

Due diligence requirements for client onboarding via digital channels

Reference:	FINMA-Circ. 16/7 "Video and online identification"
Date:	3 March 2016
Entry into force:	8 March 2016
Legal framework:	FINMASA Article 7 para. 1 let. b AMLO-FINMA Article 3 para. 2
Appendix:	Glossary

Addressees					
	BankA		ISA	SESTA	FMIA
X	Banks				
X	Financial groups and congl.				
	Other intermediaries				
X	Insurers				
X	Insurance groups and congl.				
	Intermediaries				
X	Securities dealers				
	Trading venue				
X	Central counterparties				
X	Central securities depositories				
	Trade repositories				
X	Payment systems				
	Participants				
X	Fund management companies				
X	SICAVs				
X	Limited partnerships for CIsS				
X	SICAFs				
	Custodian banks				
X	Asset manager CIsS				
	Distributors				
	Representatives of foreign CIsS				
	Other intermediaries				
	SROs				
X	DSFIs				
	SRO-supervised institutions				
X	Audit firms				
	Rating agencies				

I. Subject matter and purpose	Margin no.	1
II. Scope of application	Margin no.	2–4
III. Video identification	Margin no.	5–28
A. Video identification on a par with in-person identification for individuals	Margin no.	5–22
B. Video identification of legal entities or partnerships	Margin no.	23–26
C. Video identification on a par with in-person identification for client onboarding involving more than one contracting party	Margin no.	27
D. Documents equivalent to a simple copy of an identification document for client onboarding by correspondence	Margin no.	28
IV. Online identification	Margin no.	29–44
A. Documents equivalent to a simple copy of an identification document for client onboarding by correspondence	Margin no.	29–30
B. Online identification by electronic copy of an identification document	Margin no.	31–44
V. Declaration of beneficial ownership	Margin no.	45–50
A. Qualified electronic signature on online form	Margin no.	47
B. TAN procedure or similar methods	Margin no.	48
C. Electronic transmission of the signed form	Margin no.	49–50
VI. Involvement of third parties	Margin no.	51
VII. Audit	Margin no.	52
VIII. Technological neutrality	Margin no.	53

I. Subject matter and purpose

FINMA has issued this circular in application of Article 3 para. 2 of the FINMA Anti-Money Laundering Ordinance (AMLO-FINMA; SR 955.033.0) for the interpretation of the due diligence requirements of the Anti-Money Laundering Act (AMLA; SR 955.0) and its implementing provisions on the digital provision of financial services. 1

II. Scope of application

This circular applies directly to financial intermediaries as defined in Article 2 para. 2 AMLA and those under Article 2 para. 3 AMLA which are subject to direct supervision by FINMA (DSFIs) in accordance with Article 14 AMLA. 2

The following references to AMLO-FINMA relate to the analogous provisions of the Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB) and the regulation of the Self-Regulatory Organisation of the Swiss Insurance Association (SRO-SIA). 3

References to this circular in SRO regulations become valid as of the entry into force of the circular. Any SRO regulation which differs from this circular will be dealt with through the regular approval process. 4

III. Video identification

A. Video identification on a par with in-person identification for individuals

Video identification has equal validity to in-person identification, provided the following criteria are met: 5

a) Technical and organisational requirements

Identification is to be made via audio-visual real-time (live transmission) communication between the contracting party and the financial intermediary. The financial intermediary utilises adequate technical equipment to ensure the secure video transmission as well as the reading and decryption of the information stored in the identification document's machine-readable zone (MRZ). 6

The picture and sound quality must be adequate to enable unambiguous identification. The financial intermediary can use technical aids to compensate for poor lighting, especially when taking the photographs required for the identification. 7

