

FINMA-Rundschreiben 2016/7 „Video- und Online- Identifizierung“

**Bericht über die Anhörung vom 13. Februar 2018 bis 28. März
2018 zum Entwurf des teilrevidierten Rundschreibens**

20. Juni 2018

Inhaltsverzeichnis

Kernpunkte.....	3
Abkürzungsverzeichnis	5
1 Einleitung.....	6
2 Eingegangene Stellungnahmen	6
3 Ergebnisse der Anhörung und Beurteilung durch die FINMA	7
3.1 Allgemeine Punkte	7
3.2 Geltungsbereich (Rz 2–4)	8
3.3 Videoidentifizierung.....	9
3.3.1 Der persönlichen Vorsprache gleichgestellte Videoidentifizierung einer natürlichen Person (Rz 5– 22).....	9
3.3.1.1 Technisches und Organisatorisches (Rz 6–9)	9
3.3.1.2 Identitätsprüfung (Rz 10–17)	10
3.3.1.3 Abbruch des Identifizierungsvorgangs per Video (Rz 18–22).....	12
3.4 Online-Identifizierung	13
3.4.1 Online-Identifizierung mittels elektronischer Ausweiskopie (Rz 31–44).....	13
3.4.1.1 Elektronische Ausweiskopie mit Echtheitsprüfung durch den Finanzintermediär (Rz 32–37)	14
3.4.1.2 Elektronische Ausweiskopie mit qualifizierter elektronischer Signatur (Rz 38–39)	17
4 Weiteres Vorgehen	18

Kernpunkte

Hintergrund Teilrevision

1. Am 18. März 2016 wurde das Rundschreiben 2016/7 „Video- und Online-Identifizierung“ in Kraft gesetzt. Die ex-post Evaluation zeigt, dass einige Vorgaben noch nicht oder nicht mehr optimal auf den Finanzmarkt und die Finanzintermediäre abgestimmt sind. Durch die Teilrevision des Rundschreibens „Video- und Online-Identifizierung“ wird den Praxiserfahrungen und dem technologischen Wandel Rechnung getragen. Erkannte Hürden und ineffiziente Prozesse beim Einsatz der Video- und Online-Identifizierung werden reduziert. Gleichzeitig werden Missbrauchsrisiken adressiert, um möglichst sichere Prozesse zu gewährleisten.

Anhörungsergebnisse

2. Die Lockerungen der Vorgaben (bspw. Abschaffung TAN, Identifizierungsprozess darf bei Hinweisen auf erhöhte Risiken fortgesetzt werden, unter bestimmten Voraussetzungen ist eine Überweisung von einer Bank in einem FATF Land erlaubt) wurden von den Anhörungsmitgliedern mehrheitlich begrüsst und als sinnvoll erachtet.
3. Kritisch beurteilt wurde insbesondere die neue Vorgabe bei der Video- und Online-Identifizierung, dass drei Sicherheitsmerkmale geprüft werden müssen (vorher ein optisch-variables Merkmal, bzw. keine Prüfung bei der Online-Identifizierung) und dass ein Abgleich des Identifizierungsdokuments mit einer Referenzdatenbank erfolgen muss.
4. Einzelne Anhörungsmitglieder haben sich für strengere Vorgaben ausgesprochen und bspw. eine Videoaufzeichnung und konkrete Vorschriften zum Verschlüsselungsstandard gefordert.
5. Zudem wurde die Übergangsfrist von sechs Monaten für die Anpassungen der Prozesse als zu kurz erachtet.

Änderungen gegenüber Anhörungsentwurf

6. Festlegung der zu prüfenden Sicherheitsmerkmale auf zwei bei der Videoidentifizierung (davon ein optisch-variables) und zwei bei der Online-Identifizierung.
7. Der Abgleich der Identifizierungsdokumente mit einer Referenzdatenbank soll nicht bei jeder Identifizierung vorgenommen werden müssen, sondern nur dann, wenn der Finanzintermediär mit den vorgelegten Dokumenten nicht vertraut ist. Dies meint selten vorgelegte Ausweise von ausländischen Staaten.
8. Die Übergangsfrist für die Prozessanpassungen der Finanzintermediäre wird bis am 1. Januar 2020 verlängert. Bis dahin haben die Finanzintermediäre die Wahl, ob sie sich an die bisherige Fassung oder an das teilrevidierte Rundschreiben halten.

