Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Rundschreiben 2016/7 „Video- und Online-Identifizierung“ – Teilrevision

Bericht über die Ergebnisse der Anhörung vom 16. November 2020 bis 1. Februar 2021

6. Mai 2021

Laupenstrasse 27, 3003 Bern, Tel. +41 (0)31 327 91 00, www.finma.ch

Inhaltsverzeichnis

Kernpunkte **3**

Abkürzungsverzeichnis **4**

1 Einleitung **5**

2 Eingegangene Stellungnahmen **5**

3 Ergebnisse der Anhörung und Beurteilung durch die FINMA **6**

3.1 Video-Identifizierung generell (Rz 5–28) 6

3.2 Online-Identifizierung (Rz 29–44) 7

3.2.1 Online-Identifizierung mittels elektronischer Ausweiskopie (Rz 31–44) 7

3.3 Erklärung über die wirtschaftliche Berechtigung (Rz 45–50) 12

3.4 Beizug Dritter (Rz 51) inkl. zugehörige Ausführung in Rz 53 13

3.5 Weitere Anliegen 14

3.5.1 Begriff des Vertragspartners 14

3.5.2 Identifizierung von juristischen Personen 14

3.5.3 Qualifizierte elektronische Signatur 15

4 Auswirkungen **16**

5 Weiteres Vorgehen **16**

Kernpunkte

1. Vom 16. November 2020 bis 1. Februar 2021 wurde zum teilrevidierten Rundschreiben 2016/7 „Video- und Online-Identifizierung“ eine öffentliche Anhörung durchgeführt.

2. Das Auslesen des Chips der biometrischen Identifizierungsdokumente wird allgemein begrüsst.

3. Einige Anhörungsteilnehmende schlagen bei der Online-Identifizierung weitere Alternativen vor, bei denen auf ergänzende Sicherheitsmassnahmen wie eine Banküberweisung oder das neue Chipauslesen verzichtet werden könnte. Häufig genannt wird eine asynchrone Verifikation bei der eine Videoaufnahme ohne live-Gespräch erfolgt und eine Software die erforderlichen Identifizierungsprüfungen durchführt. Im Nachgang soll dann eine Prüfung durch einen Mitarbeitenden erfolgen. Dieses Verfahren ist jedoch nicht mit einem direkten Gespräch mit einem Menschen vergleichbar, bei dem psychologische Elemente berücksichtigt werden können und weist ein zu tiefes Sicherheitsniveau auf.

4. Um die Online-Identifizierung weiter automatisieren zu können, fordern mehrere Stellungnahmen, dass eine Geolokalisierung zur Überprüfung der Wohnsitzadresse der Vertragspartei zugelassen wird. Dieser Vorschlag wird umgesetzt. Das Fälschungsrisiko wird im Vergleich zu fotografierten oder hochgeladenen *Utility Bills* als nicht höher qualifiziert.

5. Ferner wurden zwei Präzisierungen umgesetzt: Der Begriff „Vertragspartei“ umfasst neu auch mündige Drittpersonen, die für Minderjährige eine Kundenbeziehung eröffnen. Schliesslich wird auch eine Überweisung einer nach Art. 1*b* BankG bewilligten Person zugelassen.

Abkürzungsverzeichnis

BankG	Bundesgesetz über die Banken und Sparkassen vom 8. November 1934 (SR 952.0)
DUFI	der FINMA direkt unterstellte Finanzintermediäre
FINIG	Finanzinstitutsgesetz vom 15. Juni 2018 (SR 954.1)
FINMAG	Finanzmarktaufsichtsgesetz vom 22. Juni 2007 (SR 956.1)
GwG	Geldwäschereigesetz vom 10. Oktober 1997 (SR 955.0)
GwV	Geldwäschereiverordnung vom 11. November 2015 (SR 955.01)
GwV-FINMA	Geldwäschereiverordnung-FINMA vom 3. Juni 2015 (SR 955.033.0)
IBAN	*International Bank Account Number*. Standardisierte Internationale Bankkontonummer
MRZ	*Machine Readable Zone*. Sichtbarer Teil eines Ausweisdokumentes, der speziell dafür ausgelegt wurde, durch optische Texterkennung gelesen zu werden
NFC	*Near Field Communication.* Übertragungsstandard zum kontaktlosen Austausch von Daten
VIZ	*Visual Inspection Zone.* Hier sind die Personendaten des Inhabers sowie ein Passfoto abgebildet
VZertES	Verordnung vom 23. November 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (SR 943.032)
WB	an den Vermögen wirtschaftlich berechtigte Person
ZertES	Bundesgesetz vom 18. März 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (SR 943.03)