Specially trained employees at the financial intermediary are responsible for identifying the contracting party. The full duration of the interview must be audio-recorded.	8
The financial intermediary must define a process for conducting the identification interview and a dialogue guide for those employees responsible for video identification.	9
b) Identity verification	
The video identification process for individuals is set out in margin nos. 11–22.	10
The financial intermediary structures the online onboarding process in such a way that the contracting party fills out the details required under Articles 44 and 60 AMLO-FINMA electronically and transfers them to the financial intermediary before the audio-visual identification interview takes place. The financial intermediary then reviews the details using appropriate technical tools or by posing targeted questions during the identification interview. At this stage of the process, the financial intermediary is looking for conspicuous behaviour patterns which could indicate that the identification documents are not authentic. In addition, the financial intermediary checks the information gathered during the onboarding process against the information contained in the contracting party's identification document.	11
The financial intermediary must obtain the contracting party's explicit consent to conduct the video identification and audio recording before starting the video interview.	12
During the video transmission, the financial intermediary takes photographs of the contracting party as well as of all the relevant pages in the identification document and checks whether the photographs taken during the interview match those in the identification document.	13
The financial intermediary also reviews the authenticity of the identification documents by using a machine to read and decrypt the information in the MRZ and by examining one or more of the optically variable features of the identification document (e.g. a kinegram). This can be done by using technical tools or by visual confirmation (e.g. by tilting the identification document). The financial intermediary checks that the decrypted information matches the other information in the identification document and the data provided by the contracting party during the onboarding process.	14
Only official identification documents issued by the relevant country can be accepted for this process. Moreover, the documents must have an MRZ and optical security features, such as holographic-cinematic marks or printed elements with latent image effects.	15
The identity of the contracting party is to be verified by means of a TAN or another similar method.	16
Each identification process must be documented. The photographs of the identification document and contracting party must be filed and archived along with the audio recording of	17

the entire identification process.

c) Stopping the video identification process

The financial intermediary will stop the video identification process if: 18

- the picture or sound quality does not enable unambiguous identification of the contracting party; 19
- the financial intermediary identifies evidence of increased risks; or 20
- there are any doubts regarding the authenticity of the identification document or the identity of the contracting party. 21

The identification process can also be stopped and the client asked to use conventional channels (i.e. opening an account in person or by correspondence) instead. 22

B. Video identification of legal entities or partnerships

Video identification can be used to onboard legal entities or partnerships provided that the requirements outlined in margin nos. 24–25 and the provisions in Section III.A are met. 23

For contracting parties in the form of legal entities or partnerships, the financial intermediary must obtain an electronic extract either from the database of the relevant registration authority or from a trustworthy privately managed directory. The extract may also be submitted to the financial intermediary outside the video identification process. 24

The financial intermediary takes note of the electronic copy of the power of attorney for the contracting party and checks the identity of the individuals representing the legal entity/partnership through the video identification process as described in Section III.A. The identities of the legal entity's or partnership's representatives do not all have to be verified at the same time. 25

The financial intermediary may receive the declaration regarding the controlling person electronically in accordance with the provisions set out in Section V. 26

C. Video identification on a par with in-person identification for client onboarding involving more than one contracting party

Video identification is on a par with in-person identification when onboarding more than one contracting party, provided the procedure outlined in Section III.A and/or III.B is completed individually for each contracting party. 27

D. Documents equivalent to a simple copy of an identification document for client onboarding by correspondence

If the requirements outlined in Section III.A to III.C cannot be met in full, the documents generated electronically during the video identification process have the same validity as a simple copy of an identification document and fall under Articles 45 para. 2, 49 and 59 para. 1 let. d AMLO-FINMA. 28

IV. Online identification

A. Documents equivalent to a simple copy of an identification document for client onboarding by correspondence

A photograph of the identification document provided by the contracting party is equivalent to a simple copy of an identification document. The photograph can be sent electronically to the financial intermediary for filing. 29

Photographs of identification documents taken as part of the process described in Section IV.B are also equivalent to a simple copy of an identification document, even if not all of the criteria outlined in that section are met. 30

B. Online identification by electronic copy of an identification document

Electronic copies of identification documents submitted to the financial intermediary are equivalent to an authenticated copy of an identification document if they are generated through one of the following processes and in compliance with the requirements set out in margin nos. 32–37, 38–39, 40–41 or 42–44: 31

a) Electronic copy of an identification document authenticated by the financial intermediary

