

EBA/GL/2022/15

22/11/2022

Final Report

Guidelines on the use of Remote Customer Onboarding Solutions
under Article 13(1) of Directive (EU) 2015/849

Contents

1. Executive Summary	3
2. Background and rationale	4
3. Guidelines	7
1. Compliance and reporting obligations	9
2. Subject matter, scope and definitions	10
3. Implementation	11
4. Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849	12
4. Accompanying documents	24

1. Executive Summary

In September 2020, the European Commission published its Digital Finance Strategy for the European Union. This document sets out a strategic objective ‘to embrace digital finance for the good of consumers and businesses and identifies EU priorities and actions to ‘make the benefits of digital finance available to European consumers and businesses while also mitigating risks¹.

One of the Commission’s priorities is to address the fragmentation in the Digital Single Market for financial services. To this end, the Commission asked the EBA to issue guidelines on the application of anti-money laundering and countering the financing of terrorism (AML/CFT) rules where customers are onboarded remotely. In the Commission’s view, customer due diligence (CDD) rules in Directive (EU) 2015/849 do not provide sufficient clarity about what is, and what is not, allowed in a remote and digital context.

The EBA confirms that supervisory expectations and what credit and financial institutions do to comply differs across Member States. Regulatory divergence is an obstacle to innovation and the cross-border provision of financial services; it can also create gaps and expose the Union’s single market to financial crime. For this reason, these Guidelines set common EU standards on the development and implementation of sound, risk-sensitive initial CDD processes in the remote customer onboarding context. They set out the steps credit and financial institutions should take when choosing remote customer onboarding tools and what credit and financial institutions should do to satisfy themselves that the chosen tool is adequate and reliable, that it remains adequate and reliable, and that it enables them to comply effectively with their initial CDD obligations. The Guidelines are clear that as long as the conditions set out in these guidelines are met, and to the extent that this is permitted by national law, the choice of individual technological solutions is the credit and financial institutions.

The EBA publicly consulted on a version of these guidelines between 10 December 2021 and 10 March 2022 and amended them as necessary to address concerns raised in this context. The Guidelines will enter into force 6 months after their publication in all EU official languages.

Next steps

The guidelines will be translated into the official EU languages and published on the EBA website. The deadline for competent authorities to report whether they comply with the guidelines will be two months after the publication of the translations. The guidelines will apply from **dd.mm.yyyy**.

¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591>

2. Background and rationale

Background

1. In 2020, when publishing its Digital Finance Strategy¹, the European Commission invited the EBA, to develop guidelines in consultation with the other European Supervisory Authorities (ESAs) on elements related to identification and verification for customer remote onboarding and reliance on CDD processes carried out by third parties, specifically:
 - a. the types of innovative technologies that are acceptable when financial institutions on-board customers remotely,
 - b. the conditions that need to be met when financial institutions use innovative technologies to on-board customers remotely,
 - c. the acceptable forms of digital documentation used for remote customer onboarding, and
 - d. the conditions under which it is acceptable for financial institutions to rely on information provided by third parties when on-boarding customer remotely.
2. The Commission made this request to address the fact that in the Commission's view, the current AML/CFT rules on CDD in Directive (EU) 2015/849 do not provide sufficient clarity about what is, and what is not, allowed in a remote and digital context.
3. There has been a significant increase in demand for remote onboarding from institutions and their customers. This trend was exacerbated by restrictions on movement in the context of the COVID-19 pandemic, which highlighted the importance of institutions having at their disposal reliable and effective means to meet their CDD obligations in this context.
4. The EBA considers it important for competent authorities and credit and financial institutions to understand the capabilities of these new remote solutions to onboard customers to make the most of the opportunities they offer. At the same time, to support their sound and responsible use, competent authorities and credit and financial institutions need to be aware of ML/TF risks arising from the use of such tools and take steps to mitigate those risks effectively. Consequently, the EBA published a first Opinion, in 2018, on the use of innovative solutions by credit and financial institutions in the CDD process², and included specific guidance on collecting identity's evidence for non-face to face situations in its revised Risk Factors Guidelines³. These new guidelines complement existing guidelines with specific instructions on the steps credit and financial

¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591>

² JC 2017 81

³ EBA/GL/2021/02



institutions should take when choosing remote customer onboarding tools, and when ascertaining whether these tools are sufficient to enable them to comply effectively with their initial CDD obligations. Supervisors will use these guidelines to assess whether credit and financial institutions' tools are adequate.

Rationale

5. Under the EBA competences within its regulatory framework, the EBA has a leading role in the area of prevention of the use of the EU's financial system for ML/TF purposes, and is mandated to lead, monitor and coordinate the EU financial sector's fight against ML/TF. Through these guidelines, the EBA establishes a common understanding by competent authorities and credit and financial institutions on the steps credit and financial institutions should take to ensure safe and effective remote customer onboarding practices that are in line with the applicable AML/CFT legal and data protection framework.
6. These Guidelines do not favour specific technological solutions and respect the principle of technological neutrality. Technological neutrality is important to foster ongoing innovation and to ensure that the AML/CFT principles and procedures set out in these guidelines remain relevant and applicable. These guidelines should help credit and financial institutions to mitigate risks arising from the use of technological solutions in the remote onboarding context, such as impersonation fraud risks.
7. These guidelines apply to standard remote customer onboarding journeys. Nevertheless, in situations where simplified due diligence could be applied, credit and financial institutions may adjust the elements of these guidelines that relate to the nature and type of verification data and documentation in line with a risk-based approach. Paragraphs 4.40 to 4.44 of the EBA ML/TF Risk Factors Guidelines set out what simplified due diligence might entail.
8. These guidelines also support the use of non-qualified trust services or other solutions that are regulated, recognized, approved, or accepted at a national level, in accordance with the Article 13(1) (a) of the AMLD. The use of such services and solutions is, however, contingent on the application of adequate safeguards that mitigate against impersonation and identity fraud risks in this context. The guidelines set out what these safeguards should be.

Interaction with other guidelines

9. The guidelines complement the following ESAs Guidelines:
 - EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849⁴;

⁴ EBA/GL/2021/02



- EBA Guidelines on internal governance under Directive 2013/36/EU⁵;
- EBA Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849⁶;
- EBA Guidelines on outsourcing arrangements⁷;
- EBA Guidelines on ICT and security risk management⁸.

⁵ EBA/GL/2021/05

⁶ EBA/CP/2021/31

⁷ EBA/GL/2019/02

⁸ EBA/GL/2019/04



3. Guidelines

EBA/GL/2022/15

22/11/2022

Guidelines

on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849

1. Compliance and reporting obligations

Status of these guidelines

1. This document contains guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010⁹. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with these guidelines.
2. Guidelines set the EBA view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by **[dd.mm.yyyy]**. In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website with the reference 'EBA/GL/2022/15'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to EBA.
4. Notifications will be published on the EBA website, in line with Article 16(3).

⁹ Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, (OJ L 331, 15.12.2010, p.12).

2. Subject matter, scope and definitions

Subject matter and scope of application

5. These guidelines set out the steps credit and financial institutions should take when adopting or reviewing solutions to comply with their obligations under Article 13(1) points (a), (b) and (c) of Directive (EU) 2015/849¹⁰ to onboard new customers remotely. It also sets out the steps credit and financial institutions should take when relying on third parties in accordance with Chapter I, Section 4 of Directive (EU) 2015/849, and the policies controls and procedures credit and financial institutions should put in place in relation to customer due diligence (CDD) as referred to in Article 8(3) and (4) point (a) of Directive (EU) 2015/849 where the CDD measures are performed remotely.
6. Competent authorities should have regard to these guidelines when assessing whether the steps credit and financial institutions take to comply with their obligations under Directive (EU) 2015/849 in the remote customer onboarding context are adequate and effective.

Addressees

7. These guidelines are addressed to competent authorities as defined in point (i) Article 4(2) of Regulation (EU) No 1093/2010. These guidelines are also addressed to financial sector operators as defined in Article 4(1a) of that Regulation, which are credit and financial institutions as defined in Article 3(1) and 3(2) of Directive (EU) 2015/849.