1 Einleitung

Vom 16. November 2020 bis 2. Februar 2021 führte die FINMA eine öffentliche Anhörung zum Änderungsentwurf des Rundschreibens 2016/7 „Video- und Online-Identifizierung“ durch.

Zielsetzung dieses Rundschreibens ist es einerseits, die Sorgfaltspflichten nach GwG und seiner Ausführungsbestimmungen (GwV-FINMA, VSB 20, Reglement SRO-SVV) hinsichtlich eines digitalen Umfelds auszulegen, insbesondere betreffend die Aufnahme von Geschäftsbeziehungen über elektronische Kanäle.[1] Andererseits soll die Auslegung der massgeblichen Bestimmungen der GwV-FINMA im digitalen Kontext konkretisiert werden.

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

2 Eingegangene Stellungnahmen

Folgende Personen und Institutionen haben an der Anhörung teilgenommen und der FINMA eine Stellungnahme eingereicht (in alphabetischer Reihenfolge):

- AsyLex
- Baloise Bank SoBa
- EXPERTsuisse
- fidentity GmbH
- PXL Vision AG
- Raiffeisen Schweiz
- ROCKON Digital Evolution AG
- SBVg – Schweizerische Bankiervereinigung
- SRO – SVV
- SFTI – Swiss Fintech Innovations
- SwissSign Group
- Ticino Blockchain Technologies Association
- ubitec AG
- YAPEAL AG

[1] Die nachfolgenden Verweise auf die GwV-FINMA beziehen sich auch (ohne explizite Erwähnung) auf die analogen Bestimmungen der VSB und des Reglements der SRO-SVV.

3 Ergebnisse der Anhörung und Beurteilung durch die FINMA

Im vorliegenden Bericht werden die eingegangenen Stellungnahmen von der FINMA zusammengefasst, gewichtet und ausgewertet.

Der Bericht wurde vom Verwaltungsrat der FINMA verabschiedet (Art. 11 Abs. 4 Verordnung zum Finanzmarktaufsichtsgesetz). Er wird zusammen mit den verabschiedeten Regulierungen und den Stellungnahmen der Anhörung veröffentlicht. Ausserdem veröffentlicht die FINMA sog. Erläuterungen. Diese basieren auf dem Erläuterungsbericht der Anhörung, in dem ergänzend auch die Anpassungen nach der Anhörung abgebildet sind. Das soll den Rechtsanwendern als benutzerfreundliches Begleitdokument zur finalen Vorlage dienen.

Die Ergebnisse der Anhörung und die Beurteilung durch die FINMA werden nachfolgend nach Themenblöcken gegliedert dargestellt. Die Abfolge der Themenblöcke entspricht der Reihenfolge der Randziffern des Rundschreibens. Themen, die sich nicht direkt auf einzelne Randziffern oder das Rundschreiben beziehen, sind am Ende des Kapitels aufgeführt.

3.1 Video-Identifizierung generell (Rz 5–28)

Stellungnahmen

Die Video-Identifizierung ist nicht Gegenstand der vorliegenden Teilrevision. Gleichwohl sind Eingaben eingereicht worden, die sich auf dieses Verfahren beziehen. Insbesondere geht es um die Forderung, die Video-Identifizierung ohne menschliche Interaktion vornehmen zu können.

Diesbezüglich wurde von einzelnen Anhörungsteilnehmenden der Vorschlag eingebracht, die Identifizierung durch eine Software mittels Videoaufzeichnung durchzuführen und ergänzend im Nachgang eine Verifikation durch geschulte Mitarbeitende (asynchrone Verifikation) vorzunehmen. Die meisten Stellungnahmen wollen dabei stichprobeweise vorgehen bzw. schlagen eine Verifikation durch geschulte Mitarbeitende nur bei Unstimmigkeiten oder Betrugsverdacht vor.

