EBA/CP/2021/40

10 December 2021

Consultation Paper

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

Contents

1. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 10 March 2022. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the EBA website.

2. Executive Summary

In September 2020, the European Commission published its Digital Finance Strategy[1] for the European Union. This document sets out a strategic objective for digital finance in the EU and identifies priorities and related actions to enable consumers and businesses to benefit from digital finance while also mitigating risks.

One of the Commission's priorities is to address the fragmentation in the Digital Single Market for financial services, with a particular focus on remote customer onboarding. 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 and convergence about what is, and what is not, allowed in a remote and digital context. As a result, supervisory expectations and what financial sector operators do to comply differs across Member States.

The EBA, through its work, confirms that Member States have taken different views on what is permissible in relation to remote customer onboarding. Most Member States set out in their national law, regulation or regulatory guidance provisions in relation to remote customer onboarding. While several Member States take a broad view of the methods financial sector operators can use to onboard remotely their costumers, others have opted for a more restrictive approach. These divergences might be an obstacle fostering innovation and at the same time, they might hamper cross-border provisions of the financial services. The EBA considers that the identification of common criteria to assess whether innovative technology is acceptable in a remote onboarding context will help align different interpretations of the AMLD by Member States.

Following the restrictions on movements imposed by COVID-19, financial sector operators are accelerating the implementation of new methods to onboard customers. Recent technological developments are leveraging this trend as the reliability of the digital tools to identify and verify that the customer is the person that they claim to be is also increasing. It is, however, important to ensure that financial sector operators put in place safeguards to mitigate the ML/TF risks and impersonation fraud risks when performing the initial CDD.

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 financial sector operators should follow when choosing remote customer onboarding tools and what financial sector operators should do to satisfy themselves that the chosen tool is adequate and reliable on an ongoing basis and allows them to comply effectively with their initial CDD obligations. While these Guidelines address initial CDD obligations, they do not prevent financial sector operators from gathering all information needed to perform all CDD obligations at the same time as they are performing initial CDD remotely. These Guidelines are clear that the

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

choice of individual technological solutions is the financial sector operators', to the extent that this is permitted by national law.

Next steps

The draft guidelines are published for a three-months public consultation.

The EBA will finalise these guidelines once the consultation responses have been assessed.

3. Background and rationale

Background

1. In 2020, in the context of the publication of its Digital Finance Strategy[2], the European Commission invited the EBA, in consultation with the other European Supervisory Authorities (ESAs), to develop guidelines "*on elements related to identification and verification for customer remote on-boarding and reliance on customer due diligence (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;

    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 in the context of its 'A Digital Finance Strategy for Europe', and through this request, aims 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 the demanding of digital tools from financial sector operators to onboard their customers remotely. 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 support remote business customer onboarding and wider remote CDD checks.

4. The EBA considers it important for competent authorities and financial sector operators 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 financial sector operators 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 process[3], and included specific guidance on collecting identity's evidence for non-face to face situations in its revised Risk Factors Guidelines[4].

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591

[3] JC 2017 81

[4] EBA/GL/2021/02

Rationale

5. The EBA has a legal duty to prevent the use of the EU's financial system for ML/TF purposes, and a mandate to lead, monitor and coordinate the EU financial sector's fight against ML/TF. Through these guidelines, the EBA aims to achieve a common understanding by competent authorities and financial sector operators on the steps financial sector operators 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 and observe the principle of technological neutrality.

6. This section explains the reasoning behind the provisions in these guidelines.

Interaction with other guidelines

7. 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) 2015/849[5];
- EBA Guidelines on internal governance under Directive 2013/36/EU[6];
- 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) 2015/849[7];
- EBA Guidelines on outsourcing arrangements[8];
- EBA Guidelines on ICT and security risk management[9].

Internal policies and procedures

8. Evidence provided by Competent Authorities suggests that ML/TF risks do not arise exclusively from the use of specific types of remote onboarding solutions. Instead, cases of crystallised ML/TF risk are often due to financial sector operators' failure to put in place sufficient pre-implementation safeguards or take steps to ensure the ongoing reliability and adequacy of their remote onboarding solutions.