¹⁰ Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

Definitions

8. Unless otherwise specified, terms used and defined in Directive (EU) 2015/849 have the same meaning in the guidelines. In addition, for the purposes of these guidelines, the following definitions apply:

Biometric data

Personal data relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data, which is obtained and processed using technical means.

3. Implementation

Date of application

These Guidelines apply from **dd.mm.yyyy**. {instruction to editors: please insert that date that corresponds to the date six months after publication in all EU official languages.}

4. Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849

4.1 Internal policies and procedures

4.1.1 Policies and procedures relating to remote customer onboarding

9. Credit and financial institutions should put in place and maintain policies and procedures to comply with their obligations under Article 13(1) (a) and (c) of Directive (EU) 2015/849 in situations where the customer is onboarded remotely. These policies and procedures should be risk-sensitive and set out at least:
- a) a general description of the solution credit and financial institutions have put in place to collect, verify, and record information throughout the remote customer onboarding process. This should include an explanation of the features and functioning of the solution;
 - b) the situations where the remote customer onboarding solution can be used, taking into account the risk factors identified and assessed in accordance with Article 8 (1) of the Directive (EU) 2015/849 and in the business-wide risk assessment, including a description of the category of customers, products and services that are eligible for remote onboarding;
 - c) which steps are fully autonomized and which steps require human intervention;
 - d) the controls in place to ensure that the first transaction with a newly onboarded customer is executed only once all initial customer due diligence (CDD) measures, have been applied;
 - e) a description of the induction and regular training programs to ensure staff awareness and up-to-date knowledge of the functioning of the remote customer onboarding solution, the associated risks, and of the remote customer onboarding policies and procedures aimed at mitigating such risks.
10. The policies and procedures, when implemented, should enable credit and financial institutions to ensure compliance with the provisions in Section 4.2 to 4.7 of these Guidelines.

4.1.2 Governance



11. In addition to the provisions set out in the Section 4.2.4 of the EBA Compliance Officer Guidelines¹¹, the AML/CFT Compliance Officer¹² should, as part of their general duty to prepare policies and procedures to comply with the CDD requirements, make sure that remote customer onboarding policies and procedures are implemented effectively, reviewed regularly and amended where necessary.
12. The management body of the credit and financial institution should approve remote customer onboarding policies and procedures and oversee their correct implementation.

4.1.3 The pre-implementation assessment of the remote customer onboarding solution

13. When considering whether to adopt a new remote customer onboarding solution, credit and financial institutions should carry out a pre-implementation assessment of the remote customer onboarding solution.
14. Credit and financial institutions should set out the scope, steps and record keeping requirements of the pre-implementation assessment in their policies and procedures, which should include at least:
 - a) an assessment of the adequacy of the solution regarding the completeness and accuracy of the data and documents to be collected, as well as of the reliability and independence of the sources of information it uses;
 - b) an assessment of the impact of the use of the remote customer onboarding solution on its business-wide risks, including ML/TF, operational, reputational and legal risks;
 - c) the identification of possible mitigating measures and remedial actions for each risk identified in the assessment under letter b);
 - d) tests to assess fraud risks including impersonation fraud risks and other information and communications technology (“ICT”) and security risks, in accordance with the provision 43 of the EBA Guidelines on ICT and security risk management¹³;
 - e) an end-to-end testing of the functioning of the solution targeting customer(s), product(s) and service(s) identified in the remote customer onboarding policies and procedures.
15. Credit and financial institutions should consider the criteria in paragraph 14 (a) (d) and (e) to be met where the solution uses one of the following:

¹¹ Draft Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive

¹² In accordance with the Proportionality criteria set out in Section 4.2.2 of the Compliance Officer Guidelines

¹³ EBA/GL/2019/04



- a) electronic identification schemes notified in accordance with Article 9 of Regulation (EU) No 910/2014 and meeting the requirements of assurance levels 'substantial' or 'high' in accordance with Article 8 of that Regulation;
 - b) relevant qualified trust services that meet the requirements of Regulation (EU) No 910/2014, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation.
16. Credit and financial institutions should be able to demonstrate to their competent authority which assessments they carried out before implementation of the remote customer onboarding solution, the outcome of their assessment and how its use is appropriate in light of the ML/TF risks identified for the types of customer(s), service(s), geographies and product(s) in its scope.
17. Credit and financial institutions should start using a remote customer onboarding solution only once they are satisfied that it can be integrated into the institution's wider internal control system, thereby allowing the institution to adequately manage the ML/TF risks that may arise from the use of the remote customer onboarding solution.

4.1.4 Ongoing monitoring of the remote customer onboarding solution

18. Credit and financial institutions should monitor the remote customer onboarding solution on an ongoing basis to ensure that it operates in line with the credit and financial institutions expectations. They should complement their policies and procedures described in paragraph 9 with a description of at least:
- a) the steps they will take to be satisfied of the ongoing quality, completeness, accuracy and adequacy of data collected during the remote customer onboarding process, which should be commensurate to the ML/TF risks to which the credit and financial institution is exposed to;
 - b) the scope and frequency of such regular reviews; and
 - c) the circumstances that will trigger ad hoc reviews, which should include at least:
 - a. changes to the ML/TF risk exposure of the credit and financial institution;
 - b. deficiencies on the functioning of the solution detected in the course of monitoring, audit or supervisory activities;
 - c. A perceived increase in fraud attempts;
 - d. changes to the legal or regulatory framework.

19. Credit and financial institutions should set out in their procedures and processes remedial measures where a risk has materialised, or where errors have been identified that have an impact on the efficiency and effectiveness of the general remote customer onboarding solution. These measures should include at least:
- a) a review of all affected business relationships, to assess whether sufficient initial CDD has been applied by the credit and financial institutions in order to comply with article 13 (1), (a), (b) and (c) of the AMLD. Credit and financial institutions should prioritise those business relationships that carry the highest ML/TF risk;
 - b) taking into account the information obtained in the above-mentioned review, an assessment of whether an affected business relationships should be:
 - a. subject to additional due diligence measures;
 - b. subject to limitations, such as limits on the volume of transaction, where permitted under national law, until such time as a review has taken place;
 - c. terminated;
 - d. reported to the FIU;
 - e. reclassified into a different risk category.
20. Credit and financial institutions should consider the most effective way to monitor the ongoing adequacy and reliability of the remote customer onboarding solutions. They should consider one or more of, but not limited to, the following means:
- i. quality assurance testing;
 - ii. automated critical alerts and notifications;
 - iii. regular automated quality reports;
 - iv. sample testing;
 - v. manual reviews.
21. This section also applies where fully automated remote customer onboarding solutions are used which are highly dependent on automated algorithms, without or with little human intervention.
22. Credit and financial institutions should be able to demonstrate to their competent authority which reviews they carried out and the remedial steps they have taken to rectify any shortcomings identified throughout the lifetime of the remote customer onboarding solution.

4.2 Acquisition of information

4.2.1 Identifying the customer

23. In addition to the points set out in paragraph 9, credit and financial institutions should set out in their policies and procedures the information needed to identify the customer, the types of documents, data, or information the institution will use to verify the customer's identity and the manner in which this information will be verified.
24. Credit and financial institutions should ensure that:
- a) the information obtained through the remote customer onboarding solution is up-to-date and adequate to meet the applicable legal and regulatory standards for initial customer due diligence;
 - b) any images, video, sound and data are captured in a readable format and with sufficient quality so that the customer is unambiguously recognisable;
 - c) the identification process does not continue if technical shortcomings or unexpected connection interruptions are detected.
25. Credit or financial institutions should consider the criteria in paragraph 24 to be met where the solution uses one of the following:
- a) electronic identification schemes notified in accordance with Article 9 of Regulation (EU) No 910/2014 and meeting the requirements of assurance levels 'substantial' or 'high' in accordance with Article 8 of that Regulation;
 - b) relevant qualified trust services that meet the requirements of Regulation (EU) No 910/2014, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation.
26. The documents and information collected during the remote identification process, which are required to be retained in accordance with Article 40(1) point (a) of Directive (EU) 2015/849, should be time-stamped and stored securely by the credit and financial institution. The content of stored records, including images, videos, sound and data should be available in a readable format and allow for ex-post verifications.