Abkürzungsverzeichnis

FATF	<i>Financial Action Task Force on Money Laundering</i>
GwG	Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (SR 955.0)
GwV-FINMA	Verordnung vom 3. Juni 2015 der Eidgenössischen Finanzmarktaufsicht über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor (SR 955.033.0)
MRZ	<i>Machine Readable Zone</i> . Sichtbarer Teil eines Ausweisdokumentes, der speziell dafür ausgelegt wurde, durch optische Texterkennung gelesen zu werden
PRADO	<i>Public Register of Authentic Identity and Travel Documents Online</i> . Öffentliches Online-Register echter Identitäts- und Reisedokumente
TAN	Transaktionsnummer, die der Finanzintermediär als Einmalpasswort zustellt
VSB	Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken
ZertES	Bundesgesetz vom 18. März 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (SR 943.03)

1 Einleitung

Vom 13. Februar 2018 bis 28. März 2018 führte die FINMA eine öffentliche Anhörung zum Entwurf des teilrevidierten Rundschreibens 2016/7 „Video- und Online-Identifizierung“ durch.

Zielsetzung der Teilrevision ist es, das Rundschreiben an die technologischen Neuerungen und an die Erfahrungen zur Anwendung des Rundschreibens seit seiner Inkraftsetzung im März 2016 anzupassen.

Der vorliegende Bericht geht in allgemeiner und zusammengefasster Form auf die eingegangenen Stellungnahmen der Anhörungsteilnehmer zum Anhörungsentwurf ein und erläutert, wo angebracht, einzelne Bestimmungen.

2 Eingegangene Stellungnahmen

Folgende Personen und Institutionen haben an der Anhörung teilgenommen und sich nicht gegen eine Publikation ihrer Stellungnahme ausgesprochen (in alphabetischer Reihenfolge):

- BitIncubator & Venture SA / Eidoo Sagl
- Bity SA
- DecentAge AG
- Dukascopy Bank SA
- EXPERTsuisse
- IDnow GmbH / Intrum AG
- Loyens & Loeff Schweiz GmbH
- Moving Media GmbH
- Schweizerische Bankiervereinigung
- Simplewealth AG
- SRO-SLV
- SRO-SVV
- Swisscom Blockchain AG
- Swisscom (Schweiz) AG
- Swiss Payment Association
- Swissquote Bank SA
- Verband Schweizerischer Kantonalbanken
- Verband Schweizerischer Vermögensverwalter VSV

3 Ergebnisse der Anhörung und Beurteilung durch die FINMA

3.1 Allgemeine Punkte

Stellungnahmen

Die Eingaben zur Anhörung spiegeln einen Querschnitt über die vom Rundschreiben betroffenen Marktteilnehmer. Es haben sich Banken und weitere Finanzintermediäre, im Bereich der Kryptowährungen tätige Unternehmen, Beratungsunternehmen für Fintech, Verbände, Selbstregulierungsorganisationen wie auch Anbieter, welche direkt Identifizierungsprozesse umsetzen, gemeldet.

Dabei stehen die meisten Anhörungsteilnehmer den geplanten Änderungen des Rundschreibens positiv gegenüber und begrüßen die zeitnahe Anpassung an technologische Entwicklungen.

Teilweise wurde seitens der Teilnehmer darauf hingewiesen, dass bei der Identifizierung mittels persönlicher Vorsprache oder auf dem Korrespondenzweg keine Vorgaben zur Überprüfung der Identifizierungsdokumente gelten. Dies stehe im Gegensatz zum vorliegenden Rundschreiben, welches strengere Vorgaben für das digitale Umfeld aufstelle.

Zudem haben einige Stellungnahmen in Bezug auf einzelne Bestimmungen eine Lockerung der entsprechenden Regelungen beantragt, währenddem sich andere Anhörungsteilnehmer für Präzisierungen und mehr Details, oder für eine strengere Umsetzung, ausgesprochen haben.

Würdigung

Technologieneutralität im Rahmen der Regulierung bedeutet, Regeln gegenüber technologischen Entwicklungen und Geschäftsmodellen neutral zu definieren. Allerdings heisst dies nicht zwingend, dass die digitale Erbringung unter denselben Anforderungen erfolgen kann wie die analoge. Im Fokus steht vielmehr, dass der mit der Regelung verfolgte Zweck und das Ergebnis, unabhängig von der Wahl des jeweiligen Kanals, gewährleistet werden können. Insbesondere im Kontext der Risikoüberwachung und -begrenzung führt dies unter Umständen dazu, dass die entsprechenden Anforderungen, je nach Risikoprofil, im digitalen Umfeld anders als im analogen auszugestalten sind.