Würdigung

Wie bereits im Erläuterungsbericht zur öffentlichen Anhörung ausgeführt[2], sind Identifizierungsverfahren ohne unmittelbare menschliche Interaktion der

[2] https://www.finma.ch/de/dokumentation/archiv/abgeschlossene-anhoerungen/2020/ Direkter Link: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/anhoerungen/laufende-anhoerungen/20201116-video-und-online-identifizierung/eb_rs16_07_20201116.pdf?la=de.

Online-Identifizierung zuzuordnen. D.h. auch wenn entsprechende Videoaufnahmen erfolgen, liegt trotzdem eine Online-Identifizierung im Sinne des Rundschreibens vor. Ein vollautomatisiertes Verfahren wie vorliegend vorgeschlagen, kann umgesetzt werden, falls die flankierenden Sicherheitsmassnahmen gemäss Rz 33 f. vorgesehen werden.

Da auch bei der Online-Identifizierung das mögliche Verfahren mittels asynchroner Verifikation angesprochen wird, erfolgt die Würdigung der Vorschläge im Kapitel 3.2.1.

Fazit

Die Video-Identifizierung ist der persönlichen Vorsprache gleichgestellt und bedingt eine unmittelbare menschliche Interaktion. Automatisierte Identifizierungsverfahren sind der Online-Identifizierung zuzuordnen.

3.2 Online-Identifizierung (Rz 29–44)

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

Stellungnahme zu Rz 32 (Auslesen MRZ)

Ein Anhörungsteilnehmender hat ausgeführt, dass die Vorgabe die MRZ auszulesen zu streng und nicht mehr zeitgemäss sei und die Eröffnung von Geschäftsbeziehungen erschweren würde. Identifizierungsdokumente könnten optisch auch durch andere Verfahren ausgelesen werden.

Würdigung

Das Erfordernis, die MZR auszulesen, stellt eine zusätzliche Sicherheitsmassnahme dar. Auch wenn die Zusammenstellung der MRZ leicht nachvollzogen werden kann, können die darin festgehaltenen Informationen einerseits auf innere Widersprüche geprüft werden und somit Hinweise auf Fälschungen liefern, und andererseits einen Abgleich mit den Angaben zulassen, welche die Vertragspartei über sich im Eröffnungsprozess gemacht hat. Zudem ist das Auslesen der MRZ gut automatisierbar und stellt ein mittlerweile gängiges Verfahren dar, das leicht im Identifizierungsprozess integriert werden kann.

Fazit

Am Erfordernis, die MRZ im Rahmen des Identifizierungsvorgangs mit geeigneten technischen Hilfsmitteln auszulesen, wird festgehalten.

Stellungnahmen zu Rz 33 (Banküberweisung)

Mehrere Anhörungsteilnehmende haben sich zum Erfordernis der Banküberweisung geäussert und ausgeführt, dass diese im Identifizierungsprozess häufig Probleme verursache und nicht praktikabel sei. Es komme häufig zu Abbrüchen im Identifizierungsprozess, weil der Zahlungseingang von einem Konto stamme, das nicht dem Vertragspartner zugeordnet werden könne (z.B. bei Überweisungen von den Eltern für die Kontoeröffnung des Kindes oder bei Lohneingängen vom Arbeitgeber). Auch seien die IT-Systeme oftmals nicht in der Lage, die Zahlungseingänge zu melden bzw. weiterzuverarbeiten um den Identifizierungsprozess automatisiert abschliessen zu können. Erwähnt wurde ebenfalls, dass eine Banküberweisung für gewisse Kunden zu komplex sei und diese deshalb den Vorgang abbrächen. Zusätzlich erschwere das zeitliche Auseinanderliegen von Identifizierung, Überweisung und der Aufnahme der Geschäftsbeziehung den Prozess. Herausfordernd sei auch, dass für die Banküberweisung dem Kunden eine Konto- bzw. IBAN-Nummer bekannt gegeben werden müsse, bevor die Identifizierung vollständig sei. Allfällige Eingänge von Vermögenswerten könnten dann nicht mehr ohne Weiteres gestoppt werden.