4.2.2 Identifying natural persons

27. Credit and financial institutions should determine in their policies, as set out in Section 4.1.1 paragraph 9, the information they need to obtain to identify customers remotely in accordance with Article 13(1) (a) and (c) of Directive (EU) 2015/849. In addition, credit and financial institutions should define what information:
- a) is manually entered by the customer;

- b) is automatically captured from the documentation provided by the customer;
- c) is gathered using other internal or external sources.

28. Credit and financial institutions should put in place and maintain appropriate mechanisms to ensure that the information they capture automatically in line with paragraph 27 is reliable. They should apply controls to address associated risks, including risks associated with automatic capture of data such as the obfuscation of the location of the customer's device spoofed Internet Protocol (IP) addresses or services such as Virtual Private Networks (VPNs).

4.2.3 Identifying Legal Entities

29. Where credit and financial institutions remotely onboard customers that are legal entities, they should define in their policies and procedures, as set out in Section 4.1.1 paragraph 9, which category of legal entities they will onboard remotely, taking into account the level of ML/TF risk associated with each category, and the level of human intervention required to validate the identification information.

30. Credit and financial institutions should ensure that the remote customer onboarding solution has features to collect:

- a) all relevant data and documentation to identify and verify the legal person
- b) all relevant data and documentation to verify that the natural person acting on behalf of the legal person is legally entitled to act as such;
- c) the information regarding the beneficial owners in accordance with provision 4.12 of the EBA Risk Factors Guidelines¹⁴.

31. For the natural person acting on behalf of a legal person, credit and financial institutions should apply the identification process described in the Section 4.2.2.

4.2.4 Nature and purpose of the business relationship

32. When credit and financial institutions assess and, as appropriate, obtain information on the purpose and intended nature of the business relationship in accordance with Article 13(1) point (c) of Directive (EU) 2015/849, as further specified in Section 4.38 of the EBA Risk Factors Guidelines, they should, for the purposes of these guidelines, have completed the relevant actions before the end of the remote customer onboarding process.

4.3 Document authenticity & integrity

¹⁴ EBA/GL/2021/02



33. Where credit and financial institutions accept reproductions of an original document and do not examine the original document, they should take steps to ascertain that the reproduction is reliable. Credit and financial institutions should establish at least the following:
- a) if the reproduction includes security features embedded in the original document and if the specifications of the original document that are being reproduced are valid and acceptable, in particular, type, size of characters and structure of the document, by comparing them with official databases, such as PRADO¹⁵;
 - b) whether personal data has been altered or otherwise tampered with or, where applicable, whether the picture of the customer embedded in the document was not replaced;
 - c) whether the integrity of the algorithm used to generate the unique identification number of the original document, in case the official document has been issued with machine-readable zone (MRZ);
 - d) whether the provided reproduction is of sufficient quality and definition so as to ensure that relevant information is unambiguous;
 - e) that the provided reproduction has not been displayed on a screen based on a photograph or scan of the original identity document.
34. Where credit and financial institutions use features to automatically read information from documents, such as Optical Character Recognition (OCR) algorithms or Machine Readable Zone (MRZ) verifications, they should take the steps necessary to ensure that that these tools capture information in an accurate and consistent manner.
35. In situations where the device the customers use to prove their identity allows the collection of relevant data, for example because the data is contained in the chip of a national identity card, and it is technically feasible for the credit and financial institutions to access this data, credit and financial institutions should consider using this information to verify its consistency with the information obtained through other sources, such as the submitted data or other documents submitted by the customer.
36. Where available, during the verification process, credit and financial institutions should verify the security features embedded in the official document, if any, such as holograms, as a proof of their authenticity.
37. Credit and financial institutions should set out in their policies and procedures how they will adjust their documentation requests for the purposes of financial inclusion. Where weaker or non-traditional forms of documentation are accepted as a result, credit and financial institutions should carry out in addition to measures as set out in paragraph 4.10 of the EBA

¹⁵ <https://www.consilium.europa.eu/prado/en/prado-start-page.html>

Risk Factors Guidelines, controls or increased human intervention to satisfy themselves that they understand the ML/TF risk associated with the business relationship.

4.4 Matching customer identity as part of the verification process

38. Remote customer onboarding solutions implemented by a credit and financial institutions should, as a minimum, allow for the following, as part of their verification process:
- a) there is a match between the visible information of the natural person and the documentation provided;
 - b) where the customer is a legal entity, it is publicly registered, where applicable;
 - c) where the customer is a legal entity, the natural person that represents it is entitled to act on its behalf.
39. Where the remote customer onboarding solution involves the use of biometric data to verify the customer's identity, credit and financial institutions should make sure that the biometric data is sufficiently unique to be unequivocally linked to a single natural person. Credit and financial institutions should use strong and reliable algorithms to verify the match between the biometric data provided on the submitted identity document and the customer being onboarded. In situations where the solution does not provide the required level of confidence, additional controls should be applied.
40. In situations where the evidence provided is of insufficient quality resulting in ambiguity or uncertainty so that the performance of remote checks is affected, the individual remote customer onboarding process should be interrupted and restarted or redirected to a face-to-face verification.
41. Where credit and financial institutions use unattended remote onboarding solutions, in which the customer does not interact with an employee to perform the verification process, they should:
- a) ensure that any photograph(s) or video is taken under adequate lighting conditions and that the required properties are captured with necessary clarity to allow the proper verification of the customer's identity;
 - b) ensure that any photograph(s) or video is taken at the time the customer is performing the verification process;
 - c) perform liveness detection verifications, which may include procedures where a specific action from the customer is required to verify that he/she is present in the communication session or which can be based on the analysis of the received data and does not require a specific action by the customer;



- d) use strong and reliable algorithms to verify if the photograph(s) or video taken matches the picture(s) retrieved from the official document(s) belonging to the customer.
42. Where credit and financial institutions use attended remote customer onboarding solutions in which the customer interacts with an employee to perform the verification process, they should:
- a) ensure that the quality of the image and audio is sufficient to allow the proper verification of the customer's identity and that reliable technological systems are used;
 - b) foresee the participation of an employee that has sufficient knowledge of the applicable AML/CFT regulation and security aspects of remote verification and who is sufficiently trained to anticipate and prevent the intentional or deliberate use of deception techniques related to remote verification, and to detect and react in case of their occurrence;
 - c) develop an interview guide defining the subsequent steps of the remote verification process as well as the actions required from the employee. The interview guide should include guidance on observing and identifying psychological factors or other features that might characterise suspicious behaviour during remote verification.
43. Where possible, credit and financial institutions should use remote customer onboarding solutions that include randomness in the sequence of actions to be performed by the customer for verification purposes to guard against risks such as the use of synthetic identities or coercion. Where possible, credit and financial institutions should also provide random assignments to the employee responsible for the remote verification process to avoid collusion between the customer and the responsible employee.
44. In addition to the above, and where commensurate with the ML/TF risk associated with the business relationship, credit and financial institutions should use of one or more of the following controls or a similar measure to increase the reliability of the verification process. These controls or measures may include, but are not limited to, the following:
- a) the first payment is drawn on an account in the sole or joint name of the customer with an EEA-regulated credit or financial institution or in a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849;
 - b) send a randomly generated passcode to the customer to confirm the presence during the remote verification process. The passcode should be a single-use and time-limited code;



- c) capture biometric data to compare them with data collected through other independent and reliable sources;
 - d) telephone contacts with the customer;
 - e) direct mailing (both electronic and postal) to the customer.
45. Credit and financial institutions should consider the criteria in paragraphs 38 to 43 to be met where the solution uses one of the following:
- a) electronic identification schemes notified in accordance with Article 9 of Regulation (EU) No 910/2014 and meeting the requirements of assurance levels 'substantial' or 'high' in accordance with Article 8 of that Regulation;
 - b) relevant qualified trust services that meet the requirements of Regulation (EU) No 910/2014, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation.