Dies hat zur Folge, dass unter Technologieneutralität im Zusammenhang mit Finanzmarktregulierung nicht zwingend dieselben Regeln auf die digitale und die analoge Erbringung Anwendung finden. Bereits beim Inkrafttreten

des Rundschreibens im 2016 wurde darauf hingewiesen, dass die Aufnahme einer Geschäftsbeziehung und namentlich die Identifizierung der Vertragspartei über digitale Kanäle höhere Risiken beherbergt als dies bei einer persönlichen Vorsprache der Fall ist. Die Betrugs- und Fälschungsrisiken im Internet sind wesentlich grösser, weil digitale Bilddateien von Ausweisen einfacher und überzeugender gefälscht werden können als physische Ausweise. Dem steht gleichzeitig eine schwierigere Erkennbarkeit von Fälschungen durch den Finanzintermediär gegenüber, weil er vom Ausweis nur ein zweidimensionales Abbild zu sehen bekommt, währendem bei der persönlichen Vorsprache wie auch bei der Echtheitsbestätigung ein dreidimensionaler, physischer Ausweis vorgelegt wird, dessen mögliche Veränderungen durch Laminierung oder aufgeklebte Bilder einfacher zu erkennen sind. Um diesen anders gelagerten Risiken zu begegnen, sind über digitale Kanäle im Vergleich zur persönlichen Vorsprache zusätzliche und andere Anforderungen erforderlich, um eine vergleichbare Verlässlichkeit bei der Identifizierung der Vertragspartei zu bewirken.

Fazit

Die möglichst prinzipienbasierte Regulierung soll unter Berücksichtigung der Technologieneutralität beibehalten werden.

Das Rundschreiben wird auch zukünftig an neue technologische Entwicklungen angepasst werden.

3.2 Geltungsbereich (Rz 2–4)

Stellungnahmen

Insbesondere Banken, die neben anderen Finanzintermediären vom Anwendungsbereich des Rundschreibens erfasst werden, haben ausgeführt, dass die kurze Übergangsfrist zur Prozessanpassung zu knapp bemessen und eine zeitliche Annäherung an die kommende VSB-Revision gewünscht sei.

Würdigung

Die Übergangsfrist von 6 Monaten ab Publikation wird verlängert. Das teilrevidierte Rundschreiben wird per sofort in Kraft treten, den Finanzintermediären wird jedoch eine Übergangsfrist zur Anpassung der Prozesse bis am 1. Januar 2020 gewährt. Bis dahin können Finanzintermediäre entweder alle Erfordernisse des bisherigen oder alle Erfordernisse des teilrevidierten Rundschreibens anwenden.

Fazit

Die Übergangsfrist für die Finanzintermediäre wird bis am 1. Januar 2020 verlängert.

3.3 Videoidentifizierung

3.3.1 Der persönlichen Vorsprache gleichgestellte Videoidentifizierung einer natürlichen Person (Rz 5–22)

3.3.1.1 Technisches und Organisatorisches (Rz 6–9)

Stellungnahmen zu Rz 6 der Anhörungsversion

Ein Anhörungsteilnehmer hat angeregt, die Vorgaben zur „sicheren Übertragung“ im Rundschreiben genauer zu spezifizieren und insbesondere die Anforderungen an die Verschlüsselung aufzuführen.

Würdigung

Eine sichere und vertrauliche Datenübertragung ist eine Grundvoraussetzung für die Identifizierung über digitale Kanäle. Im Hinblick auf die rasanten technischen Entwicklungen und die prinzipienbasierte Regulierung wird auf die Spezifikation der Verschlüsselung verzichtet.

Fazit

Es wird keine Vorgabe zum Verschlüsselungsstandard eingeführt.

Stellungnahmen zu Rz 8 der Anhörungsversion

Eine Stellungnahme hat sich darauf bezogen, dass aus Nachvollziehbarkeitsgründen eine audiovisuelle Archivierung des Videogesprächs erfolgen sollte.

Würdigung

Eine Audioaufzeichnung des Videogesprächs reicht aus, um den Identifizierungsprozess nachvollziehen zu können und die Dokumentationspflicht zu erfüllen. Um den Prozess der Videoidentifizierung möglichst schlank zu halten und eine kosteneffiziente Umsetzung zu begünstigen, beschränkt sich das Archivierungserfordernis bewusst auf die Audiodatei.