The financial intermediary obtains photographs of the contracting party and its identification document from the contracting party. Using appropriate technology, which at least permits the information contained in the MRZ to be read and decrypted, the financial intermediary then checks the decrypted information against the other information in the identification document and the data provided by the contracting party during the onboarding process. 32

In addition, the financial intermediary or custodian bank arranges to receive a payment from the contracting party transferred from an account held in the contracting party's name at a bank in Switzerland. 33

The identity of the contracting party must be verified using a TAN or similar method. The 34

financial intermediary must also confirm the contracting party's residential address by means of a:

- utility bill (power, water or telephone); 35
- postal delivery; or 36
- a public register, or a trustworthy, privately managed database/directory. 37

b) Electronic copy of an identification document with qualified electronic signature

The financial intermediary obtains an electronic copy of the contracting party's identification document transmitted electronically by the contracting party and an authentication by means of a qualified electronic signature from a provider of certification services recognised in Switzerland under the Federal Certification Services Act (ZertES; SR 943.03). 38

The financial intermediary checks the information in the identification document against the qualified electronic signature profile. The financial intermediary also verifies the contracting party's identity on the basis of a transfer from a bank account held in the contracting party's name in Switzerland or in a country with equivalent anti-money laundering regulations and supervision, as well as a TAN or similar method, and verifies the residential address as described in margin nos. 34–37. 39

c) Digital authentication

The authentication provider as defined in Article 49 AMLO-FINMA can also issue confirmations of authenticity electronically to the financial intermediary. To do so, the provider makes an electronic copy of the identification document, inseparably attaches a confirmation that its contents match those of the identification document, adds a digital timestamp and an employee signature to the file, and provides it to the financial intermediary. The financial intermediary then adds the file to its records. 40

If the authentication provider confirms the identification document's authenticity at the same address which was provided by the contracting party to the financial intermediary during the onboarding process as the contracting party's place of residence, and if confirmation of authenticity can be verifiably demonstrated from documentation as having been performed at that address, the authentication issued in this way also serves as a confirmation of domicile under Article 45 para. 2 AMLO-FINMA. 41

d) Legal entities and partnerships

The financial intermediary requests and verifies photographs of the individuals who are onboarding on behalf of the legal entity/partnership, as described in margin no. 32. 42

In addition, the financial intermediary or custodian bank arranges to receive a payment from the legal entity/partnership from an account held in the name of the legal entity/partnership at a bank in Switzerland, and verifies the contracting party's identity using a TAN or similar method. 43

Moreover, the financial intermediary obtains an extract as described in margin no. 24 and the document specifying the power of attorney for the legal entity/partnership. The financial intermediary can obtain the declaration concerning the controlling person electronically in line with the same criteria in Section V below. 44

V. Declaration of beneficial ownership

The requirements set out below apply to the declaration regarding the beneficial owner of assets as described in Article 59 ff. AMLO-FINMA as well as to the declaration regarding the beneficial owner in unlisted operational legal entities or partnerships (controlling person) as described in Article 56 ff. AMLO-FINMA. These requirements also apply to the declaration in connection with associations of individuals, trusts and other economic units, as defined in Article 64 AMLO-FINMA, and for the declaration of the policyholder/premium payer. 45

The financial intermediary adds both the declaration and the documentation regarding the contracting party's confirmation to its files. 46

A. Qualified electronic signature on online declaration form

The financial intermediary can obtain the contracting party's declaration as described in margin no. 45 by means of an electronic form signed by a qualified electronic signature. 47

B. TAN processes or similar methods

In the context of video or online identification, as an alternative to a qualified electronic signature, the contracting party can also confirm the declaration using a TAN or similar method, provided it enables reliable attribution to the contracting party (e.g. IP address). 48

C. Electronic transmission of the signed declaration form

The financial intermediary can also accept for its records an electronic copy, transmitted electronically, of a form printed and manually signed as a declaration within the meaning of margin no. 45. The financial intermediary adds to its files the documentation regarding the electronic transmission of the form by the contracting party and compares the signature on the form with that on the identification document. 49

The electronic transfer of the signed form can also take place within the context of an existing business relationship. 50