Eine Stellungnahme fordert, gänzlich auf die Banküberweisung und auch auf alternative Sicherheitsverfahren (vorliegend Chipauslesen Rz 33.1 gemeint) bei der Online-Identifizierung zu verzichten, da die Vorgaben aus Rz 32 in Verbindung mit der Überprüfung der Wohnsitzadresse (Rz 34–37) für eine sichere Identifizierung ausreichten.

In Bezug auf die neuen Fintech-Geschäftsmodelle wurde von einer Partei eingebracht, dass Unternehmen, die ausschliesslich in Kryptowährungen aktiv seien, die Banküberweisung als alternative Identifizierungsmöglichkeit nicht nutzen könnten. Es solle zusätzlich erlaubt werden, anstelle einer Banküberweisung eine Wallet-Identifizierung zuzulassen.

Ferner wurde gefordert, dass auch eine Überweisung von einem nach Art. 1*b* BankG bewilligten Institut als „Banküberweisung“ zur Identifizierung zugelassen werden solle.

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 unmittelbares 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 mit ausreichendem Standard vorgenommen wurde. Insofern stellt eine Banküberweisung eine geeignete flankierende Sicherheitsanforderung bei der Online-Identifizierung dar. Zudem muss den Kunden noch

keine IBAN angegeben werden, die sich auf ihr eigenes Konto bezieht. Eine Kleinstüberweisung an den Finanzintermediär ist ausreichend. Es steht letzterem auch frei, sich mit der Überweisung gleichzeitig und je nach Ausgestaltung des jeweiligen Vertrages, auch eine anderweitig erbrachte oder zu erbringende Dienstleistung vergüten zu lassen.

Ein gänzlicher Verzicht auf die Banküberweisung, ohne weitere flankierende Sicherheitsmassnahmen (wie neu dem Auslesen des Chips der biometrischen Identifizierungsdokumente) würde die Sicherheit der Online-Identifizierung empfindlich reduzieren und das Betrugsrisiko erhöhen. Die Identifizierung einer Krypto-Wallet als alternative Sicherheitsmassnahme ist aus Sicherheitsüberlegungen abzulehnen. Wallet-Betreiber unterstehen keiner gleichwertigen Aufsicht wie bewilligte Bankinstitute. Zur Klarstellung sei erwähnt, dass Überweisungen von Banken mit Fokus auf Geschäftsmodelle im Fintechbereich („Kryptobanken“) zulässig sind. Dies umfasst auch gemäss Art. 1*b* BankG bewilligte Institute, was im Rundschreiben entsprechend klargestellt wird.

Fazit

Am Erfordernis flankierender Sicherheitsanforderungen bei der Online-Identifizierung, wie einer Banküberweisung oder neu dem Auslesen des Chips der biometrischen Identifizierungsdokumente, wird festgehalten. Den Forderungen der Anhörungsteilnehmenden wird insofern entsprochen, als dass neu bei Rz 33 eine Überweisung eines nach Art. 1*b* BankG bewilligten Instituts explizit erwähnt wird (Fussnote).

Stellungnahmen zu Rz 33.1 (Chipauslesen)

Die neue Identifizierungsalternative durch Auslesen des Chips der biometrischen Identifizierungsdokumente wird allgemein begrüsst. Allerdings führten zahlreiche Anhörungsteilnehmende aus, dass nur wenige Identifizierungsdokumente bereits über einen biometrischen Chip verfügten. Bspw. habe die in der Schweiz sehr verbreitete Identitätskarte keinen Chip. Besonders im Retailsegment sei diese aber beliebt. Zudem verfüge nicht jedermann über einen Reisepass mit Chip und ein NFC fähiges Mobilgerät der neueren Generation. Dadurch sei der Einsatz dieser neuen Identifizierungsvariante eingeschränkt. Auch sei das Auslesen des Chips wenig benutzerfreundlich und fehleranfällig.

