

Eidgenössische Finanzmarktaufsicht FINMA  
Isabel Grüninger  
Laupenstrasse 27  
CH-3003 Bern

Per Mail zugestellt an: [isabel.grueninger@finma.ch](mailto: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 risikoreicher 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 geeigneten 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.<sup>1</sup> 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

---

<sup>1</sup> [https://docbox.etsi.org/esi/Open/Latest\\_Drafts/Draft%20ETSI-TS-119-461-v0.0.5.pdf](https://docbox.etsi.org/esi/Open/Latest_Drafts/Draft%20ETSI-TS-119-461-v0.0.5.pdf).

# • SwissBanking

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:

- **Videsequenzen 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<sup>2</sup> genutzt und weitere EU-Länder folgen diesem Beispiel. Möglich macht dies die in der eIDAS<sup>3</sup> 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<sup>4</sup> hohe Branchenstandards entwickelt.
- Eine Lebendigkeitsprüfung kann durch sinnvolle und zufällig ausgewählte **Challenge-Response Elemente** in Ton, Video oder am *User Interface* angereichert werden.

---

<sup>2</sup> Die *Servicio Ejecutivo de la Comisión de Prevención 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.

<sup>3</sup> 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.

<sup>4</sup> 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 gleichgestellt 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).

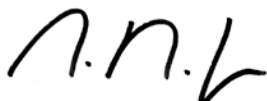
### **V.3 Knappe Anhörungsfrist und Zeitpunkt**

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