'ultimo passaporto emesso per i cittadini australiani (AUS-AO-05001) è un documento con pochissimi elementi di sicurezza ottici (unicamente elementi UV e watermark non verificabili attraverso una Videoidentificazione o attraverso la procedura d'identificazione online). Il valore giuridico del documento e il suo principale obiettivo è essere utilizzato come documento di viaggio rilasciato unicamente a cittadini australiani. Questo fatto escluderebbe de facto la possibilità di aprire relazioni a distanza con cittadini australiani in quanto la mancanza di due elementi ottici di sicurezza richiesti dalla Circolare FINMA 2016/7 non sono garantiti, apertura di relazione d'affari che invece può avvenire senza problemi in altri paesi europei.

  Occorre inoltre osservare che i requisiti posti dalla Circolare FINMA 2016/07 sono superati. La richiesta di un documento provvisto di un testo in formato Machine Readable Zone (MRZ) in particolare non ha più alcuna ragione. Oggigiorno i provider di servizi KYC leggono i documenti di identità tramite algoritmi basati sulle informazioni contenute sul documento e non più sulla MRZ. Lo scopo del richiedere un testo in formato MRZ, ovvero poter controllare la veridicità delle informazioni fornite dall'utente con quelle previste nel documento e controllare il nominativo dell'utente nelle apposite liste di persone oggetto di sanzioni, condannate in passato o con una funzione di PEP, sono oggi eseguite senza usufruire della MRZ. La stessa MRZ può essere facilmente falsificata esistendo diversi siti internet[1] che permettono di generare il codice MRZ sulla base delle informazioni contenute in un documento, compresi i numeri di sicurezza. La richiesta di una MRZ prevista nella Circolare FINMA 2016/17 pertanto non soltanto è inutile, ma come sopra esposto sta seriamente limitando le possibilità di aprire relazioni d'affari in Svizzera. A nostra conoscenza, la Svizzera è uno dei rari paesi che richiede la presenza di una MRZ nei documenti di identificazione per la conclusione di una identificazione online. Questa esigenza, che come detto sopra è tecnologicamente superata, sta ora portando un grave danno alla concorrenzialità della piazza FinTech svizzera e potenzialmente anche per tutte le altre attività finanziarie svolte dai classici intermediari finanziari. A nostro avviso l'autorità dovrebbe lasciare aperti gli aspetti tecnici su come leggere le informazioni riportate nei documenti di

[1] http://www.emvlab.org/mrz/
http://www.highprogrammer.com/cgi-bin/uniqueid/mrzp
http://extranet.cryptomathic.com/mrz/index

identificazione, in modo da permettere l'uso delle tecnologie più appropriate, senza doversi focalizzare su una tecnologia specifica che, nel tempo, diventerà sicuramente obsoleta, come è il caso della MRZ.

b) Limitazione nell'uso degli utility bills

Un ulteriore elemento che limita fortemente l'applicazione dell'identificazione online è la possibilità limitata di utilizzo dei cosiddetti "utility bills" per la conferma della residenza dell'utente. Oggi la Circolare FINMA 2016/17 prevede quali elementi utilizzabili una fattura per il pagamento delle imposte o una fattura emessa da un'altra autorità oppure una fattura dell'elettricità, dell'acqua o del telefono. Purtroppo nel resto del mondo vi sono diversi casi in cui è difficile ottenere un tale documento. In diversi paesi infatti le imposte sono prelevate direttamente dallo Stato, senza emissione di una fattura. Inoltre, vi sono diverse casistiche di persone che non dispongono di utility bills a loro nome, come ad esempio le mogli (sovente le fatture sono intestate ai mariti) o i "millenials" maggiorenni ma che vivono ancora con i loro genitori. In altri stati il gas (non contemplato tra i possibili utility bill accettabili) è più usato dell'elettricità, mentre i documenti bancari dovrebbero essere pure annoverati tra gli utility bills utilizzabili. Anche questo requisito inoltre non è richiesto in diverse giurisdizioni europee, creando in questo un danno competitivo alla Svizzera.

c) Formulario A come ostacolo all'identificazione a distanza

La sottoscrizione del formulario A (un documento che ha sicuramento svolto le sue funzioni in passato, ma che appare superato con l'implementazione delle regole sullo scambio automatico di informazioni e con l'avvento dell'era digitale) comporta un importante ostacolo all'esecuzione di un'identificazione online. L'esecuzione del KYC online richiede una user experience (UX) e un'interfaccia di semplice utilizzo, onde evitare che l'utente, non riuscendo nell'intento, abbandoni la richiesta optando per un servizio con un servizio KYC di più semplice utilizzo. Oggi, l'art. 59 cpv. 4 ORD-FINMA richiede all'intermediario finanziario di documentare in maniera adeguata qualora non nutra dubbi sul fatto che la controparte o il detentore del controllo sia anche l'avente economicamente diritto dei valori patrimoniali. Questa norma ha portato ad applicazione estensiva del formulario A, ritenuto che si tratta di un processo più semplice della "documentazione adeguata" prevista dall'art. 59 cpv. 4 ORD-FINMA. Tuttavia, la Circolare FINMA 2016/17 chiede che il formulario A venga firmato con una firma elettronica qualificata (una funzione di cui il 99% delle persone non dispone), un TAN (processo fattibile ma complesso) o con la trasmissione elettronica del modulo firmato a mano (un altro processo che richiede molto tempo). Ne consegue che l'introduzione del formulario A nell'identificazione online sta rendendo così complesso il KYC elvetico da renderlo poco attrattivo rispetto alla concorrenza europea, quando invece il processo potrebbe essere risolto in altro modo, ovvero con una dichiarazione semplificata.