Da das Auslesen des Chips für die breite Masse noch keine Automatisierung des digitalen Eröffnungsprozesses gestatte, haben einige Anhörungsteilnehmende die Implementation weiterer Identifizierungsalternativen, bei denen auf die Banküberweisung verzichtet werden könne, gefordert. So ermögliche die Kombination von verschiedenen Technologien wie bspw. Videosequenzen in Echtzeit, Gesichtserkennung, Lebenderkennung (*Liveness Detection* – allf. mit *Challenge Response* Elementen angereichert) und dem Auslesen

der VIZ und MRZ der Ausweisdokumente eine sichere Online-Identifizierung ohne unnötigen Unterbruch des Prozesses. Andere Anhörungsteilnehmende schlagen zudem vor, eine nachgelagerte (asynchrone) Verifikation durch geschulte Mitarbeitende als Sicherheitselement zuzulassen, um auf eine flankierende Banküberweisung verzichten zu können. Diesbezüglich variieren die Vorschläge von stichprobeweisen bzw. anlassbezogenen Kontrollen (z.B. wenn die Angaben des Vertragspartners nicht mit der MRZ übereinstimmen, die Lichtverhältnisse zu schlecht sind, bei Betrugsverdacht usw.) bis zu einer flächendeckenden nachgelagerten asynchronen Verifikation. Auch sei mittlerweile möglich, beim Einsatz von Videosequenzen mit einer Software Hologramme, Kippbilder und weitere optisch variable Sicherheitselemente der Identifizierungsdokumente zu prüfen. Ein Anhörungsteilnehmender schlug vor, den ganzen Identifizierungsprozess risikoorientiert umzusetzen (analog den vereinfachten Sorgfaltspflichten in Art. 12 GwV-FINMA) und je nach Risiko der gewünschten Geschäftsbeziehung andere bzw. umfassendere Sicherheitsmassnahmen vorzugeben. Sollte sich das Risikoprofil der Geschäftsbeziehung ändern, könne die Identifizierung dem Risiko konform wiederholt oder ergänzt werden.

Spezifisch zur Identifizierungsalternative des Chipauslesens forderten zwei Anhörungsteilnehmende, auf die Prüfung der Authentizität und Integrität der Daten zu verzichten. Die Prüfung der staatlichen Zertifikate erschwere den Prozess zusätzlich. Zudem solle das Rundschreiben die auszulesenden Daten auflisten, da sich diese je nach Land unterschieden.

Weiter wurde moniert, dass auch die neuen N und F Ausweise, die ab Mitte 2021 im Kreditkartenformat ausgegeben würden, keinen Chip hätten, was im Asylbereich den Zugang zur digitalen Eröffnung einer Bankbeziehung behindere, da betroffene Personen auch keine Banküberweisung zu Identifizierungszwecken tätigen könnten.

Würdigung

Eine asynchrone Verifikation, wie von Anhörungsteilnehmenden vorgeschlagen, gilt im Sinne des vorliegenden Rundschreibens als Online- und nicht als Video-Identifizierung. Dabei spielt es keine Rolle, ob das Identifizierungsverfahren auf Videotechnologie beruht oder ob mit Fotos gearbeitet wird. Eine Video-Identifizierung würde eine unmittelbare menschliche Interaktion bzw. ein Live-Gespräch bedingen, weil diese der persönlichen Vorsprache entspricht. Beim direkten Kontakt dienen psychologische Elemente als Sicherheitsmechanismen. Zudem ist die Hürde für Betrugsversuche aufgrund der direkten Interaktion in einem live-Gespräch höher. Wie bei den Stellungnahmen zu Rz 33 (Banküberweisung) bereits ausgeführt, sind zur Sicherstellung der Online-Identifizierung aufgrund des fehlenden analogen Kontakts zusätzliche Sicherheitsmassnahmen notwendig. Dies ist entweder eine Banküberweisung oder neu das Auslesen des Chips der biometrischen Identifizierungsdokumente. Eine asynchrone Verifikation bietet hingegen kein

vergleichbares Sicherheitsniveau. Das Anliegen einer unterbruchsfreien, automatisierten und sicheren Identifizierung ist bei der Online-Identifizierung gewährleistet.

Auf die Daten, welche durch das Chipauslesen für den Identifizierungsprozess verwendet werden sollen, wird im Erläuterungsbericht zur öffentlichen Anhörung eingegangen:[3] Es handelt sich um Daten, die unmittelbar für den Identifizierungsprozess benötigt werden (z.B. allgemeine Ausweisdaten inkl. MRZ und Gesichtsbild). Das Auslesen von speziell schützenswerten Daten, namentlich den Fingerabdrücken, ist Behörden vorbehalten.