4.5 Reliance on third parties and outsourcing

46. In addition to the points set out in paragraph 9, credit and financial institutions should include in their policies and procedures specifications setting out which remote customer onboarding functions and activities will be carried out or performed by the credit and financial institution, by third parties or by another outsourced service provider.

4.5.1 Reliance on Third Party Providers in accordance with Chapter II, Section 4 of Directive (EU) 2015/849

47. In addition to the EBA Risk Factors Guidelines¹⁶, in particular to guidelines 2.20 to 2.21 and 4.32 and 4.37 of those Guidelines, they should apply the following criteria:
- a) take the steps necessary to be satisfied that the third party's own CDD remote customer onboarding processes and procedures and the information and data they collect in this context, are sufficient and consistent with requirements laid down in these Guidelines;
 - b) ensure the continuity of the business relationships established between the customer and the credit and financial institution to guard against events that might reveal shortcomings on the remote customer onboarding process carried out by the third party.

4.5.2 Outsourcing of CDD

¹⁶ EBA/GL/2021/02



48. Where credit and financial institutions outsource all or parts of the remote customer onboarding process to an outsourced service provider, as referred to in Article 29 of Directive (EU) 2015/849, credit and financial institutions should apply in addition to guidelines 2.20 to 2.21 and 4.32 and 4.37 of the EBA Risk Factors Guidelines and in addition to the EBA Guidelines on Outsourcing¹⁷ where applicable, before and during the business relationship with the outsourced service provider the following measures, the extent of which should be adjusted on a risk-sensitive basis:

- a) ensure that the outsourced service provider effectively implements and complies with the credit and financial institution's remote customer onboarding policies and procedures in accordance with the outsourcing agreement. This should be achieved through regular reporting, ongoing monitoring, on-site visits or sample testing;
- b) carry out assessments to ensure that the outsourced service provider is sufficiently equipped and able to perform the remote customer onboarding process. Assessments may include, but are not limited to, the assessment of staff training, technology fitness and data governance at the outsourced service provider;
- c) ensure that the outsourced service provider informs the credit and financial institutions of any proposed changes of the remote customer onboarding process or any modification made to the solution provided by the outsourced service provider.

49. Where the outsourced service provider stores customer data, including, but not limited to, photography, videos, and documents, during the remote onboarding process, credit and financial institutions should ensure that:

- a) only necessary customer's data is collected and stored in line with a clearly defined retention period;
- b) access to the data is strictly limited and registered;
- c) appropriate security measures are implemented to ensure that the stored data is protected.

4.6 ICT and security risk management

50. Credit and financial institutions should identify and manage their ICT and security risks related to the use of the remote customer onboarding process, including where credit and financial institutions rely on third parties or where the service is outsourced, including to group entities.

51. In addition to complying with requirements set out in the EBA Guidelines on ICT and security risk management¹⁸ where applicable, credit and financial institutions should use secure

¹⁷ [EBA Guidelines on outsourcing arrangements.docx \(europa.eu\)](#)

¹⁸ [EBA/GL/2019/04](#)



communication channels to interact with the customer during the remote customer onboarding process. The remote customer onboarding solution should use secure protocols and cryptographic algorithms according to the industry best practices to safeguard the confidentiality, authenticity, and integrity of the exchanged data, where applicable.

52. Credit and financial institutions should provide a secure access point for starting the remote customer onboarding process based on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 or for website authentication as referred to in Article 3(39) of that Regulation. The customer should also be informed about the applicable security measures that should be taken to ensure a secure use of the system.
53. Where a multi-purpose device is used to perform the remote customer onboarding process, a secure environment should be used for the execution of the software code on the customer's side, where applicable. Additional security measures should be implemented to ensure the security and reliance of the software code and the collected data, according to the security risk assessment as laid down in EBA Guidelines on ICT and security risk management.

4.7 Compliance with these guidelines where credit and financial institutions use trust services and national identification processes as referred to in Article 13(1) (a) of Directive (EU) 2015/849

54. Credit and financial institutions may use relevant trust services and electronic identification processes regulated, recognised, approved, or accepted by the relevant national authorities as referred to in Article 13 (1) point (a) of Directive (EU) 2015/849 to comply with these guidelines. When using such solutions, credit and financial institutions should assess in how far the solution complies with the provisions in these guidelines and apply measures necessary to mitigate any relevant risks that arise from the use of these solutions. They should particularly take into account whether the following risks are addressed:
 - a) the risks involved in the authentication and set out in their policies and procedures specific mitigation measures, especially with regard to impersonation fraud risks;
 - b) the risk that the customer's identity is not the claimed identity;
 - c) the risk of lost, stolen, suspended, revoked, or expired identity evidence, including, as appropriate, tools to detect and prevent the use of identity frauds.

4. Accompanying documents

4.1 Draft cost-benefit analysis / impact assessment

Article 16(2) of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) (EBA Regulation) provides that the EBA should carry out an analysis of ‘the potential related costs and benefits’ of any guidelines it develops. Such analyses shall be proportionate in relation to the scope, nature and impact of the guidelines. This analysis should provide an overview of the findings regarding the problem to be dealt with, the solutions proposed and the potential impact of these options.

In this section we look at specific issues where various options were weighed and choices made. The section explains the costs of benefits of each of these options and explains the preferred option.

More generally, the guidelines are not expected to create a significant burden on credit and financial institutions that use remote customer onboarding solutions- The guidelines are expected to provide significant benefit to the institutions as they will be able to have a common standard to follow and to make sure that the AML risk is minimized by following the recommended steps.

1. Inclusion of a “policies and procedures” section in the Guidelines

A. Problem identification

In its request to the EBA, the COM asked the EBA to draft guidelines, in consultation with the other ESAs, with a view to providing greater clarity and convergence on four points:

- 1) The types of innovative technologies that are acceptable when financial institutions onboard customers remotely;
- 2) The conditions that need to be met when financial institutions use innovative technologies to on-board customers remotely, including any supplemental measures that may be required;
- 3) The acceptable forms of digital documentation used for remote customer onboarding;
- 4) The conditions under which it is acceptable for financial institutions to rely on information provided by third parties when on-boarding customers remotely, including, where relevant, clarification of any issues arising in respect of liability.

In addition to the above points, some issues related to remote customer onboarding stem from governance shortcomings, rather than technical features. The governance arrangements however are not covered in the European Commission request.

B. Policy objectives

The objective is to prevent the use of the EU’s financial system for ML/TF purposes, while observing the principle of technology neutrality.

C. Options considered

Option 1: No governance arrangements included in the guidelines, in line with the European Commission request

Option 2: Governance arrangements included in the guidelines, in line with the EBA survey findings

D. Cost-benefit analysis

The table below shows the pros and cons of each of the options considered.

	Pros	Cons
Option 1: No governance arrangements included in the guidelines	Follows exactly the request from the European Commission	Does not cover an important source of risk in the remote customer onboarding
Option 2: Governance arrangements included in the guidelines	Covers governance, that was identified as an important source of risks related to remote customer onboarding	

E. Preferred option

Option 2 is preferred, as it ensures that the credit and financial institutions oversee the remote customer onboarding solution(s) during its lifecycle, while all areas of potential risks, including shortcomings in governance, are covered.

2. Proportionality in governance arrangements when using solutions under eIDAS regulation

A. Problem identification

The section “Policies and procedures relating to remote customer onboarding” sets out governance arrangements necessary to create an ongoing secure environment and ensure consistency in the process.



In cases where credit and financial institutions resort to digital interties under the eIDAS framework, some aspects of the policies and procedures may have been covered in the assessments conducted as part of rigorous conformity assessments and peer-to-peer reviews under A. 8-12 eIDAS.