d) Video identificazione tramite sistemi automatizzati (bot)

Nell'ambito della video identificazione, sono nel frattempo nate diverse società che offrono questo servizio tramite l'uso di programmi automatizzati (bot) che chiedono all'utente di svolgere determinate azioni in modo da garantire che davanti alla telecamera vi sia una persona. Ora la Circolare FINMA 2016/17 chiede che la video identificazione venga svolta in "tempo reale" (Circ. FINMA 2016/17 nm 6). Riteniamo necessaria, per poter sfruttare tutte le novità tecnologiche, di sottolineare come l'intermediario finanziario possa utilizzare, a questo scopo, anche soluzioni tecnologiche, senza richiedere la necessità di una presenza umana anche dall'altra parte della telecamera. Vi sono infatti purtroppo delle OAD che non vogliono accettare questa nuova tecnologia ma richiedo una presenza umana da entrambi i lati della telecamera, generando in questo modo costi che non tutte le società possono sopportare (si veda sotto punto e).

e) Pagamento da conto bancario per società attive solo nelle criptovalute

La richiesta del bonifico bancario per le società attive unicamente in ambito di criptovalute, anche se sarà eliminata con la nuova procedura di identificazione dei chip del passaporto biometrico (una possibilità che potrà all'inizio essere usata da un numero limitato di persone), non può essere mantenuta. Le società attive solo con criptovalute, senza denaro fiat, non possono richiedere un versamento in valuta fiat. Questo impone a queste società di abbandonare il mercato svizzero (si veda la già citata Swissborg). Vi sono altri metodi di verifica che possono sostituire il bonifico bancario, quali ad esempio la verifica del controllo del proprio wallet criptografico, oppure la videoidentificazione tramite un bot (ad oggi non accettata dagli OAD). La semplice videoidentificazione è una procedura troppo cara per la maggior parte delle società attive solo con criptovalute, che hanno un margine di guadagno molto limitato e che non permette di coprire i costi di una videoidentificazione senza l'uso di strumenti automatizzati (si veda sopra d).

Siamo pertanto dell'avviso che la Circolare FINMA 2016/17 debba essere modificata al più presto onde evitare di limitare fortemente le possibilità di attività da parte delle future aziende FinTech in Svizzera, come già sta scucendo. Siamo consapevoli che la messa in consultazione in corso porta su temi diversi, ma la situazione richiede un rapido intervento onde evitare di rendere inutile tutte le attività svolte in ambito di criptovalute sin qui svolte.

Per questi motivi, richiediamo di apportare alla Circolare FINMA 2016/17 le seguenti modifiche:

- Sostituzione della richiesta di una lettura dei dati della MRZ con una richiesta di lettura dei dati dei documenti di identificazione.
- Delega del riconoscimento degli utility bill da utilizzare all'intermediario finanziario stesso, che a sua discrezione potrà utilizzare il documento più opportuno in considerazione della giurisdizione del cliente al fine di verificarne la residenza.
- Permettere la sottoscrizione agevolata del formulario A tramite un check in the box durante la procedura di identificazione online.
- Autorizzazione dell'uso da parte dell'intermediario finanziario di sistemi automatizzati (bot) du-

rante la video identificazione.

- Sostituzione del bonifico bancario con una identificazione del wallet per le società attive unicamente in ambito criptovalute.
-

2.3. Delegazione obblighi di diligenza in ambito di riciclaggio di denaro

Attualmente stiamo vivendo una tendenza nell'ampliamento del campo di applicazione della LRD a sempre nuove attività. Questa tendenza è visibile non unicamente nel progetto posto, ma pure nelle proposte modifiche della legge sul riciclaggio di denaro (LRD, come l'abbassamento delle soglie per operazioni in contanti da CHF 100'000 a CHF 15'000), ma anche e soprattutto nel mondo digitale e FinTech, con l'abbassamento della soglia di identificazione dei clienti a CHF 1'000. In particolare i business model FinTech che prevedono l'uso di criptovalute sono attualmente confrontati ad un assoggettamento alla LRD dovuta all'ampia interpretazione data alla qualifica di payment token. In questo caso imprese che non hanno un'attività in ambito prettamente finanziario (es. società che vendono merci e/o servizi online tramite propri token qualificati da FINMA quali payment tokens) risultano assoggettate alla LRD, fatto questo che risulta estremamente oneroso per imprese non finanziarie dove anche le transazioni sono svolte digitalmente e l'identificazione deve essere svolta online. Risulta pertanto importante per le imprese poter garantire un controllo dei dati forniti dai clienti in modo rapido ed economicamente sostenibile.

Questo è possibile solo con la possibilità di delegare degli oneri legati alla lotta al riciclaggio di denaro a società terze specializzate. Ora purtroppo il diritto svizzero non prevede la possibilità di delegare l'applicazione dei doveri di diligenza in ambito di riciclaggio di denaro senza essere a propria volta assoggettato a tale legge e richiedere un'affiliazione ad un organo di autodisciplina (OAD).