Da die neuen N und F Ausweise keinen biometrischen Chip aufweisen werden, können diese ohne ergänzende Banküberweisung nicht für die digitale Eröffnung einer Kundenbeziehung verwendet werden. Die Identifizierung kann mit einem N oder F Ausweis aber weiterhin auf anderem Weg erfolgen.

Fazit

Am Auslesen des Chips der biometrischen Identifizierungsdokumente wird als alternative Sicherheitsmassnahme festgehalten. Zusätzliche weitere Alternativen werden nicht vorgesehen.

Stellungnahmen zu Rz 34–37 (Überprüfung Wohnsitzadresse)

Einige Anhörungsteilnehmende argumentierten, dass die Wohnsitzprüfung mittels *Utility Bill* nicht mehr zeitgemäss sei. Insbesondere sei die Echtheit einer hochgeladenen oder kopierten/fotografierten *Utility Bill* kaum überprüfbar. Gewünscht wird das Zulassen der Geolokalisierung (Prozess zur Ermittlung des Standorts eines Computers oder Mobilgerätes) für die Prüfung des Wohnsitzes.

Ferner hat eine Eingabe verlangt, auch Gasrechnungen ergänzend zu Stromrechnungen als *Utility Bill* für eine Wohnsitzprüfung zu erlauben.

Würdigung

Eine Geolokalisierung als Überprüfungsmechanismus der Wohnsitzadresse zu verwenden, scheint zeitgemäss und im digitalen Kontext vertretbar. Das Fälschungsrisiko dürfte im Vergleich zu Fotokopien bzw. fotografierten/hochgeladenen *Utility Bills* nicht erhöht sein. Zudem fördert die Geolokalisierung einen unterbruchsfreien Identifizierungsvorgang.

[3] https://www.finma.ch/de/dokumentation/archiv/abgeschlossene-anhoerungen/2020/ Direkter Link: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/anhoerungen/laufende-anhoerungen/20201116-video-und-online-identifizierung/eb_rs16_07_20201116.pdf?la=de.

Der guten Ordnung halber wird festgehalten, dass Rz 35 erlaubt, die Wohnsitzprüfung anhand einer Energie- Wasser- oder Telefonrechnung vorzunehmen. Gasrechnungen sind dabei ebenfalls erfasst.

Fazit

Die Geolokalisierung zur Überprüfung der Wohnsitzadresse wird neu zugelassen und als Rz 37.1 im Rundschreiben eingefügt.

3.3 Erklärung über die wirtschaftliche Berechtigung (Rz 45–50)

Stellungnahme

Ein Teilnehmender hat ausgeführt, dass die Einholung der Erklärung des wirtschaftlich Berechtigten (WB) für die Online-Identifizierung hinderlich sei. Art. 59 Abs. 4 der GwV-FINMA verlange eine Dokumentation, dass keine Zweifel bestehen, dass der WB mit dem Vertragspartner übereinstimme. Für das digitale Äquivalent verlange das Rundschreiben entweder eine qualifizierte Signatur, TAN oder elektronische Übermittlung eines physisch unterzeichneten Formulars. Einfacher wäre es jedoch, wenn während des Identifizierungsprozesses eine Bestätigung des WB mittels Anwählen eines Formularfeldes (*check the box*) erfolgen könnte.

Würdigung

Rz 48 erlaubt anstelle einer TAN auch eine ähnliche Methode, sofern sie eine verlässliche Zuordnung zur Vertragspartei ermöglicht. Sind somit während der Online-Identifizierung keine Unstimmigkeiten hervorgetreten und es sind keine Zweifel an der Übereinstimmung von WB und Vertragspartei entstanden, reicht das Anwählen eines Feldes durch die Vertragspartei (*check the box*) noch während der Online-Identifizierung für die Bestätigung aus. Allerdings muss der Finanzintermediär, auch wenn er keine Zweifel hat, dass die Vertragspartei auch die an den Vermögenswerten wirtschaftlich berechtigte Person ist, dies nach Art. 59 Abs. 4 GwV-FINMA in geeigneter Form dokumentieren.