Fazit

Bei der Videoidentifizierung muss das Gespräch weiterhin mittels Audioaufzeichnung, und nicht mittels Videoaufzeichnung, festgehalten werden.

3.3.1.2 Identitätsprüfung (Rz 10–17)

Stellungnahmen zu Rz 14 der Anhörungsversion

Bezüglich der MRZ hat eine Bank ausgeführt, dass nicht alle Länder ihre Identifizierungsdokumente mit einer MRZ versehen und solche Dokumente nicht vom Prozess der Videoidentifizierung ausgeschlossen werden sollten. Es wird vorgeschlagen, dass die MRZ nur als mögliche, jedoch nicht als zwingende Vorgabe zur Identifizierung gelten sollte. Ein weiterer Anhörungsteilnehmer hat angeregt, dass die Anforderung des maschinellen Auslesens der MRZ gestrichen werden sollte.

Zur Prüfung von drei optischen Sicherheitsmerkmalen haben etliche Anhörungsteilnehmer Bedenken geäußert und ausgeführt, dass nur wenige Länder über Identifizierungsdokumente mit drei oder mehr optisch-variablen Sicherheitsmerkmalen verfügen. Auch die Schweizer Identitätskarte habe keine drei optisch-variablen Sicherheitsmerkmale.

Kommentiert wurde zudem die neue Vorgabe, die Identifizierungsdokumente mit Referenzen aus einer Ausweisdatenbank abzugleichen. Der Abgleich wurde als aufwändig, zeit- und kostenintensiv sowie als manuell geprägt beurteilt. Einige Anhörungsteilnehmer haben vorgeschlagen, einen Datenbankabgleich nur dann vornehmen zu müssen, wenn Zweifel zur Echtheit der Dokumente bestehen sollten.

Würdigung

Aufgrund grösserer Betrugs- und Fälschungsrisiken im Internet besteht bei der Geschäftsaufnahme über digitale Kanäle, wie eingangs festgehalten, ein höheres Risiko als bei der Identifizierung via persönlicher Vorsprache oder bei der bisherigen Korrespondenzeröffnung mit Echtheitsbestätigung. Dabei kommt der maschinenlesbaren Zone eine besondere Bedeutung zu, da die darin festgehaltenen Informationen einerseits auf Widersprüche in sich geprüft werden können und somit Hinweise auf Fälschungen liefern können, und weil sie andererseits einen Abgleich mit den Angaben zulassen, welche die Vertragspartei über sich im Eröffnungsprozess gemacht hat. Da es sich dabei um maschinenlesbare Informationen handelt, macht ein visuelles Auslesen wenig Sinn und dürfte das Auslesen mit geeigneten Hilfsmitteln an Aufwand, Kosten und Risiken schnell übersteigen. Die Verwendung einer automatischen Texterkennung erfüllt das Kriterium des maschinellen Auslesens.

Reisedokumente enthalten eine maschinenlesbare Zone. Das Auslesen und Abgleichen der Informationen in der maschinenlesbaren Zone mit den restlichen Angaben auf dem Ausweis dienen einerseits dazu, die Echtheit des Identifizierungsdokuments zu plausibilisieren, und andererseits, die Übereinstimmung der Vertragspartei mit der Person auf dem vorgelegten Ausweis

sicherzustellen. Die maschinenlesbare Zone ist ein zusätzliches Sicherheitselement, das den erhöhten Fälschungsrisiken bei der Identifizierung auf dem digitalen Weg Rechnung trägt.

Bisher war im Rundschreiben die Prüfung eines optisch-variablen Sicherheitsmerkmals gefordert. Diesem Kriterium entsprechen bspw. die beugungsoptischen Merkmale wie Kinegram und Movigram. Neu wurde in der Teilrevision vorgeschlagen, drei optische Merkmale zu prüfen. Das Wort *optisch* hat sich dabei auf die optische Erkennbarkeit bezogen und nicht nur die beugungsoptischen, sondern insbesondere auch die weiteren Sicherheitsmerkmale wie Mikroschrift, Guillochen etc. umfasst. Die zahlreichen Rückmeldungen hierzu haben jedoch gezeigt, dass die Anhörungsmitglieder die zu prüfenden optischen Sicherheitsmerkmale anders aufgefasst haben und unter dem Ausdruck der *optischen Merkmale* weiterhin optisch-variablen Merkmale subsumierten.