Riteniamo pertanto necessario e indispensabile, per poter garantire un'efficace applicazione delle normative sul riciclaggio di denaro e al contempo non imporre alle società digitali non finanziarie e alla piccole-medie imprese procedure che non sono in grado di implementare, la possibilità di delegare l'adempimento di tali obblighi a società terze specializzate senza l'obbligo di assoggettamento agli OAD.

Osserviamo in particolare che nella sua legge blockchain il Principato del Liechtenstein prevede espressamente il ruolo dell'identificatore KYC per conto di terzi. Questa figura è indispensabile anche in Svizzera e dovrebbe essere riconosciuta da subito. In caso contrario, diversi progetti sceglieranno nuovamente la via delle giurisdizioni estere con una perdita di attrattività per la piazza finanziaria svizzera.

* * *

Vi ringraziamo per voler prendere in debita considerazione quanto sopra.

Ticino Blockchain Technologies Association

Ticino Blockchain Technologies Association
Email: info@tbta.ch
Web: https://www.tbta.ch

Eidgenössische Finanzmarktaufsicht FINMA
Laupenstrasse 27
CH-3003 Bern

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

Wallisellen, 4. Januar 2021

Stellungnahme ubitec zum **Entwurf der „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 16. November 2020 eröffnete Anhörung bezüglich der Teilrevision des FINMA-Rundschreibens 2016/7 Video- und Online-Identifizierung (nachfolgend «Rundschreiben»). Mit diesem Schreiben möchten wir zum teilrevidierten Rundschreiben Stellung nehmen und Ihnen unsere Anliegen unterbreiten. Wir bedanken uns sehr für diese Möglichkeit einer Stellungnahme.

Die ubitec AG (nachfolgend ‚ubitec‘) ist Spezialistin für digitale Lösungen im Finanz- und Versicherungssektor. Mit ubiID bieten wir auf dem Finanzplatz in der Schweiz und in Europa eine Softwarelösung an, welche die digitale Identifizierung ermöglicht. Unser Ziel ist es dabei, eine sichere Lösung anzubieten, die gleichzeitig den Bedürfnissen der Endnutzer entspricht. Im Rahmen dieser Softwarelösung standen wir in den letzten sechs Monaten mit über 50 Schweizer Banken zum Thema digitale Identifizierung in Kontakt. Dabei decken sich unsere Erfahrungen mit jenen unserer europäischen Kollegen: Die Banken sind auf der Suche nach einer Alternative zum Video-Identifizierungsverfahren. Anhand dieser Gespräche mit Finanzmarktteilnehmern und basierend auf unserer technologischen Expertise, möchten wir folgende Punkte festhalten:

1 ubitec begrüsst die Anpassung des Rundschreibens an neue technologische Möglichkeiten.

2 Die im Rundschreiben definierten flankierenden Sicherheitsvorkehrungen bei der Online-Identifizierung sind unserer Ansicht nach nur teilweise praxistauglich. Die Sicherheitsvorkehrungen sollten wenigstens um einen Optionenkatalog von Sicherheitsvorkehrungen erweitert werden. So kann der Finanzintermediär aus verschiedenen Optionen mind. zwei Sicherheitsvorkehrungen auswählen.

3 Die FINMA kann mit geringfügigen Anpassungen des Rundschreibens ein asynchrones Video-Identifizierungsverfahren ermöglichen, welches den aktuellen Sicherheitsstandard bewahrt und wesentliche Nachteile der heutigen Video- und Online-Identifizierung eliminiert.

Folgende weitere Anliegen möchten wir zudem bei der FINMA platzieren:

4 Das KKG verlangt für den Abschluss und den Widerruf des Kreditvertrages die Form der einfachen Schriftlichkeit. Damit der Abschluss auf digitalem Weg erfolgen kann, ist eine qualifizierte elektronische Signatur (QES) notwendig. Gemäss Art. 7 Abs. 2 VZertES kann die QES bei Finanzintermediären nur im Rahmen einer «audiovisuellen Kommunikation in Echtzeit» erfolgen. BAKOM bezieht sich mit diesem Ausdruck auf das Video-Identifizierungsverfahren. Wir würden es sehr begrüssen, wenn die FINMA mit dem BAKOM zusammen gemeinsam eine Lösung erarbeitet, um in Zukunft auch die weiteren von der FINMA erlaubten Identifizierungsverfahren für eine qualifizierte elektronische Signatur nutzen zu können.

5 Aufgrund der dynamischen technologischen Entwicklung und des zunehmenden internationalen Wettbewerbsdrucks, würden wir einen kürzeren Aktualisierungszyklus des Rundschreibens Video- und Online-Identifizierung begrüssen.

1 Anpassung des Rundschreibens

Wir begrüssen, dass die FINMA dem technologischen Wandel Rechnung trägt und neue Möglichkeiten regelmässig prüft. Die von der FINMA vorgeschlagenen Änderungen des Rundschreibens gehen unserer Meinung nach in eine gute Richtung, decken aber wesentliche Teile einer nutzerfreundlichen Identifizierungslösung sowie die Kernbedürfnisse der Schweizer Finanzinstitute nicht oder nur ungenügend ab. Ausserdem gehen die vorgeschlagenen Anpassungen aus unserer Sicht zu wenig weit, da sie den aktuellen technologischen Möglichkeiten nicht genügend Rechnung tragen. Gerne legen wir Ihnen nachfolgend unsere Ansichten und Anliegen dar.