Für den Fall einer nachgelagerten Bestätigung, bspw. via Link auf ein Formular, muss diese dem Vertragspartner wieder einwandfrei zugeordnet werden können. Dies erfolgt zum Beispiel, indem ein entsprechendes Formular nach dem Einloggen im Online-Banking ausgefüllt wird. Alternativen sind auch die qualifizierte elektronische Signatur auf der Bestätigung (Rz 47), die Einholung einer TAN (Rz 48) oder die Zustellung einer Kopie eines physisch unterzeichneten Formulars (Rz 49).

Fazit

Am Rundschreiben erfolgt keine Änderung. Die Bestätigung des WB ist direkt während der Online-Identifizierung bereits umsetzbar.

3.4 Beizug Dritter (Rz 51) inkl. zugehörige Ausführung in Rz 53

Stellungnahmen

Zwei Stellungnahmen beschäftigten sich mit einem Widerspruch zwischen dem Rundschreiben und der VSB 20. Art. 43 Abs. 3 der VSB 20 schliesse eine Weiterdelegation sowie eine Korrespondenzeröffnung durch den Beauftragten aus. Im Gegensatz hierzu erlaube Rz 51 des Rundschreibens explizit einen Beizug Dritter im Rahmen der Online-Identifizierung, welche einer Eröffnung auf dem Korrespondenzweg gleichgestellt sei. Die Stellungnahmen fordern eine Klarstellung, dass trotz Einschränkung in der VSB eine Weiterdelegation auch bei einer Online-Identifizierung erfolgen könne.

Eine weitere Eingabe wünschte, die Präzisierung in der Tabelle zur Technologieneutralität offener zu formulieren und es auch beigezogenen Technologiespezialisten zu ermöglichen, ihrerseits Dritte beizuziehen.

Würdigung

Eine Übertragung technischer Identifizierungsprozesse oder –teilprozesse bei der Video- oder Online-Identifizierung durch einen Finanzintermediär an einen technischen Anbieter stellt keine Weiterdelegation der Sorgfaltspflichten dar. Das in Art. 43 Abs. 3 VSB 20 festgeschriebene Verbot einer Korrespondenzeröffnung durch beauftragte Finanzintermediäre sollte längerfristig im Rahmen einer VSB Revision adressiert werden.

Die vorgeschlagene Präzisierung zum Beizug Dritter in der Tabelle zur Technologieneutralität soll explizit nur für die Delegation an einen Finanzintermediär gelten, wenn dieser beispielsweise einen Technologieanbieter beizieht. Eine generell mehrstufige Delegation ist nicht vorgesehen.

Fazit

Keine Anpassung im Rundschreiben.

3.5 Weitere Anliegen

3.5.1 Begriff des Vertragspartners

Stellungnahmen

Im Rahmen der Anhörung wurde durch zwei Stellungnahmen eingebracht, dass durch die Verwendung des Begriffs des Vertragspartners die Anwendbarkeit des Rundschreibens eingeschränkt werde. Es seien Konstellationen möglich, wo die Eröffnung der Geschäftsbeziehung nicht durch den Vertragspartner erfolge. So bspw. bei Minderjährigen (Eröffnung durch mündige Drittpersonen) oder bei Kapitaleinzahlungskonten. In diesen Fällen sei die Anwendung des Rundschreibens und damit eine digitale Kundeneröffnung nicht möglich.

Würdigung

Das Rundschreiben soll breit anwendbar sein. Die Sonderformen der Identifizierung gemäss VSB 20 sollen mitberücksichtigt werden.

Fazit

Im Rundschreiben wird eine präzisierende Fussnote eingefügt. Der Begriff Vertragspartei soll auch mündige Drittpersonen, die für Minderjährige eine Kundenbeziehung eröffnen, mitumfassen.

3.5.2 Identifizierung von juristischen Personen

Stellungnahmen

Eine Eingabe hat ausgeführt, dass zur Identifizierung von juristischen Personen erlaubt sein sollte, einen elektronischen Handelsregisterauszug (vom Handelsregisteramt oder einem anerkannten Dienstleister wie www.Moneyouse.ch) als gleichwertige Alternative zu einem notariell beglaubigten physischen (papierbasierten) Handelsregisterauszug zu verwenden.