Zur Klarstellung wird im Vergleich zur Anhörung die Anzahl und Art der zu prüfenden Sicherheitsmerkmale präzisiert. Neu soll ein optisch-variables (entspricht der ursprünglichen Anforderung) plus ein weiteres zufällig ausgewähltes Sicherheitsmerkmal überprüft werden. Beispiele für weitere Sicherheitsmerkmale sind (nicht optisch-variable, nicht abschliessende Aufzählung):

Beispiele CH Identitätskarte

- Farbige Linienmuster (Guillochen)
- Optisch erkennbare Erhebungen (ID-Nummer, Geburtsdatum, Grösse)
- Mikroschrift
- Farbverlauf
- Gravierte Nummer über dem Bild des Gesichts

Beispiele CH Pass

- Allgemein:
 - Geometrische farbige Muster auf den Seiten
 - Durchstich der Seiten
- Einbandinnenseite vorne:
 - Verschiedenfarbige Kreuze
 - Farbige Linienmuster (Guillochen)
- Einbandinnenseite hinten:
 - Farbige Linienmuster (Guillochen)
- Personaldatenseite:
 - Mikroschrift
 - Optisch erkennbare Erhebungen (Passnummer und Grösse)

- Innenseiten:
 - Nummerierung mit zugehörigen Kantonswappen oder verschiedenfarbigen Vierecken mit unterschiedlichen geometrischen Formen
 - Wasserzeichen Bundespalast
 - Seiten 02 und 03: Text in 26 europäischen Sprachen

Zusätzlich wird die Formulierung zum Abgleich der Identifizierungsdokumente mit einer Datenbank (z.B. öffentliches Online-Register PRADO oder private Datenbanken mit gleichwertigem Inhalt) angepasst. Es wird klargestellt, dass nur dann ein Datenbankvergleich zwingend gefordert ist, wenn der Finanzintermediär mit dem vorgelegten Identifizierungsdokument nicht vertraut ist. Dies ist insbesondere dann der Fall, wenn gewisse Dokumente nur selten bzw. unregelmässig zur Identifizierung vorgelegt werden und betrifft insbesondere Ausweise ausländischer Staaten.

Fazit

Rz 14 wird dahingehend angepasst, dass die Anzahl der zu überprüfenden Sicherheitsmerkmale von drei auf zwei reduziert wird (ein optisch-variables und ein weiteres zufällig ausgewähltes Sicherheitsmerkmal).

Zusätzlich wird im Rundschreiben klargestellt, dass ein Abgleich mit einer Datenbank nur dann zwingend nötig ist, wenn der Finanzintermediär mit den vorgelegten Identifizierungsdokumenten nicht vertraut ist.

3.3.1.3 Abbruch des Identifizierungsvorgangs per Video (Rz 18–22)

Stellungnahmen zu Rz 21 der Anhörungsversion

Generell wird seitens der Anhörungsteilnehmer begrüsst, dass beim Hinweis auf erhöhte Risiken der Identifizierungsvorgang fortgeführt werden darf und eine Geschäftsbeziehung, unter Voraussetzung der Zustimmung einer vorgesetzten Person, eröffnet werden kann.

Einzelne Stellungnahmen haben zusätzlich angeregt, dass die Möglichkeit bestehen sollte, den Identifizierungsvorgang auch dann fortzuführen, wenn Zweifel zur Echtheit der Identifizierungsdokumente bestehen. Zudem haben einige Anhörungsteilnehmer den Begriff der erhöhten Risiken als unklar bezeichnet.

Würdigung

Der gesamte Prozess der Videoidentifizierung hat zum Ziel, die Identität einer Person zu erfassen. Insbesondere soll während des Videogesprächs bestätigt werden, dass die Person und die vorgelegten Identifizierungsdokumente übereinstimmen und letztere gültig und echt sind. Verbleiben trotz der Prüfungsvorgänge während des Gesprächs Zweifel an der Echtheit der Identifizierungsdokumente, darf die Kundenbeziehung nicht eröffnet werden. Ergänzend steht es dem Finanzintermediär jederzeit zu, den Kunden auf die Identifizierung via herkömmliche Kanäle (persönliche Vorsprache, Korrespondenzweg) zu verweisen.

Der Begriff „erhöhte Risiken“ bezieht sich wie bisher auf Art. 13 GwV-FINMA.