9. For this reason, this section sets expectations regarding the controls financial sector operators should put in place when using a remote customer onboarding solution. It also defines the role of

[5] EBA/GL/2021/02
[6] EBA/GL/2021/05
[7] EBA/CP/2021/31
[8] EBA/GL/2019/02
[9] EBA/GL/2019/04

the AML Compliance Officer when putting in place the financial sector operators' remote customer onboarding policies and procedures.

Acquisition of information

10. Guideline 4.2 serves to ensure that the remote process of acquisition of customer data is sound and that it does not impair the financial sector operator's ability to comply with their AML/CFT obligations.

11. For this reason, Guideline 4.2 does not define which information financial sector operators need to fulfil in their initial CDD obligations, but rather the conditions that need to be met when financial sector operators use innovative technologies to on-board customers remotely.

12. Guideline 4.2 also does not set out which information financial sector operators need for individual ML/TF risk assessment purposes. Guidance on those aspects is contained in the EBA Risk Factors Guidelines and applies in the remote customer onboarding context as it does in situations where customers are physically present for onboarding purposes. This guideline does not prevent financial sector operators from gathering such information at the same time as they are performing initial CDD remotely.

Document Authenticity & Integrity

13. The extent to which documentation provided during the remote customer onboarding process is reliable determines what financial sector operators need to do to mitigate potential ML/TF and impersonation fraud risks. Guideline 4.3 sets out the steps financial sector operators should take to satisfy themselves of the veracity of the documentation they have obtained remotely.

Authenticity Checks

14. The methods financial sector operators use to verify that the person is the person that claims to be in a remote customer onboarding environment are one of the key aspects of these Guidelines. While technology may have an important role in this specific step, the financial sector operators should understand the risks and create robust safeguards to ensure the reliability of the verification process.

15. As such, these Guidelines do not favour or discriminate against particular technological solutions through which firms choose to comply with the requirements. Instead, they focus on sound processes that financial sector operators should put in place to mitigate the impersonation fraud risks.

Digital Identities

16. While the eIDAS Regulation[10] introduced some convergence of approaches by defining standards that aim to increase the reliability of the digital representation of natural and legal persons, the use of digital identities particularly in a cross-border environment, remains a challenge as there is no

[10] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/E

requirement for Member States to develop a national digital identity framework and to make it interoperable with the frameworks of other Member States.

17. To address the challenge of identifying reliable digital identity issuers, the European Commission recently proposed the creation of a secure Digital Identity for all European citizens[11]. This could be an important step towards a convergent process at the European level as it would decrease fragmentation among Member States while making the use of digital identities more attractive and safer to the customers.

18. Nevertheless, in the meantime, these Guidelines provide that it is possible for financial sector operators to determine themselves, whether a Digital Identity Issuer is independent and sufficiently reliable to perform the initial CDD process, subject to certain conditions that are set out in these Guidelines, as this is in line with the risk-based approach. In this scenario, financial sector operators are responsible for demonstrating to their competent authority that the digital identity solution used is appropriate and sufficient to ensure the financial sector operator's compliance with its AML/CFT obligations.

Reliance on Third Parties and Outsourcing

19. Reliance on third parties that are obliged entities for CDD purposes is admissible in accordance with Section 4 of Directive (EU) 2015/849. The EBA Risk Factor Guidelines already contain several high-level provisions in that regard. These draft Guidelines complement those provisions by setting out how they apply in the remote onboarding context.

20. Furthermore, the EBA Guidelines on Outsourcing Arrangements contain a detailed set of provisions financial sector operators should consider when outsourcing compliance-related tasks. Those guidelines also apply in the remote onboarding context. There are, however, a number of points financial sector operators should consider that are specific to the remote onboarding context and these are set out in Section 4.6 of these guidelines.