VI. Involvement of third parties

As set out in Articles 28 and 29 AMLO-FINMA, the financial intermediary may mandate individuals and companies to identify the contracting party in line with the procedure described in Sections III and IV and to establish the identity of the beneficial owner in accordance with Section V. The financial intermediary verifies in particular whether the person/company in question has the requisite professional knowledge and technology to process the identification documents of the relevant countries. The financial intermediary is sent the photographs/electronic copies, sound recordings, declarations and documentation generated by the third party and files them accordingly. 51

VII. Audit

The recognised regulatory auditors verify compliance with this circular in line with the provisions of FINMA Circular 2013/3 “Auditing” and disclose their findings in the audit report. 52

VIII. Technological neutrality

The wording in the following AMLO-FINMA articles extends to the following formats in a digital context: 53

Article and wording	Explanations and practical examples of the digital format
Article 16 para. 1 let. a AMLO-FINMA: The clarifications comprise [...] obtaining written or verbal information from the contracting party, the controller or the beneficial owner of the assets.	Written information: text-based information received electronically (e.g. e-mail, chat etc.) Verbal information: telephone, video conference
Article 28 para. 1 AMLO-FINMA: The financial intermediary may [...] mandate in writing if [...]	The mandate may also be awarded electronically, e.g. by digital signature
Article 28 para. 2 AMLO-FINMA: The financial intermediary may entrust the fulfilment of these due diligence requirements without a written agreement [...]	In principle, a written agreement is not necessary.
Article 29 para. 2 AMLO FINMA: The financial intermediary must add a copy of the documents, which served to fulfil the requirements for the prevention of money laundering and the financing of terrorism, to its files and obtain written confirmation that these copies are identical to the original.	Electronic copies of the documents are equivalent to a copy. The confirmation can, for example, also be sent by e-mail or another secure electronic channel (e.g. an upload portal) provided that the identity of the person submitting the copies and the fact that the confirmation is for the copies in question can be shown clearly and unambiguously.
Article 45 para. 2 AMLO-FINMA: If the onboarding is initiated without personal contact, the DSFI shall also confirm the address by postal delivery or in	See Section IV.B.

some other way which is similarly conclusive [...]	
Article 47 para. 1 let. b AMLO-FINMA: [...] a written extract from the commercial register database;	Electronic files (e.g. PDF and corresponding picture formats) have equal validity to the written extracts.
Article 47 para. 2 let. c AMLO-FINMA: [...] a written extract from trustworthy, privately managed directories and databases.	Electronic files (e.g. PDF and corresponding picture formats) have equal validity to the written extracts.
Articles 56, 57, 58, 59, 60, 61, 62, 63, 64 AMLO-FINMA: [...] written declaration [...]	See Section V.
Articles 48 and 60 AMLO-FINMA: [...] signed [...]	See Sections IV and V.
Articles 12, 29, 45, 48, 49, 74 copy/copies	See Section IV.

Glossary

Simple copy of an identification document

This is an unauthenticated copy of an identification document. It was presented either in person or during onboarding by correspondence and/or via digital channels in line with simplified due diligence requirements, to which exemptions from mandatory authentication apply.

Machine-readable zone (MRZ)

The machine-readable zone is the visible part of an identification document designed specifically for optical text recognition.

TAN

A transaction number which a financial intermediary issues to a contracting party as a one-time password for the purposes of video/online identification and determining the beneficial owner. There are various procedures, including:

- **indexed TAN list, iTAN:** list with numbered (indexed) TANs with no time limit.
- **mTAN:** mobile TAN subject to a time limit, which the financial intermediary sends to the user by SMS on a mobile telephone number registered in the user's name.
- **photoTAN/QR-TAN:** app-based TAN process in which a coloured or black-and-white code displayed on a screen in a mosaic format is scanned in order to generate a TAN.
- **pushTAN:** app-based TAN process used by financial intermediaries. For video and online identification, any app provided by the financial intermediary to perform its services is eligible provided it is password-protected.
- **TAN generator:** TANs can be generated by a TAN generator.
- **TAN list:** list with TANs with no time limit.

The use of TANs is subject to the following conditions:

- the TAN must be issued by the financial intermediary to the client through a second, independent channel; or
- the app must be password-protected.