Fazit

Rz 21 der Anhörungsversion bleibt unverändert. Bei Zweifeln an der Echtheit des Identifizierungsdokuments darf der Identifizierungsvorgang nicht zur Eröffnung einer Geschäftsbeziehung verwendet werden.

3.4 Online-Identifizierung

3.4.1 Online-Identifizierung mittels elektronischer Ausweiskopie (Rz 31–44)

Stellungnahmen zu Rz 31.1 der Anhörungsversion

Die meisten Stellungnahmen kritisieren die Vorgabe, dass die Online-Identifizierung durch geschulte Mitarbeitende des Finanzintermediärs erfolgen muss und haben ausgeführt, dass durch diese Formulierung sowohl eine Automatisierung wie auch eine Delegation an einen spezialisierten Anbieter von Identifizierungsprozessen ausgeschlossen wird.

Würdigung

Bei geeigneten technologischen Hilfsmitteln soll eine Automatisierung möglich sein. Zudem soll die Formulierung eine Delegation nicht ausschliessen. Der letzte Satz zu Rz 31.1 wird zur Klarstellung gestrichen.

Fazit

Der Begriff „geschulte Mitarbeitende des Finanzintermediärs“ wird gestrichen, um eine Delegation und Automatisierung nicht auszuschliessen.

Stellungnahmen zu Rz 31.3 der Anhörungsversion

Die Vorgaben zu den für das Online-Identifizierungsverfahren zugelassenen Ausweisen sind für einige Anhörungsteilnehmer zu streng formuliert. Insbesondere die Forderung von optischen Sicherheitsmerkmalen bringe keinen Mehrwert und sei zu streichen.

Würdigung

Um Identifizierungsdokumente sicherer zu machen und Fälschungsversuche zu erschweren, definieren die jeweiligen Ausstellerländer von Identifizierungsdokumenten diverse Sicherheitsmerkmale, welche die Echtheit der Dokumente bescheinigen sollen. Zudem erleichtert der maschinenlesbare Bereich die Prüfung der Daten auf den Dokumenten. Auch auf diesem Gebiet entwickeln sich die technologischen Möglichkeiten weiter, weswegen Identifizierungsdokumente neueren Datums immer mehr unterschiedliche Sicherheitselemente verschiedener Kategorien aufweisen. Wie bereits ausgeführt, ist eine Identifizierung mit digitalen Hilfsmitteln anfälliger für Betrugs- und Fälschungsversuche. Die Überprüfung von Sicherheitselementen nimmt somit einen hohen Stellenwert ein. Auch wenn bei der Online-Identifizierung optisch-variable Merkmale nicht bestimmungsgemäss geprüft werden können, stellt die Anforderung des Vorhandenseins solcher Sicherheitsmerkmale (und auch der maschinenlesbaren Zone) ein gewisses Sicherheitsniveau dar, da fälschungsanfällige, ältere Identifizierungsdokumente beim digitalen Prozess ausgeschlossen werden.

Fazit

Die Anforderungen an die zugelassenen Identifizierungsdokumente bleiben unverändert.

3.4.1.1 Elektronische Ausweiskopie mit Echtheitsprüfung durch den Finanzintermediär (Rz 32–37)

Stellungnahmen zu Rz 32 der Anhörungsversion

Zahlreiche Anhörungsteilnehmer haben sich zu den zu überprüfenden drei optischen Sicherheitsmerkmalen und dem Datenbankabgleich geäußert und verweisen auf die Stellungnahmen zu Rz 14 des Rundschreibens betreffend Videoidentifizierung. Von einzelnen Teilnehmern wird bei der Online-Identifizierung zusätzlich kritisiert, dass die Vorgabe „soweit sich diese auf einem Standbild überprüfen lassen“ nicht klar verständlich sei und zu Rechtsunsicherheit führe.

Einige Stellungnahmen führen aus, dass eine Lebenderkennung nur risikobasiert zum Einsatz gelangen sollte, und vereinzelt wird ein kompletter Ver-

zucht auf eine Lebenderkennung gefordert. Andere Anhörungsteilnehmer begrüssen die Einführung einer Lebenderkennung. Verschiedentlich wurde darauf hingewiesen, dass die erklärenden Ausführungen im Erläuterungsbericht zur Lebenderkennung eine Diskrepanz zum Rundschreiben aufweisen. Im Rundschreiben sei eine Lebenderkennung als Beispiel aufgeführt („Selfie mit Lebenderkennung“), wohingegen im Erläuterungsbericht eine Lebenderkennung per se vorausgesetzt werde.