ICT and Security Risk Management

21. These Guidelines clarify several aspects in regard to ICT and Security Risks that are specific to the relation between the customer and the firm under a remote context. Nevertheless, when designing the remote customer onboarding process, financial sector operators should consult EBA Guidelines on ICT and security risk management which provide an extensive set of provisions applicable to this context.

[11] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

4. Draft Guidelines

EBA/GL-REC/20XX/XX

DD Month YYYY

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 1093/2010[12]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the 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/201x/xx'. 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).

[12] 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

5. These guidelines set out the steps financial sector operators should take to comply with their obligations under Article 13(1) of Directive (EU) 2015/849 when performing the initial customer due diligence (CDD) to onboard new customers, using remote channels, without physical contact. It also sets out the steps financial sector operators 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 financial sector operators should put in place in relation to 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 financial sector operators take to comply with their obligations under Directive (EU) 2015/849 in the remote customer onboarding context are adequate and effective.

Scope of application

7. These guidelines apply to financial sector operators when carrying out initial due diligence measures in accordance with Article 13(1) points (a) (b) and (c) of Directive (EU) 2015/849 where customers are onboarded remotely.

Addressees

8. 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.

Definitions

9. 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:

Digital Identity	A material or immaterial unit that contains person identification data, which is used to verify the identity of the user and for authentication purposes in an online service.

Digital Identity Issuer	A third party trusted with the assessment and verification of the authenticity of the credentials or attributes which will serve as basis for the customer's identification.
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.
Impersonation Fraud Risk	The risk that the customer uses another person's (natural or legal) details without the consent or knowledge of the person whose identity is being used.

3. Implementation

Date of application

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

4.1 Internal policies and procedures

4.1.1 Policies and procedures relating to remote customer onboarding

10. Financial sector operators should put in place and maintain policies and procedures to comply with their obligations under Art 13(1) points(a) and (c) of Directive (EU) 2015/849 in situations where the customer is onboarded remotely. These policies and procedures should set out at least:

    a) the features and functioning of the solution(s) financial sector operators will put in place to collect, verify and record information throughout the remote customer onboarding process;

    b) the remote customer onboarding functions and activities that will be carried out or performed by third parties or other outsourcing providers;

    c) which solution might apply to each category of customers, products and services, based on their respective level of exposure to money laundering and terrorist financing ("ML/TF") risks, as identified and assessed in the business-wide risk assessment carried out by the financial sector operators;

    d) the types of documents that are admissible and the information that is necessary to identify the customer and verify their identity;

    e) the information needed to identify the customer and instructions on which information requires verification and the manner in which this information is to be verified;

    f) the level of human intervention required in the remote verification process;

    g) the scope, steps and record keeping requirements of any pre-implementation assessment financial sector operators should carry out before implementing the end-to-end remote customer onboarding solution;

    h) 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 commensurate with the ML/TF risk, have been applied;

    i) the controls in place to monitor, on an ongoing basis, the correct and appropriate functioning of each remote customer onboarding solution(s) and the effective implementation of the remote customer onboarding policies and procedures taking into account the nature, size and complexity of the financial sector operator's business and the level of risks to which the financial sector operator is exposed;

j) 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(s), the associated risks, and of the remote customer onboarding policies and procedures aimed at mitigating such risks.

11. The policies and procedures, when implemented, should enable financial sector operators to ensure compliance with provisions in Section 4.2 to 4.7 of these Guidelines.

4.1.2 Governance

12. In addition to the provisions set out in the Section 4.2.4 of the EBA Compliance Officer GL[13], the AML/CFT compliance officer[14] should, as part of their general duty to prepare policies and procedures to comply with the CDD requirements, prepare remote customer onboarding policies and procedures and ensure that those remote customer onboarding policies and procedures are implemented effectively, reviewed regularly and amended where necessary.

13. In line with the EBA Guidelines on Internal Governance[15], the management body of the financial sector operator should approve remote customer onboarding policies and procedures, and oversee the correct implementation of those remote customer onboarding policies and procedures.

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

14. Financial sector operators should carry out a pre-implementation assessment for the end-to-end remote customer onboarding solution it intends to use. The pre-implementation assessment should be commensurate to the ML/TF risks that the financial sector operator has identified in its business-wide risk assessment.