2 Sicherheitsvorkehrungen Online-Identifizierung

Die Online-Identifizierung ist gemäss Rundschreiben nur in Verbindung mit flankierenden Sicherheitsvorkehrungen möglich. Die Praxistauglichkeit, sowohl der bestehenden als auch der neu vorgeschlagenen Sicherheitsvorkehrungen (siehe Kapitel 2.3), sind unserer Ansicht zu wenig gegeben und decken die von den Finanzintermediären erwartete sowie die von deren Endkunden geforderte Nutzerfreundlichkeit («Usability») nicht ausreichend ab. Im Folgenden möchten wir deshalb einerseits die kritischen Punkte der einzelnen Sicherheitsvorkehrungen erläutern und andererseits mögliche Alternativen aufzeigen.

2.1 Sicherheitsvorkehrung: Referenzüberweisung

Die ergänzende Referenzüberweisung schränkt die Anwenderfreundlichkeit der Online-Identifizierung stark ein. Zudem stellt es den Finanzintermediär vor verschiedene prozessuale Herausforderungen, welche oft nur mit manuellen Schritten zu überwinden sind. Konkret hat die Referenzüberweisung folgende Nachteile, die in der Gesamtbetrachtung die an sich nützliche Online-Identifizierung für eine Vielzahl von Fällen uninteressant werden lässt:

- Komplexitätssteigerung für Kunden
- Verzögerung digitaler Geschäftsbeziehungen
- Psychologische Hürde
- Komplexitätssteigerung für Finanzintermediäre
- Teilabdeckung

2.1.1 Komplexitätssteigerung für Kunden

Eine ergänzende Referenzüberweisung fügt dem zugrundeliegenden digitalen Geschäft einen Komplexitätsfaktor hinzu und macht den Gesamtprozess für den Kunden deutlich unattraktiver (fehlende „Usability"). Nachdem der Prozess aus Sicht des Endnutzers bereits abgeschlossen wurde, muss dieser anschliessend aus eigener Initiative einen weiteren Prozessschritt ausführen: Er muss sich auf sein Bankkonto einloggen, die Überweisungsmaske ausfüllen und die Referenzüberweisung autorisieren. Für letzteres muss in der Regel ein weiterer Gegenstand genutzt werden (z.B. Mobiltelefon). Dieser gesamte Vorgang schränkt die Nutzerfreundlichkeit stark ein und führt zu Prozessabbrüchen.

2.1.2 Verzögerung digitaler Geschäftsbeziehungen

Durch den weiteren Prozessschritt verzögern sich digitale Geschäfte. Einer der Vorteile der Digitalisierung ist die Beschleunigung und Vereinfachung durch automatisierte Abläufe. Durch die Referenzüberweisung wird das Gegenteil erreicht.

2.1.3 Psychologische Hürde

Ein Zwang, vor Beginn einer Geschäftsbeziehung zunächst eine Zahlung – sei diese noch so gering – an die Bank zu veranlassen, ist nicht für jeden verständlich und löst entsprechend bei vielen Menschen eine Verunsicherung aus. Dies wirkt als psychologische Hürde für die Überweisung und führt zu vermehrten Geschäftsabbrüchen.

2.1.4 Komplexitätssteigerung für Finanzintermediäre

Mit der Referenzüberweisung als Sicherheitsvorkehrung müssen Finanzintermediäre zusätzlich zum Identifikationsprozess weitere Prozesse einrichten, dauerhaft nutzen und pflegen, und zwar mindestens:

- Überwachung eingegangener Referenzüberweisungen,
- Auslesen der Überweisungsdatensätze,
- Zuordnung zu konkreten Neukunden,
- Gutschrift/Rückzahlung des überwiesenen Betrags an Kunden,
- Erinnerung des Kunden bei ausbleibender Überweisung.

Hinzu kommt, dass die technische Zuordnung der Überweisung zu einem konkreten Kunden nicht

immer trivial ist, z.B. bei Gemeinschaftskonten (Erika Meier und Hans Müller) oder wenn die Namen Umlaute enthalten, die unterschiedlich darstellbar sind (Hans Müller, Hans Mueller). Für Finanzintermediäre bedeuten diese Faktoren erhebliche Mehrkosten und der Anreiz zur Digitalisierung des Identifikationsprozesses geht verloren.

2.1.5 Teilabdeckung

Die Referenzüberweisung und damit indirekt auch die Online-Identifizierung ist in vielen Anwendungsfällen eingeschränkt oder gar nicht nutzbar, wie z.B. für

- Jugendliche, die noch kein eigenes Konto haben,
- Jugendliche, die sich bei Erreichen der Volljährigkeit identifizieren müssen,
- Ausländische Personen, welche noch kein Konto in einem Staat besitzen, welcher die FATF-Kriterien erfüllt,
- Neugegründete juristische Personen,
- Personen, bei denen eine Wiederidentifizierung notwendig ist

2.2 Sicherheitsvorkehrung: Überprüfung Wohnsitzadresse

Die Überprüfung der Wohnsitzadresse ist bereits heute vollautomatisierbar durch eine Anbindung an ein öffentliches Register oder an eine durch einen vertrauenswürdigen Privaten geführte Datenbank. Da es aber auch in diesem Prozess zu Fehler kommen kann, ist eine weitere vollautomatische Überprüfung des Wohnsitzes wünschenswert, um so eine alternative Überprüfung zu ermöglichen. Eine heute bereits verfügbare und denkbare Alternative ist die Geolokalisierung. Diese erlaubt es, mittels Standortdaten Informationen zum aktuellen Standort zu erhalten und diese mit der erfassten Wohnsitzadresse abzugleichen. Aus Praktikabilitätsgründen schlagen wir hierbei einen Abgleich auf Ebene der erfassten Ortschaft und des lokalisierten Ortes vor, da die Standortdaten nicht immer bis auf die Strasse und Hausnummer exakt sind.