The application of the governance arrangements in such cases could create disproportionate work with respect to the CDD process.

B. Policy objectives

The objective is to prevent the use of the EU's financial system for ML/TF purposes, while acknowledging the work and progress that has already been done until today in the framework of the eIDAS regulation and leveraging on this work in the CDD processes of the credit and financial institutions.

C. Options considered

Option 1: No differentiation in governance provisions

Option 2: Exemption of the eID solutions from governance provisions

Option 3: Governance provisions taking into account the assessments under eID solutions

D. Cost-benefit analysis

Option 1 envisages that the governance arrangements are the same irrespective of the method of verification of identity and that the credit and financial institution should not consider any assessment already done by the digital identity provider. While this approach may be secure, it is burdensome and involves double work with regard to assessments that already have been conducted by the digital identity issuers.

Option 2 envisages an exemption of some governance arrangements for cases when eID solutions are used. This option would reduce the burden of verification on credit and financial institutions, but at the same time, may lead to gaps in the verification process, because using a certified eIDAS digital identity does not mean by itself that there are no associated risks to the Financial Sector Operator and to the customer.

In Option 3, the Guidelines allows credit and financial institutions, when using a certified digital identity issuer, to take into account the assessment already performed by the national competent authority according to Regulation on electronic identification and trust services for electronic transactions in the internal market¹⁹. This allows the credit and financial institutions to the extent possible to leverage the assessments already conducted, but the ultimate responsibility for the underlying verification process still lies with it.

Options	Pros	Cons

¹⁹ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014

Option 1: No differentiation in governance provisions	Ensuring that the due diligence is conducted at the level of credit and financial institution	In cases where some of these steps are already taken as part of digital identity issuer, the governance provisions may lead to double work
Option 2: Exemption of the eID solutions from governance provisions	Acknowledgement of the rigorous conformity assessments and peer-to-peer reviews under eIDAS	Risk of credit and financial institutions relying on the eIDAS assessments, and not considering other risks that might be associated to the overall remote customer onboarding process
Option 3: Taking into account the assessments under eID solutions	Acknowledgement of the rigorous conformity assessments and peer-to-peer reviews under eIDAS	

E. Preferred option

The preferred option is Option 3, where the credit and financial institutions can take into account the assessments conducted under the eID solutions notified under eIDAS. In this regard, when resorting to certified digital identity issuer, credit and financial institutions should take into account the assessment already performed by the national competent authority.

3. Verification process: Liveness detection

A. Problem identification

The guidelines set out how credit and financial institutions should verify that the person entering the business relationship is the person that claims to be. One of the steps of the verification process is the ability to verify whether the video, picture or other biometric data belong to a living person at the moment of the capture. In situations where credit and financial institutions do not resort to live videoconference, credit and financial institutions can perform these checks by using active or passive liveness detection. This part discusses whether and when liveness detection should be required.

B. Policy objectives

The objective is to increase the reliability of the verification process, while observing the principle of technology neutrality.

C. Options considered

Option 1: No mandatory liveness detection

Option 2: Mandatory liveness detection for all unattended situations

Option 3: Mandatory liveness detection in all cases

D. Cost-benefit analysis

The liveness detection (passive or active) aims to increase the reliability of the verification process and it might be a key requirement for the remote customer onboarding process, therefore it should not be avoided, as suggested in option 1.

At the same time, other more advanced approaches and technologies that increase the reliability of the verification process are already developed. Implementation of liveness detection may be costly but, by itself, it is not the unique key safeguard for the verification process. Therefore, Option 3, imposing liveness detection in all cases is assessed to be disproportionate.

The second option requires the use of liveness detection only in unattended situations, i.e. where the customer does not interact with an employee of the credit and financial institution to perform the verification process. This means that all unattended situations, with fully automated remote verification, would require liveness detection (apart from situations where credit and financial institutions resort to Digital Identity Issuers).

Unattended situations are highly dependent on the technology with little or no direct human intervention. Requiring liveness detection will increase the reliability of the verification process. This approach is proportionate, acknowledges the advances in technology and makes sure that liveness detection is deployed when most needed.

E. Preferred option

The preferred option is mandatory liveness detection in all unattended situations only (Option 2). These situations are highly dependent on the technology with little or no direct human intervention. In this context, EBA considered that the reliability of the verification process increases significantly when the process resorts to liveness detection.



4.2 Feedback on the public consultation and on the opinion of the BSG

The EBA publicly consulted on a draft version of these guidelines. The consultation period lasted for 3 months and ended on 10 March 2022. 58 responses were received, including a response from the BSG. 43 non-anonymous responses are now published on the EBA website.

This chapter summarises the comments raised by respondents, the analysis and discussion resulting from these comments, and the actions the EBA has taken to address them, if deemed necessary, including changes to the draft.

In many cases, respondents made similar comments. In such cases, the comments, and the EBA's analysis thereof, are grouped in a way that the EBA considers most appropriate. The section below includes the EBA's response to the submission from the EBA's Banking Stakeholder Group. In addition, in the feedback table that follows, the EBA has summarised the most relevant comments received from all respondents and has explained which responses have or have not led to changes and the reasons for the decision.

The EBA's response to the Banking Stakeholder Group's submission

The BSG submitted a number of comments on the draft guidelines and highlighted in particular the following points:

- The scope of the guidelines. The BSG suggested to extend the scope of the Guidelines for other situations that are not initial customer due diligence, such as the acquisition of new products.

The EBA clarifies that these guidelines apply in situations where credit and financial institutions onboard new customers. This means that the scope is limited to initial customer due diligence processes under Article 13(1) (a), (b) and (c) of the AMLD. The application of remote CDD measures in situations where existing customers acquire new products is outside of the scope of these Guidelines, but many provisions in these guidelines will also be relevant in this context.

- Policies and Procedures. The BSG was of the view that the section on Policies and Procedures could be simplified. They considered that this section was prescriptive, which meant that there was a risk of imposing unnecessary cost and compliance burden for little benefit.

The EBA considers that this section does not introduce new requirements but instead explains how existing requirements apply in the remote onboarding context. To further clarify regulatory expectations, this section was reorganized by merging some of the provisions in the consultation draft with relevant provisions in later sections of the final guidelines.



- Application of simplified due diligence measures. The BSG suggested to clarify which document integrity checks and which identity verification checks should be completed in situations where simplified due diligence can be applied.

The EBA clarifies that the guidance relating to document integrity checks in these guidelines apply to all remote customer onboarding journeys. Nevertheless, in situations where credit and financial situations can apply simplified due diligence, those aspects of the guidelines may be adjusted. In those particular cases, these guidelines should be read in conjunction with paragraphs 4.40 to 4.44 of the EBA ML/TF Risk Factors Guidelines.

- Biometric Data. The BSG suggested to add technical support on how to use biometric data remotely.

The EBA clarifies that technical details of the use of biometric data is outside of the scope of these guidelines. Furthermore, the guidelines do not prevent the use of different forms of biometrics once they are sufficiently unique to be unequivocally linked to a single natural person.

- Authenticity checks: The BSG is of the view that applying liveness detection based on the ML/TF risk of the customer leaves room for different interpretations and might be difficult to implement.

The EBA agrees and clarified that liveness detection should be included in all unattended situations, irrespective of the level of ML/TF risk.

- Attended situations: The BSG considered the requirements for solutions that include interaction with an employee too burdensome, namely on the identification of psychological factors that might characterise suspicious behaviours.

The EBA recalls that customer's behaviour can be an important risk indicator, in line with provision 9.6 of the EBA Risk Factors Guidelines.

- Section on 'Digital Identities': The BSG is of the view that guidelines should not prevent the use of technical solutions that are not electronic identification schemes made available at the national level.