Würdigung

Bezüglich den Sicherheitsmerkmalen und dem Datenbankabgleich wird auf die Ausführungen zu Rz 14 bezüglich der Videoidentifizierung verwiesen. Auch bei der Online-Identifizierung sollen zwei Sicherheitsmerkmale überprüft werden. Diese brauchen nicht optisch-variabel zu sein, müssen jedoch beide zufällig ausgewählt werden. Die meisten Identifizierungsdokumente verfügen über eine genügende Anzahl von auf einem Standbild prüfbar Sicherheitsmerkmalen. Nebst den formalen Merkmalen (Layout, Orthographie und Schriftart) sind auch weitere Sicherheitsmerkmale erkennbar. Bei einer guten Kameraauflösung, wie sie mittlerweile alle gängigen Smartphones aufweisen, kann auf dem Lichtbild bspw. die Mikroschrift erkennbar sein (im Gegensatz zu einer reinen Kopie, wo sie nur als Strich erscheint und keine Buchstaben erkennbar sind). Beispiele zu den Sicherheitsmerkmalen sind unter Rz 14 aufgeführt. Auch ein Kinegram oder Movigram kann als Sicherheitsmerkmal zur Prüfung herangezogen werden. Der Kipp- bzw. Bewegungseffekt kann auf dem Standbild zwar nicht überprüft werden, allerdings sind Position, Grösse, Layout und Farbe kontrollierbar.

Bei der Online-Identifizierung zwingend ist die Sicherstellung, dass das Lichtbild der Vertragspartei im Rahmen des Identifizierungsprozesses erstellt wurde bzw. dass die Vertragspartei wirklich anwesend ist. Ziel dieser Vorgabe ist es, zum Zeitpunkt der Identifizierung bereits bestehende, veraltete oder von Drittpersonen stammende Lichtbilder zuverlässig auszuschliessen. Der Ausdruck Lebenderkennung bedeutet, dass durch geeignete Technologie oder anderweitige Verfahren überprüft wird, ob die Vertragspartei anwesend ist. Das Wort Lebenderkennung stellt dabei keine Definition eines bestimmten Verfahrens dar. Im Sinne der Technologieneutralität und prinzipienbasierten Regulierung ist es dem Finanzintermediär überlassen wie die Lebenderkennung umgesetzt werden soll. Damit Missverständnisse zur Definition von „Lebenderkennung“ vermieden werden, wird der Begriff „Selfie mit Lebenderkennung“ aus dem Rundschreiben gestrichen.

Fazit

Rz 32 wird dahingehend angepasst, dass die Anzahl der zu überprüfenden Sicherheitsmerkmale von drei auf zwei reduziert wird. Zudem ist ein Abgleich mit einer Datenbank nur dann zwingend nötig, wenn der Finanzintermediär mit den vorgelegten Identifizierungsdokumenten nicht vertraut ist.

Das Beispiel betreffend „Selfie mit Lebenderkennung“ wird aus dem Rundschreiben gestrichen. Die Anforderung, eine Lebenderkennung vorzunehmen, bleibt jedoch bestehen. Diese kann technologieneutral umgesetzt werden und es wird kein bestimmtes Verfahren vorgeschrieben.

Stellungnahmen zu Rz 33 der Anhörungsversion

Die meisten Anhörungsteilnehmer begrüßen die Ausweitung der Vorgabe zur erlaubten Banküberweisung für die Identifizierung, falls gewisse Voraussetzungen erfüllt sind, auf die Mitgliedsländer der FATF.

Insbesondere die Banken und Selbstregulierungsorganisationen würden gemäss Stellungnahmen jedoch eine noch weitergehende Öffnung begrüßen und fordern teilweise eine komplette Streichung der Vorgabe einer Banküberweisung bei der Online-Identifizierung. Ebenfalls monieren sie, dass das FATF-Kriterium zu kompliziert zur Umsetzung sei. Weitere Empfehlungen zielen darauf ab, die Formulierung möglichst offen zu lassen und auf eine angemessene prudentielle Aufsicht zu verweisen. Vereinzelt wird auch vorgeschlagen, den Kreis der Institute für eine Überweisung zur Identifizierungsbestätigung auf nicht-Banken auszuweiten und bspw. auch eine Überweisung von einem Digital Payment Service Provider oder einer Kreditkarte zuzulassen.