2.3 Sicherheitsvorkehrung: Chip Scan

Das Hauptproblem dieser Sicherheitsvorkehrung ist ihre starke Limitierung. Leider gibt es keine exakten Zahlen, wie verbreitet der Schweizer Pass in der Bevölkerung ist. Schätzungen zu Folge verfügen jedoch nur 40% (Schätzgenauigkeit +/- 10%) der Schweizerinnen und Schweizer über einen Pass 10. Die Schweizer Identitätskarte ist nach wie vor beliebter und wird entsprechend weitaus häufiger zur Identifizierung verwendet. Allerdings ist der Einsatz von NFC Chips in der Schweizer Identitätskarte nicht absehbar. Die Nutzung dieses Verfahren wird jedoch nicht nur durch die Ausweisdokumente, sondern zusätzlich durch die zum Scan benötigten Mobilgeräte limitiert: Stand heute sind nicht alle Smartphones NFC-fähig, gerade ältere Geräte verfügen nicht über die nötige Technologie. Da die Einsatzmöglichkeiten des Chip Scan somit stark limitiert sind, wird in der Praxis unter dem aktuellen Rundschreiben weiterhin in den meisten Fällen eine Referenz-Banküberweisung notwendig sein, die wir aus Gründen der Praktikabilität für ungeeignet erachten.

2.4 Fazit bestehende und neu geplante Sicherheitsvorkehrungen

Die Darlegungen im Kapitel 2 zeigen klar auf, dass die bestehenden und die neu geplanten (siehe Chip Scan) Sicherheitsvorkehrungen vor allem bezüglich ihrer Usability, der durchgängigen Prozessdigitalisierung sowie ihrer Verbreitung innerhalb der Schweizer Bevölkerung nicht genügen.

Damit der Schweizer Finanzplatz gemäss den strategischen Zielen der FINMA innovativ, sicher und wettbewerbsfähig bleibt, sollte zumindest ein Optionenkatalog an Sicherheitsvorkehrungen eingeführt werden. Dieser räumt Finanzintermediären die Wahlmöglichkeit ein, anstelle der bestehenden und neu geplanten (Chip Scan) Sicherheitsvorkehrungen gleichermassen geeignete Alternativen zu verwenden (siehe Kapitel 2.5). So wird nicht nur eine bessere Usability gewährleistet, sondern erlaubt Finanzinstituten auch eine breitere Auswahl an Use Cases abzudecken.

2.5 Optionenkatalog Sicherheitsvorkehrungen

Nachstehend listen wir einige Vorschläge auf, wie alternative Sicherheitsvorkehrungen ausgestaltet werden können.

- **Durchgängige Videosequenzen in Echtzeit:** Anstelle von Lichtbildern erhöht eine durchgängig in Echtzeit erstellte Videosequenz (Live-Videostream) über den gesamten Prozess (Ausweisscan, Gesichtsscan, Lebenderkennung) die Sicherheit massiv.
- **Lebenderkennung (liveness detection):** Es sind Vorkehrungen zu treffen, die ausschliessen, dass im Video eine fremde oder eine nicht lebende Person auftritt. Mit diesem Check wird somit geklärt, ob eine reale, lebendige Person anwesend ist oder ob die Daten von einem unbelebten Objekt (Spoof) stammen.
- **Umgebungskontrolle (environment control):** Beim Identifizierungsvorgang ist sicherzustellen, dass die Lichtverhältnisse und die Kameraauflösung den Qualitätsanforderungen für eine erfolgreiche und sichere Erkennung (biometrischer Gesichtsabgleich, Lebenderkennung, Dokumentencheck) genügt.
- **Standortdaten:** Daten über den aktuellen Standort der Vertragspartei können über die Geolokalisierung ermittelt werden. Im Rahmen des Echtzeitverfahrens können diese Daten zur Plausibilisierung des Aufenthalts- oder Wohnortes hinzugezogen werden.
- **Nachgelagerte Verifikation:** Gibt es im Prozess Unsicherheiten (z.B. Abweichung ausgelesene Daten vs. erfasste Daten, biometrischer Gesichtsabgleich keine sehr hohe Übereinstimmung etc.) muss die Videosequenz von einer geschulten Person im Nachgang angeschaut und überprüft werden.