Würdigung

Das Rundschreiben weist in Bezug zu juristischen Personen oder Personengesellschaften in Rz 24 darauf hin, dass bei der Video-Identifizierung ein Auszug in elektronischer Form aus einer durch die zuständige Registerbehörde geführten Datenbank oder aus einem vertrauenswürdigen, privat verwalteten Verzeichnisses eingeholt werden kann. Diese Bestimmung gilt analog auch für die Online-Identifizierung (Rz 44).

Fazit

Die Einholung von Handelsregisterauszügen in elektronischer Form ist sowohl bei der Video- wie auch Online-Identifizierung bereits vorgesehen.

3.5.3 Qualifizierte elektronische Signatur

Stellungnahmen

Es sind bei der Anhörung auch Stellungnahmen im Zusammenhang mit der qualifizierten elektronischen Signatur und den zugehörigen Prozessen und Gesetzen (ZertES und VZertES) eingegangen. Es wurde dargelegt, dass derzeit noch eine Pflicht zur persönlichen Vorsprache zwecks Identifikation verlangt werde. Insbesondere, wenn ein digitales Zertifikat, z.B. eine qualifizierte elektronische Signatur, verwendet werden möchte. Dies sei nur mit der Video-Identifizierung umsetzbar, da diese der persönlichen Vorsprache gleichgestellt sei und schliesse eine Online-Identifizierung für die Verwendung eines Zertifikats aus. Aktuell gehe die Entwicklung in der EU aber Richtung der Zulassung von automatisierten Identifikationen, was dann allenfalls auch im ZertES und VZertES übernommen würde. Die FINMA solle diese Entwicklungen im GwG Bereich mittragen.

Eine Eingabe hat gefordert, dass die FINMA mit dem BAKOM zusammenarbeiten solle damit im ZertES zukünftig auch die weiteren von der FINMA zugelassenen Identifizierungsverfahren für die Ausstellung von Zertifikaten verwendet werden können.

Würdigung

Gemäss Art. 7 VZertES können Zertifikate im Rahmen eines Verfahrens zur Personenidentifikation mittels audiovisueller Kommunikation in Echtzeit ausgestellt werden, falls das Verfahren den Anforderungen des Geldwäschereigesetzes entspricht. Die so ausgestellten Zertifikate dürfen nur im Rahmen der Beziehungen zwischen deren Inhaberinnen und Inhabern und den Finanzintermediären, die ihre Identität überprüft haben, verwendet werden. Hierdurch können im Rahmen der digitalen Eröffnung der Kundenbeziehung auch Verträge unterschrieben werden, die der Schriftlichkeit verlangen (bspw. Verträge im Rahmen des Konsumkreditgesetzes).

Generell sei aber hinsichtlich der qualifizierten elektronischen Signatur darauf hingewiesen, dass die Vorgaben für die qualifizierte elektronische Signatur und deren Anerkennung im ZertES und der zugehörigen VZertES geregelt sind und nicht in der Kompetenz der FINMA liegen.

Technologische und prozessuale Entwicklungen zu Identifizierungsverfahren werden nah verfolgt (international und national), analysiert und gegebenenfalls in den Regularien der FINMA adressiert.

Fazit

Das Rundschreiben wird weiterhin zeitnah den technologischen Entwicklungen angepasst werden.

4 Auswirkungen

Die vorliegende Teilrevision bietet den Finanzintermediären eine zusätzliche Alternative zur Online-Identifizierung. Zudem wird durch das Erlauben der Geolokalisierung eine Erleichterung bei der Überprüfung der Wohnsitzadresse gewährt. Es kann davon ausgegangen werden, dass durch diese Prozesse die Online-Identifizierung an Attraktivität gewinnt und neue Geschäftsmodelle gefördert werden. Gleichzeitig wird durch das Abstellen auf den Chip des biometrischen Reisepasses ein hohes Sicherheitsniveau erreicht. Allenfalls können auch Prozesserleichterungen (Automatisierung) zu Kosteneinsparungen führen.

5 Weiteres Vorgehen

Die Änderungen des FINMA-RS 16/7 „Video- und Online-Identifizierung“ treten per 1. Juni 2021 in Kraft.

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