Drei Stellungnahmen formulieren spezifische Anliegen für ICOs. Die Vorschläge zielen darauf ab, für Token-Zeichnungen unter einem bestimmten Schwellenwert Erleichterungen vorzusehen und alternativ zur Banküberweisung auch eine Wallet-Prüfung zu zulassen.

Würdigung

Der Identifizierungsprozess über digitale Kanäle birgt ein nicht zu unterschätzendes Betrugs- und Fälschungsrisiko. Eine Identifizierung, bei welcher gar kein unmittelbarer persönlicher Kontakt und auch kein Videogespräch stattfindet, ist durch zusätzliche Abklärungen sicherzustellen. Bei Banken in der Schweiz, Liechtenstein oder einem FATF Staat, welcher die Vorgaben gemäss Rz 33 erfüllt, ist sichergestellt, dass bereits eine Identifizierung nach ausreichenden Normen vorgenommen wurde. Insofern ist eine Banküberweisung ein geeignetes Hilfsmittel zur Erhöhung der Sicherheit bei der Online-Identifizierung. Die Ergebnisse der FATF-Länderprüfungen sind auf der FATF-Internetseite verfügbar¹.

Sollte ein Kunde über kein Bankkonto in einem der FATF-Länder, welche die Voraussetzungen erfüllen, verfügen, kann die Videoidentifizierung oder eine traditionelle Form der Identifizierung gewählt werden.

¹ <http://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html>.

Betreffend ICOs ist darauf hinzuweisen, dass keine Sonderregelungen vonnöten sind. Da ICOs von Zahlungstoken als Herausgabe von Zahlungsmitteln dem GwG unterliegen, gilt gemäss Praxis der FINMA analog Art. 12 Abs. 2 Bst. d GwV-FINMA bis zum Schwellenwert von Fr. 3'000, anstelle der generellen Identifizierungspflicht ab Fr. 0.-, eine erleichterte Identifizierungspflicht mittels einfacher Kopie des Ausweises.

Fazit

Das Erfordernis einer Banküberweisung aus der Schweiz, Liechtenstein oder einem FATF Staat, welcher die Vorgaben gemäss Rz 33 erfüllt, wird beibehalten.

Stellungnahmen zu Rz 34–37 der Anhörungsversion

Bei der Überprüfung der Wohnsitzadresse hat ein Anhörungsteilnehmer angeregt, auch weitere Dokumente von offiziellen Stellen zur Bestätigung zuzulassen. Bspw. sollen auch Steuer- und Gebührenrechnungen zur Identifizierung herangezogen werden können.

Würdigung

Den gleichen Zweck wie eine Utility-Bill können auch Steuer- und anderweitige behördliche Rechnungen erfüllen.

Fazit

Rz 35 wird um „Steuer- und anderweitige behördliche Rechnungen“ ergänzt.

3.4.1.2 Elektronische Ausweiskopie mit qualifizierter elektronischer Signatur (Rz 38–39)

Stellungnahmen zu Rz 39 der Anhörungsversion

Einige Stellungnahmen führen aus, dass beim Vorhandensein einer qualifizierten elektronischen Signatur bereits einmal eine gesetzeskonforme Identifizierung stattgefunden habe. Die Erfordernisse einer Banküberweisung und einer Wohnsitzbestätigung seien überflüssig.

Würdigung

Eine qualifizierte elektronische Signatur gemäss dem Bundesgesetz über die elektronische Signatur (ZertES, SR 943.03) bzw. eine qualifizierte elektronische Signatur, welche von der Schweizerischen Anerkennungsstelle anerkannt wurde, sichert einen hohen Identifizierungsstandard. Somit ist die Vorgabe einer Banküberweisung und einer Wohnsitzbestätigung obsolet.

Fazit

Die Vorgabe einer Banküberweisung und einer Wohnsitzbestätigung wird bei Rz 39 gestrichen.

4 Weiteres Vorgehen

Die Änderungen des FINMA-RS 16/7 „Video- und Online-Identifizierung“ treten per sofort in Kraft. Den betroffenen Finanzintermediären wird eine Übergangsfrist bis am 1. Januar 2020 für die Prozessanpassungen gewährt.

Die FINMA wird die technologischen Entwicklungen bezüglich Video- und Online-Identifizierung weiterverfolgen und bei Bedarf das Rundschreiben erneut anpassen.