3 Asynchrones Video-Identifizierungsverfahren

Gemäss Erläuterungsbericht Seite 5 haben diverse Finanzdienstleister gegenüber der FINMA den Wunsch nach einem Auto-Ident Verfahren geäussert. Dies deckt sich mit den Erfahrungen aus unseren Gesprächen mit über 50 Finanzintermediären in der gesamten Schweiz. Bereits heute steht fest, dass Schweizer Finanzintermediäre bezüglich Digital Client Onboarding gegenüber der europäischen Konkurrenz einen empfindlichen Wettbewerbsnachteil erleiden, was den Finanzplatz Schweiz auf Dauer schwächen könnte. Deshalb möchten wir in diesem Kapitel aufzeigen, wie die FINMA auf Basis des heutigen Rundschreibens mit lediglich geringfügigen Änderungen ein Auto-Identifizierungsverfahren im Sinne eines asynchronen Video-Identifizierungsverfahren zulassen könnte. Dieses Verfahren stiess in unseren Gesprächen mit den Finanzintermediären auf grosses Interesse, da es die Nachteile der Video-Identifizierung und Online-Identifizierung eliminiert und gleichzeitig höchste Sicherheit gewährleistet.

3.1 Beschreibung des Verfahrens

Der Prozess beim asynchronen Video-Identifizierungsverfahren ist nahezu identisch zur Video-Identifizierung gemäss aktuellem Rundschreiben. Der wesentliche Unterschied ist, dass die Vertragspartei mittels Software und nicht via Live-Agent automatisch durch den Identifizierungsprozess geleitet wird. Der Kunde kann sich somit rund um die Uhr identifizieren ohne dass er dabei mit einem Live-Agenten sprechen muss. Im Nachgang zur Video-Identifizierung führt ein geschulter Mitarbeiter anhand der aufgenommenen Videosequenz die Verifikation durch. Dieses Verfahren bietet doppelte Sicherheit: Einerseits überprüft die Software automatisch alle Dokumente und führt gleichzeitig einen biometrischen Gesichtsabgleich sowie eine Lebendigkeitserkennung durch. Andererseits werden all diese Checks zusätzlich durch einen Mitarbeiter wiederholt. Da es sich dabei um ein asynchrones Verfahren handelt, muss der Kunde dieses nicht erst abwarten und ist auch nicht auf die unmittelbare Verfügbarkeit von Mitarbeitenden angewiesen. Finanzintermediäre können die Verifikation effizient im Nachgang durchführen, was mit einer deutlichen Kostenersparnis gegenüber dem bestehenden Video-Identifizierungsverfahren einhergeht.

3.2 Konformität im internationalen Umfeld

In Bezug auf Seite sechs des Erläuterungsberichts möchten wir nun aufzeigen, wie das Verfahren im internationalen Umfeld eingegliedert werden kann. Die FATF-Konformität des asynchronen Video-Identifikationsverfahrens lässt sich mit Hilfe des Dokuments Guidance on Digital ID[1], konkret anhand der Abschnitte 89, 171 und Appendix E, Table 4, beurteilen. Die so abgeleiteten Anforderungen könnten im Rundschreiben durch die Erweiterung von Sektion III «Videoidentifizierung» einfach ergänzt werden. Zusätzlich wäre mit der Einführung einer nachgelagerten Prüfung der Videosequenzen durch einen Mitarbeiter das Identity Assurance Level 3 (IAL 3) gemäss NIST Standard erfüllt.
Im europäischen Umfeld gibt es zudem verschiedene gesetzliche Möglichkeiten, um alternative Identifizierungsverfahren zuzulassen. Ein Haupttreiber ist die in der eIDAS[2] verankerte Klausel[3], die Identifizierungsmethoden zulässt, sofern sie auf nationaler Ebene anerkannt sind und zudem eine gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten. Im europäischen Raum wird diese Möglichkeit bereits durch Spanien genutzt, weitere EU-Länder folgen aktuell diesem Beispiel. Die SEPBLAC[4] hat bereits 2017 ein asynchrones Video-Identifizierungsverfahren für Finanzintermediäre zugelassen. Durch die im Rundschreiben festgelegte Sicherheitsvorkehrung der Referenzüberweisung (siehe Rz. 33) erkennt auch die FINMA indirekt diese Verfahren an.

3.3 Vorschlag zur Eingliederung im FINMA Rundschreiben

Mit geringfügigen Änderungen des heutigen Rundschreibens kann künftig auch in der Schweiz ein asynchrones Video-Identifizierungsverfahren genutzt werden. Im beiliegenden PDF «Änderungsvorschlag FINMA RS für asynchrone Videoidentifizierung» zeigen wir auf, an welchen Stellen das Rundschreiben zur Videoidentifizierung geringfügig angepasst werden müsste. Die wesentliche

[1] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html
[2] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[3] Art. 24 Abs. 1 lit. d eIDAS
[4] Servicio Ejecutivo de la Comisión de Prevenicón de Blanqueo de Capitales e Infracciones Monetarias

Änderung betrifft dabei die Bezeichnungen: Statt vom Videogespräch ist neu vom Videoidentifizierungsvorgang die Rede. Ausserdem bräuchte es neu statt eines Gesprächsleitfadens lediglich einen Leitfaden (Prozessbeschreibung, Checkliste), anhand der betraute Mitarbeitende die Verifikation vornehmen.
Wir sind überzeugt, dass die vorgeschlagenen Änderungen die Sicherheit der Video-Identifizierung weiterhin gewährleisten, während den Finanzintermediären gleichzeitig neue Möglichkeiten eröffnet werden. Das Verfahren legt zudem die Basis für ein späteres, vollumfänglich automatisiertes Auto-Identifikationsverfahren (ohne manuelle Verifikation). Nicht zuletzt liefern die so gesammelten Erfahrungen und Daten der FINMA die Grundlage für eine faktenbasierte Entscheidung über die Einführung eines solchen vollständig automatisierten Verfahrens.