The EBA clarifies that these guidelines clarify that the use of solutions that are not within the scope of the eIDAS regulation is permitted. This is because Article 13(1) (a) of the AMLD states that relevant trust services and other solutions that are regulated, recognized, approved or accepted at a national level might also be used to perform the identification and verification process.



Summary of key issues and the EBA's response

Respondents that contributed to the public consultation were asked to provide their responses to the following questions:

- Do you have any comments on the section 'Subject matter, scope and definitions'?
- Do you have any comments on Guideline 4.1 'Internal policies and procedures'?
- Do you have any comments on the Guideline 4.2 'Acquisition of information'?
- Do you have any comments on the Guideline 4.3 'Document authenticity & integrity'?
- Do you have any comments on the Guideline 4.4 'Authenticity checks'?
- Do you have any comments on the Guideline 4.5 'Digital identities'?
- Do you have any comments on the Guideline 4.6 'Reliance on third parties and outsourcing'?
- Do you have any comments on the Guideline 4.7 'ICT and security risk management'?

In respect of Guideline 4.1, respondents asked the EBA to simplify requirements. They also considered that regulatory expectations were not always clear. The EBA considered that this section does not add additional requirements, instead, it builds on provisions in other ESA guidelines, such as the Guidelines on Internal Governance or ICT Guidelines and clarifies how these provisions apply in the remote customer onboarding context. To clarify expectations, the EBA restructured this section and moved several provisions into other sections of the Guidelines.

In respect of Guideline 4.2, respondents asked which data should be obtained for identification purpose. The purpose of these guidelines is to ensure a robust approach to obtain data, in line with the common principles set in Article 13(1) points(a) and (c) of Directive (EU) 2015/849. It is not to prescribe which documents and data that should be collected during the process. For this reason, the EBA did not amend the guidelines on this point.

In respect of Guideline 4.3 and Guideline 4.4, respondents asked the EBA to align the draft with ETSI TS 119 461 Standards. The EBA agreed to align the draft with ETSI standards where possible and updated the guidelines accordingly.

In respect of Guideline 4.5 (Digital Identities) of the consultation document, respondents asked the EBA to clarify the requirements and the situations that are included under this section. The EBA amended the guidelines to clarify that credit and financial institutions that are using solutions based on electronic identification schemes or issued by qualified trust service providers under the eIDAS Regulation comply with provisions included in the Guideline 4.5 of the consultation version. In those cases, the Guidelines should be read in conjunction with eIDAS Regulation. The use of other solutions such as non-qualified trust services or other solutions that are regulated, recognized, approved, or



accepted at a national level remains possible in line with the Article 13(1) (a) of the AMLD, subject to specific safeguards.

Summary of responses to the consultation and the EBA's analysis

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Feedback on responses to Question 1 (Subject matter, scope and definitions)			
Subject matter and scope of the Guidelines	<p>One respondent asked about the interaction between the requirements of these Guidelines and rules or restrictions issued by state authorities on remote onboarding processes.</p> <p>One respondent suggested that the Guidelines clarify the relationship between the remote onboarding process described in the draft guideline and that set out in the revised version of the Risk Factors Guidelines (EBA/GL/2021/02).</p> <p>Several respondents asked whether the Guidelines should apply to situations where CDD was carried out in a remote manner on existing customers, or whether they should be applied retrospectively to existing remote customer onboarding solutions.</p>	<p>The aim of these guidelines is to ensure that institutions put in place and maintain sound and secure remote customer onboarding processes. They do not override provisions in national law.</p> <p>These Guidelines should be read in conjunction with the Risk Factors Guidelines. They apply specifically to new business relationships but may also be useful in situations where institutions perform remote CDD on existing customers.</p> <p>These guidelines apply in situations where credit and financial institutions adopt a new remote customer onboarding solution and in situations where institutions review remote customer onboarding solutions already in place. The scope of these Guidelines was amended to make this clear.</p>	<p>“(…) These Guidelines set out the steps credit and financial institutions should take when adopting or reviewing solutions to comply with their obligations under Article 13(1) points (a), (b) and (c) of Directive (EU) 2015/849 to, when remote which use remote channels CDD. These solutions are used to carry out performing the initial customer due diligence (CDD) onboard remotely, using remote channels, without physical contact. (…)”</p>
Addressees	<p>Some respondents were confused by the use of the term ‘Financial Sector Operator’.</p> <p>Several respondents suggested that the scope of the Guidelines be extended to other entities, including CASPs.</p>	<p>The addressees of these guidelines are determined by the EBA's scope of action under the EBA's founding regulation CASPs are not currently part of this scope, which means that the Guideline cannot be extended to them.</p>	<p>The expression ‘Financial Sector Operator’ was replaced by ‘credit and financial institution’.</p>
Proportionality	<p>Some respondents considered that the Guidelines are introducing a disproportionate</p>	<p>The guidelines are clear that institutions can adjust the extent of the measures in line with a risk-based approach.</p>	<p>No change</p>

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	number of requirements which consequently will require an increase of time and effort to comply.		
Feedback on responses to Question 2 (Policies and procedures)			
General comments	<p>A respondent proposed introducing safety levels and service certification for IT solutions used for remote customer onboarding.</p> <p>Other respondents suggested that a list of standards and technical specifications should be provided separately from AML/CFT requirements, as they might involve different competent authorities (one which is competent to authorise the remote onboarding solution, and another which is competent for AML/CFT matters).</p>	<p>The ultimate responsibility under AMLD lies with the credit and financial institution and could not be transferred to a third party. This aspect goes beyond the scope of these Guidelines and would be too prescriptive with insufficient legal bases.</p> <p>Although EBA understands that in some countries, remote onboarding solutions must be authorised, it is not the case everywhere. The Guidelines should be relevant for all addressees.</p> <p>There is no official list of relevant standards and technical specifications and these Guidelines do not intend to give prescriptive indications as to how credit and financial institutions are expected to draw up their policies and procedures.</p>	No change
General comments	<p>A respondent noted that, as the internal policies and procedures should be risk-based, either the 'Guidelines on the use of remote customer onboarding' or the 'The ML/TF Risk Factors Guidelines' should be supplemented with the list of potential risk factors concerning the remote-onboarding process for example the behavioural factors concerning the client.</p>	<p>The ML/TF Risk Factors Guidelines set out risk factors that also apply in the remote onboarding context.</p>	No change
Old GL 10 c)	<p>Some respondents considered that the choice of the remote onboarding solution should be the</p>	<p>The Guidelines were amended to clarify that types of customers/services/products covered by the solution</p>	<u>New draft:</u>

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
New GL 9 c)	<p>result of the risk assessment of the business relationship as a whole, and not only of a single factor such as e.g., the product.</p> <p>Some respondents argued that a client risk category is often defined only after the onboarding process is initiated, i.e., when the onboarding solution has already been chosen. They considered that "products and services" should also be removed from the Guideline as customer onboarding is specific to the customers and including all products and services makes it a risk assessment as opposed to a customer onboarding question.</p>	<p>should be clearly identified in the institution's policies and procedures, in line with the institution's business-wide risk assessment.</p>	<p>"the situations where the remote customer onboarding solution can be used, taking into account the risk factors identified and assessed in accordance with Article 8 (1) of the Directive (EU) 2015/849 and in the business-wide risk assessment, including a description of the category of customers, products and services that are eligible for remote onboarding"</p>
<p>Old GL 10 d) New GL 23</p>	<p>Some respondents argued that Guidelines 10 d) and e) might be redundant regarding the concept of "information" that is required to identify the customer and suggest deleting it in Guideline 10 d).</p>	<p>The Guidelines were amended to clarify this point.</p> <p>To simplify the reading, this provision was moved to Section 4.2.</p>	<p><u>New draft:</u></p> <p>In addition to the points set out in paragraph 9, credit and financial institutions should set out in their policies and procedures the information needed to identify the customer, the types of documents, data, or information the institution will use to verify the customer's identity and the manner in which this information will be verified.</p>
<p>Old GL 10 h) New GL 10 d)</p>	<p>A respondent argued that the Guidelines should allow for transactions to be executed even before the identity has been fully verified, as long as some safeguards have been put in place to reduce the risk (very low transactional limit, geographical</p>	<p>The derogations included in Article 14 of the AMLD apply irrespective of the content included in these Guidelines.</p>	<p>No Change</p>