3.4 Abschliessende Überlegungen

Viele europäischen Staaten erkennen bereits heute Verfahren zur automatisationsgestützten Online-Identifizierung an (z.B. Grossbritannien, Spanien, Liechtenstein, Luxemburg, Rumänien, etc), womit es sich zum neuen Standard in der FinTech-Industrie entwickelt hat. Grund dafür ist die Sicherheit der Verfahren, die hohe Betrugserkennungsrate, die Geschwindigkeit der Identifizierung sowie die wesentlich geringeren Kosten pro Identifizierung. Der bereits sehr hohe Sicherheitsstandard dieser Verfahren wird durch immer bessere Algorithmen im Bereich Text- und Bilderkennung stetig verbessert und gewährleistet. Auch im Bereich der Betrugserkennung kommen automatisierte Programme zum Einsatz, da diese Daten und Muster wesentlich schneller erkennen und abgleichen können. Als zusätzliche Sicherheitsstufe, um die Ergebnisse solcher Programme zu überprüfen, werden alle Identifizierungen dann noch von einem Mitarbeiter nachvollzogen und abschliessend bestätigt. Da herkömmliche Methoden faktisch kein höheres Sicherheitsniveau bieten als das beschriebene asynchrone Video-Identifizierungsverfahren, gibt es aus unserer Perspektive keine objektivierbare Rechtfertigung dafür, diese Verfahren, welche den höchsten Sicherheitsstandard bieten, nicht auch in der Schweiz anzuerkennen. Schliesslich stellt eine fehlende offizielle Anerkennung dieses Verfahrens für Schweizer Finanzintermediäre einen signifikanten Wettbewerbsnachteil im europäischen Kontext dar.

Wir bitten Sie freundlich, unsere Anträge wohlwollend zu prüfen. Für Rückfragen oder eine Diskussion stehen wir jederzeit gerne zur Verfügung.

Freundliche Grüsse

ubitec AG

Patrick Brazzale
CEO

Ralf Jenzer
Managing Partner

Anhang:

- Dieses Schreiben als Word
- «Änderungsvorschlag FINMA RS für asynchrone Videoidentifizierung» als Excel und PDF

Anpassung FINMA RS 2016/7 Videoidentifizierung Rz. 5 - 22: Abdeckung einer "klassischen" und "asynchronen" Video-Identifizierung

Rz	FINMA RS aktuell	Änderungsvorschlag für Video-Identifizierung "klassisch" und "asynchron"
5	Der Identifizierung bei persönlicher Vorsprache gleichgestellt ist die Videoidentifizierung, soweit sie die folgenden Grundsätze erfüllt:	
	III.A. a) Technisches und Organisatorisches	
6	Die Identifizierung erfolgt mittels audiovisueller Kommunikation in Echtzeit (live-Schaltung) zwischen der Vertragspartei und dem Finanzintermediär.	
6	Der Finanzintermediär setzt dafür geeignete technische Hilfsmittel ein, die eine sichere Übertragung sowie das Auslesen und Entschlüsseln der Informationen in der maschinenlesbaren Zone (Machine Readable Zone, MRZ) auf dem Identifizierungsdokument sicherstellen.	
7	Bild- und Tonqualität müssen geeignet sein, um eine einwandfreie Identifizierung zu ermöglichen. Der Finanzintermediär kann technische Mittel einsetzen um schwierige Lichtverhältnisse, insbesondere bei der Erstellung der im Rahmen der Identifizierung notwendigen Lichtbilder, zu kompensieren.	
8	Die Identifizierung der Vertragspartei erfolgt durch entsprechend geschulte Mitarbeitende des Finanzintermediärs.	
8	Die **gesamte Dauer des Gesprächs** muss mittels Audioaufzeichnung festgehalten werden.	Die **gesamte Dauer des Identifizierungsvorgangs** muss mittels einer Audio- oder Videoaufzeichnung festgehalten werden.
9	Der Finanzintermediär erstellt für die Durchführung **des Identifizierungsgesprächs** einen Prozess sowie einen **Gesprächsleitfaden** für die mit der Videoidentifizierung betrauten Mitarbeiter.	Der Finanzintermediär erstellt für die Durchführung **der Identifizierung** einen Prozess sowie einen **Leitfaden** für die mit der Videoidentifizierung betrauten Mitarbeiter.
	III.A. b) Identitätsprüfung	
10	Die Identitätsprüfung von natürlichen Personen mittels Videoidentifizierung richtet sich nach Rz 11–22.	
11	Der Finanzintermediär gestaltet den Prozess zur Aufnahme der Geschäftsbeziehung über Online-Kanäle so, dass die Vertragspartei die Angaben nach Art. 44 und 60 GwV-FINMA bereits vor dem audiovisuellen Identifizierungsgespräch elektronisch erfasst und dem Finanzintermediär übermittelt.	
11	Dieser überprüft sie im Rahmen **des Identifizierungsgesprächs** mittels geeigneter technischer Hilfsmittel oder anhand von gezielten Fragen.	Dieser überprüft sie im Rahmen **des Identifizierungsvorgang**s mittels geeigneter technischer Hilfsmittel oder anhand von gezielten Fragen.
11	Dabei achtet er auch auf auffällige Verhaltensweisen, welche Hinweise auf gefälschte Ausweise liefern könnten.	
11	Ferner gleicht er die Angaben, die er im Rahmen des Prozesses zur Aufnahme der Geschäftsbeziehung erlangt hat, mit denjenigen auf dem Identifizierungsdokument der Vertragspartei ab.	
12	Der Finanzintermediär holt vor Beginn **des Videogesprächs** das ausdrückliche Einverständnis der Vertragspartei zur Durchführung der Videoidentifizierung und **der Audioaufzeichnung des Gesprächs** ein.	Der Finanzintermediär holt vor Beginn **des Identifizierungsvorgangs** das ausdrückliche Einverständnis der Vertragspartei zur Durchführung der Videoidentifizierung und der **Audio- bzw. Videoaufzeichnung des Vorgangs** ein.
13	Der Finanzintermediär erstellt während der Videoübertragung Lichtbilder von der Vertragspartei wie auch von allen relevanten Seiten des Identifizierungsdokuments und prüft die Übereinstimmung der erstellten Lichtbilder der Vertragspartei mit dem Lichtbild des Identifizierungsdokuments.	