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	<p>limitations, etc.). In the same vein, a respondent claims this Guideline should be deleted, as it is at odds with Article 14(2) AMLD which allows for the verification to be performed after the business relationship has been established.</p>		
<p>Old GL 14 New GL 13</p>	<p>Several respondents requested the EBA to clarify that the requirement to conduct a pre-implementation assessment does not apply to onboarding processes already implemented by the credit and financial institution, prior to the entry into force of this Guideline.</p> <p>Some respondents asked to include an explicit exemption for cases where the remote onboarding solution has been officially approved, recognised, or otherwise accepted by the competent authority or to consider this obligation as part of other general risk management requirements (such as MaRisk, BAIT or the EBA's ICT risk management guidelines).</p>	<p>The Guidelines were amended to clarify expectations regarding the pre-implementation assessment. The use of additional documentation remains possible, including documents made available by the competent authorities or the output of the general risk management requirements, to inform and complement the pre-implementation process.</p>	<p><u>“When considering whether to adopt a new remote customer onboarding solution,</u> Financial credit and financial institutions should carry out a pre-implementation assessment (...).”</p>
<p>Old GL 15 New GL 14</p>	<p>Some respondents asked for further guidance on how letter a) and e) of the list should be measured. In particular, the respondent would like that the expression “completeness and accuracy of the collected data and documents” mentioned in letter a) be more closely defined.</p> <p>Some respondents argued that the requirement under letter e) is difficult to achieve and to measure: the adaptability of the solution(s) to any changes in legal or regulatory requirements may</p>	<p>In accordance with the risk-based approach, credit and financial institutions should define what they consider to be “complete” and “accurate” in relation to their specific CDD measures.</p> <p>The EBA agrees that the requirement in letter e) might be difficult to meet under the pre-implementation assessment and removed this provision.</p>	<p>Provision 15 e) was removed.</p>

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	<p>not be properly assessed in advance without knowing the specific terms of such legislative/regulatory amendment. Likewise, potential consequences of changes in the geographical distribution of services and products cannot take into consideration unpredictable political situations, e.g. the outbreak of a war and/or any further international sanction in a specific geographic area and/or involving a specific geographic area.</p>		
<p>Old GL 19 and 20 New GL 18 and 19</p>	<p>Several respondents cautioned against the risk that the Guideline adopt a too prescriptive and onerous approach, in particular for solutions provided by a qualified trust service provider.</p> <p>Other respondents referred to that this process cannot always be performed by credit and financial institutions due to the fact that in some situations the solution is implemented primarily by the service provider itself.</p>	<p>The Guidelines provide that credit and financial institutions should define in their policy with which frequency and according to which process they intend to carry out ongoing reviews.</p> <p>The ongoing monitoring requirements addressed to credit and financial institutions relate to the quality, completeness, accuracy, and adequacy of the data for CDD purposes, which remains the responsibility of credit and financial institutions.</p>	No change
<p>Old GL 21 New GL 20</p>	<p>Some respondents asked to add new means to carry out the ongoing monitoring as well as to add further guidance on what EBA's expectations are with regard to the examples.</p>	<p>The examples listed in paragraph 21 are not exhaustive and institutions can meet their obligations in other ways.</p>	No change
Old GL 22	<p>Some respondents questioned the rationale for this provision and requested clarifications on the use of external or internal auditors in other sub-processes of the remote customer onboarding process.</p>	<p>External audits do not replace the responsibility of the institution to ensure ongoing effectiveness of the solution it uses.</p>	Guideline removed.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	Some respondents suggested to make the use of external auditors mandatory, since internal audits are not considered sufficiently neutral.		
Feedback on responses to Question 3 (Acquisition of information)			
Old GL 25 New GL 24	<p>Several respondents requested more detail on this Guideline, namely on the data format of the information.</p> <p>One respondent requested to delete the requirement to investigate any connection interruptions because sometimes it is unfeasible, worthless and places redundant responsibility on the credit and financial institution.</p>	<p>Once the conditions set out in this Guideline are fulfilled, the technical details are at the discretion of the credit and financial institution.</p> <p>The EBA agrees with the argument regarding the investigation of connection interruptions and amended this point.</p>	<p>d) any technical shortcomings that might hinder the identification process does not continue if technical shortcomings or, such as unexpected connection interruptions, are detected and investigated.</p>
GL 26	<p>Some respondents requested more detailed information on which data should be obtained for identification purposes.</p> <p>Some respondents asked for more detail regarding data retention periods and encryption policies, as the Guideline makes reference to ‘ex-post verifications’.</p> <p>One respondent requested that it is necessary to specify that the obligations under this provision should lie on the credit and financial institution.</p>	<p>These Guidelines specify which conditions institutions should put in place when obtaining data, in line with the common principles set in Art 13(1) points(a) and (c) of Directive (EU) 2015/849.</p> <p>The GDPR applies, therefore the guidelines do not specify retention periods. In the same vein, references to ‘ex-post verifications’ do not prevent the encryption of data, in line with Article 32 of the GDPR Regulation.</p> <p>The EBA agrees to specify that the obligation to store and time stamp the identification proofs lies with the credit and financial institution.</p>	<p>“(…) should be time-stamped and stored securely by the credit and financial institution. The content (…)”</p>

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
GL 28	Some respondents questioned how the location of the customer can be leveraged during the remote identification and verification process.	The location of the customer might be used to access potential geographical risks, however, it should be the only factor to be taken into account. The guidelines were amended to make this clear.	Editorial amendments.
GL 32	Some respondents suggested to remove references to the nature and purpose of the business relationship as this could generate confusion and could be captured outside of initial customer due diligence.	The risk factors guidelines clarify that initial customer due diligence includes a specific step to identify the purpose and intended nature of the business relationship, in line with Article 13 of the AMLD. The guidelines were amended to make this clear.	Editorial amendments.
Feedback on responses to Question 4 (Document authenticity & integrity)			
GL 33	<p>Some respondents requested to add into the Guidelines 33 the case when credit and financial institution accepts videos of physical identity document.</p> <p>Some respondents indicated that using copies, photos or scans of identity documents during remote onboarding process of customer is not in line with most national requirements, prevailing practise and increases the risk of fraud and ID theft.</p> <p>Some respondents asked for clarification of the sentence “this may include verifying” so that the requirement is not confused with the verification obligation of the AML/CFT requirements legislation.</p>	The EBA agrees and amended the guideline on this point and brought consequential amendments to guidelines 33, 33 a) 33 d).	“Where the credit and financial institutions accept reproductions of the original document paper copies, photos or scans of paper-based documents (...) ”

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
GL 33	Some respondents suggested to add additional security measures during the verification of the identity document to prevent replay attacks.	The EBA agrees and amended the Guidelines accordingly.	New point: “e) that the provided reproduction has not been displayed on a screen based on a photograph or scan of the original identity document.”
GL 35	<p>Some respondents expressed concerns regarding what they interpreted as the mandatory nature of the requirement. These concerns varied from issues concerning the operationalisation of the provision and potential competitive issues due to nature of how NFC chips are accessed on devices</p> <p>Another respondent proposed to clarify that such checking can take place not only against “submitted data and other submitted documents” but also in reliable external, including public, databases.</p> <p>Several respondents suggested that the Guidelines should cross reference ETSI TS 119 461.</p>	<p>The EBA amended this Guideline to clarify that the use of data contained in the chips of the national identity card is not mandatory.</p> <p>The proposal to include the checking of data against reliable external sources is already included.</p> <p>EBA considers ETSI TS 119 461 (Electronic Signatures and Infrastructures Policy and security requirements for trust service components providing identity proofing) a relevant set of standards and agreed to amend the draft of these Guidelines with it, where possible.</p>	Editorial amendments.
GL 37	A number of respondents noted that ETSI TS 119 461 exclusively requires that an authorized type of identification evidence: an official identity document (physical or digital), electronic identification of sufficient quality (level substantial), or a qualified signature should be accepted as main evidence. Other documentation can be used as supplementary evidence only.	<p>Paragraph 4.10 of the Risk Factors Guidelines states that “<i>firms should put in place appropriate and risk-sensitive policies and procedures to ensure that their approach to applying CDD measures does not result in unduly denying legitimate customers access to financial services</i>”.</p> <p>Where credit and financial institutions accept alternative documentation for the purposes of financial inclusion, it is expected that it is done in a</p>	Editorial amendments.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	One respondent stated that remote onboarding should not be possible in the case of customers being accepted as part of financial inclusion.	way which balances the need for financial inclusion with the need to mitigate ML/TF risk. Explicitly excluding such customers from remote onboarding, as per respondent suggestions, would be contrary to the goal of financial inclusion.	
Feedback on responses to Question 5 (Authenticity checks)			
GL 39	Several respondents suggested to add more details, including examples, regarding the use of biometric data, as it is not clear, for example, whether a picture might be considered itself, as biometric data. One respondent suggested that human intervention should be considered when the comparison algorithms are not reliable.	The definition of ‘biometric data’ is aligned with GDPR regulation which also includes the reference to ‘facial images’. EBA recognises the importance of implementing strong algorithms to match the customer’s information with the biometric data, however the level of reliability could be achieved using other mechanisms, not exclusively based on human intervention.	Added in the Guideline: “(..) In situations the solution does not provide the required level of confidence, additional controls should be considered. ”
Old GL 40 and 43 New GL 41	Several respondents argued that references to ‘increased ML/TF risk’ are unclear. Other respondents questioned why liveness detection should only be mandatory in situations with increased ML/TF risk, as this approach is not aligned with ETSI standard TS 119 461. Some respondents requested more guidance on specific procedures in the scope of the liveness detection	EBA amended guidelines 40 and 43 to include liveness detection in all unattended situations (the customer does not interact with an employee of the credit and financial institution to perform the verification process). This guideline does not establish the liveness detection methods that might be used. As stated in guideline 43, it is up to the credit and financial institution to decide whether liveness detection should be performed actively or passively. ISO 30.107 defines several standards for liveness detection	Guideline 40 removed Guideline 43 was amended: “Where credit and financial institutions use unattended remote onboarding solutions in which the customer does not interact with an employee to perform the verification process, photograph(s) as a mean to verify the identity of the customer by comparing it with a picture(s) ”

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		<p>techniques that might be consulted by the credit and financial institution.</p>	<p>incorporated in an official document, they should:</p> <p>a) ensure that the photograph(s) or video (...)"</p>
<p>Feedback on responses to Question 6 (Digital Identities)</p>			
<p>Section on Digital Identities</p>	<p>Some respondents raised concerns about the scope of this section. Other respondents requested clarifications on the concepts used among this section, namely the references to 'digital identity providers' and 'trust service providers'.</p>	<p>Following the feedback received, the EBA agreed to amend this section and clarify the conditions that are met when credit and financial institutions use electronic identification schemes with an assurance level that is substantial or high, or qualified trust service providers.</p> <p>As a result of the above, these Guidelines introduce a final provision to include other solutions such as non-qualified trust services or other solutions that are regulated, recognized, approved, or accepted at a national level. According to the Article 13(1) (a) of the AMLD, the use of such solutions is permitted. However, the EBA is empowered to further specify what level of quality and what security level should be applied - in general - in order to onboard remotely for the purposes of CDD measures under Article 13 of the AMLD, irrespective of which means, process, services or scheme is used. In conclusion, when using non-qualified trust services and those identification processes regulated, recognised, approved, or accepted by the national relevant authority, it should</p>	<p>New section (Compliance with these guidelines where credit and financial institutions use trust services and national identification processes as referred to in Article 13(1) (a) of Directive (EU) 2015/849)</p>

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		<p>be up to the credit and financial institutions to assess and make sure that they still meet the standards established in the EBA guidelines. To ensure a robust approach to remote customer onboarding, the Guidelines set out the safeguards institutions should apply in those cases.</p> <p>Finally, the EBA is aware that the European Commission's proposal to review the eIDAS Regulation and introduce a European Digital Identity Wallet would significantly help overcome the existing fragmentation in this area. However, until the review is finalised and enters into force, the EBA must base its assessment on the existing regulatory framework.</p>	
Feedback on responses to Question 7 (Outsourcing and Reliance on Third Parties)			
<p>Old Section 4.6.1 New Section 4.5.1</p>	<p>Some respondents suggested that Guidelines should be densified in order to provide for lighter/more flexible guidance for intra-group shared services/tools.</p>	<p>The remote customer onboarding processes carried out by intra-group entities should follow the same approach as the other methods of onboarding new customers, therefore, the same principles should be applied. This means that, for example, nothing prevents the use of the pre-implementation assessment carried out by an entity of the group that uses the remote customer onboarding solution by another entity of the group.</p>	No change
<p>Old Section 4.6.2 New Section 4.5.1</p>	<p>Several respondents suggested to include further guidance on sub-outsourcing.</p>	<p>Relevant guidance is contained in the EBA Guidelines on Outsourcing.</p>	No change
Old GL 58 c)	<p>Several respondents noted that the solutions provided by outsourcing providers are usually</p>	<p>The EBA amended the guidelines accordingly.</p>	<p>Ensure that the outsourcing provider request the agreement</p>

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
New GL 48 c)	used by other associates of the provider that require similar services (such as points of entry in a country or governmental authorities) as well. Therefore, requesting the agreement of the credit and financial institutions may cause disturbance in the providers business and the providers will not be willing to contractually bind to this.		inform the credit and financial institutions on any proposed changes of the remote customer onboarding process or any modification made to the solution provided by the outsourcing provider.
Feedback on responses to Question 8 (ICT and security risk management)			
Old GL 61 New GL 51	One respondent proposed to specify the situations where secure protocols and encryption techniques should be used to safeguard the confidentiality, authenticity, and integrity of the exchanged data at rest and in transit (including examples). It was also requested to clarify if this refers to internal or external exchanges; and the meaning of “widely recognised”.	These Guidelines are technology neutral. It is up to the credit and financial institution to ensure that appropriate security measures are implemented. The guidelines were amended in this regard.	“(…) The remote customer onboarding solution should use secure protocols and cryptographic algorithms according to the industry best practices and strong and widely recognised encryption techniques should be used to safeguard the confidentiality, authenticity, and integrity of the exchanged data, where applicable at rest and in transit.”
Old GL 62 New GL 52	One respondent mentioned that the current reference to qualified website authentication certificate can be considered misleading, as service providers following CA/B Forum requirements for issuance of website authentication certificates can achieve same level of assurance.	The Guidelines were amended accordingly.	“Credit and financial institutions should provide a secure access point for starting the remote customer onboarding process, based on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 or for website authentication as referred to in



Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Old GL 63 New GL 53	One respondent highlighted that security mechanisms used to ensure the integrity of the software code and the confidentiality and authenticity of data on a multi-purpose device are desirable but insufficient to protect such authenticity.	The EBA agrees to broaden the scope of this provision. The applicable measures should be implemented on a case-to-case basis addressing both the software and data integrity and reliance. This shall be in result of an adequate security risk assessment as laid down in EBA Guidelines on ICT and security risk management	<p>Article 3(39) of that Regulation. The use of a qualified website authentication certificate provides higher authenticity to the website where the customer can initiate the remote customer onboarding process.</p> <hr/> <p>“(…) Additional security measures should be implemented to ensure the security and reliance of the software code and the collected data, according to the security risk assessment as laid down in EBA Guidelines on ICT and security risk management. A security mechanism should be used to ensure the integrity of the software code and the confidentiality and authenticity of sensitive data.”</p>