Rz	FINMA RS aktuell	Änderungsvorschlag für Video-Identifizierung "klassisch" und "asynchron"
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 eines optisch variablen und eines weiteren zufällig ausgewählten Sicherheitsmerkmals des Identifizierungsdokuments.	
14	Letzteres kann mittels technischer Unterstützung oder visueller Überzeugung (bspw. Kippen des Ausweises) erfolgen.	
14	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.	
14	Ist er mit dem Identifizierungsdokument nicht vertraut, vergleicht er das Dokument mit Referenzen aus einer Ausweisdatenbank bezüglich Sicherheitsmerkmalen, Zeichenart sowie -grösse und Layout.	
15	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.	
16	Aufgehoben	
17	Jeder Identifizierungsvorgang ist zu dokumentieren. Die Lichtbildaufnahmen des Identifizierungsdokuments und der Vertragspartei sowie die Audioaufzeichnung des gesamten Identifizierungsvorgangs sind zu den Akten zu nehmen und zu archivieren.	Jeder Identifizierungsvorgang ist zu dokumentieren. Die Lichtbildaufnahmen des Identifizierungsdokuments und der Vertragspartei sowie die Audio- **bzw. Videoaufzeichnung** des gesamten Identifizierungsvorgangs sind zu den Akten zu nehmen und zu archivieren.
	III.A. c) Abbruch des Identifizierungsvorgangs per Video	**Abbruch des Identifizierungsvorgangs**
18	Der Finanzintermediär bricht den Identifizierungsvorgang **per Video** ab,	Der Finanzintermediär bricht den Identifizierungsvorgang ab,
19	wenn die Bild- und/oder Tonqualität eine einwandfreie Identifizierung der Vertragspartei nicht erlauben; oder	
20	aufgehoben	
21	wenn Zweifel an der Echtheit des Ausweisdokuments oder der Identität der Vertragspartei aufkommen.	
22	Der Abbruch des Identifizierungsvorgangs kann auch darin bestehen, dass der Kunde für die fraglichen Identifizierungsschritte auf herkömmliche Kanäle (persönliche Vorsprache, Korrespondenzweg) verwiesen wird.	
22	Sofern der Finanzintermediär Hinweise auf erhöhte Risiken erlangt, darf er den Identifizierungsvorgang zwar fortführen.	
22	Er stellt jedoch sicher, dass die Geschäftsbeziehung erst aufgenommen wird, wenn die erforderliche Zustimmung einer vorgesetzten Person, einer vorgesetzten Stelle oder der Geschäftsführung gemäss Art. 18 GwV-FINMA vorliegt.	

Zürich, 1.2.2021

Anhörung Teilrevision FINMA Rundschreiben 2016-17 – Feedback YAPEAL

Guten Tag

Als Fintech-lizenziertes Unternehmen (Person nach Art. 1b Bankengesetz) hat YAPEAL AG folgende Anforderungen:

1. Gleichwertige Berücksichtigung von **Person nach Art. 1b Bankengesetz** wie «Bank». Z.B. in Rz 33 «… lautenden Konto bei einer **Bank…**» . Begründung: YAPEAL muss dieselbe GwG-Regelung bei der Kundenidentifikation wie eine Bank anwenden. Daher sollte eine initiale Geldüberweisung ab einem YAPEAL Kundenkonto zur Kundenidentifikation von anderen Finanzintermediären für welche dieses Rundschreiben gilt akzeptiert werden können.

Der Finanzintermediär lässt sich bzw. der ~~Depotbank~~ Bank 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 Bank in einem 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.	33

2. Zur Identifikation von Firmenkunden (juristische Personen wie AG, GmbH oder Einzelfirmen, welche im Handelsregister eingetragen sind) sollte es erlaubt sein, einen technisch sicher verifizierten elektronischen Handelregisterauszug (vom Handelsregisteramt oder einem anerkannten Dienstleister wie www.Moneyouse.ch) als gleichwertige Alternative zu einem notariell beglaubigten physischen (papierbasierten) Handelsregisterauszug zu verwenden.

Freundliche Grüsse

Enrico Bauer
COO

079 360 21 21
enrico.bauer@yapeal.ch