15. The scope of the pre-implementation assessment process should include at least:

a) an assessment of the adequacy of the solution regarding the completeness and accuracy of the collected data and documents, as well as of the reliability and independence of the sources of information it uses;

b) an assessment of the impact arising from the use of the remote customer onboarding solutionin its business-wide risks, including ML/TF, operational, reputational and legal risks;

[13] 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

[14] In accordance with the Proportionality criteria set out in Section 4.2.2 of the Compliance Officer Guidelines

[15] EBA Guidelines on internal governance under Directive 2013/36/EU and EIOPA Guidelines on system of governance.

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 management[16];

e) an assessment of the level of adaptability of the solution(s) to any changes in legal or regulatory requirements or in the exposure to ML/TF and business-wide risks, including potential consequences of changes in the geographical distribution of services and products;

f) an end-to-end testing of the functioning of the solution(s) for the targeted customer(s), product(s) and service(s) identified in the remote customer onboarding policies and procedures.

16. Financial sector operators should consider the assessment criteria in paragraph 15 to be appropriately met to the extend that the solution includes qualified trust services in accordance with Regulation (EU) 910/2014[17].

17. The assessments should be duly documented and financial sector operators should be able to demonstrate to their competent authority which assessments they carried out before implementation of the remote customer onboarding solution and, more generally, that its use is appropriate in light of the ML/TF risks identified for the types of customer(s), service(s) and product(s) in its scope.

18. The use of the remote customer onboarding solution should only be initiated once the financial sector operator has sufficient assurance that the internal control system allows it to adequately manage the ML/TF risks to which it is exposed and to mitigate any vulnerabilities that may arise from the use of the remote customer onboarding solution(s).

4.1.4 Ongoing monitoring of the remote customer onboarding solution(s)

19. Financial sector operators should carry out ongoing monitoring of the remote customer onboarding solution(s) to ensure that it operates effectively and continues to fulfil its objective. Financial sector operators should describe in their policies and procedures at least:

a) the scope and frequency of the reviews, and the steps to take to check the quality, completeness, accuracy and adequacy of data collected during the remote

[16] EBA/GL/2019/04

[17] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ 257,28.8.2014, p.73).

customer onboarding process, which should be commensurate to the ML/TF risks to which the financial sector operator is exposed to;

b) the circumstances under which ad hoc reviews are triggered, such as, but not limited to cases, where the ML/TF risk exposure of the financial sector operator changes, deficiencies are detected in the course of monitoring, audit or supervisory activities, there is an increase in fraud attempts or when the legal or regulatory framework has changed.

20. Financial sector operators should put in place remedial measures in case of identified weaknesses, additional risks, or systematic errors with material impact on the efficiency and effectiveness of the general remote customer onboarding. These should include, but are not limited to:

a) a review of all affected business relationships, to assess whether sufficient initial CDD has been applied by the financial sector operator in order for the financial sector operator to be compliant with article 13 (1), letter a, b and c) of the AMLD;

b) taking into account the information obtained in the above-mentioned review, an assessment of whether (i) any affected business relationships should be terminated and/or the execution of transactions within the affected business relationships should be limited or stopped (ii) any Suspicious Transaction Reports should be filled or (iii) changes in the risk profile of affected customers are needed.

21. To carry out the ongoing monitoring of the remote customer onboarding solutions, financial sector operators should consider one or more of the following means, but are not limited to:

i) quality assurance testing;

ii) automated critical alerts and notifications;

iii) regular automated quality reports;

iv) sample testing;

v) manual reviews.

22. Where relevant, financial sector operators should consider the use of internal or external auditors to perform ongoing monitoring activities.

23. The use of a fully automated remote customer onboarding solution, which is highly dependent on automated algorithms, without or with little human intervention, does not exempt financial sector operators from their duty to carry out ongoing monitoring of the reliability and adequacy of the solution.

24. The review findings should be duly documented and financial sector operators 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 they have identified throughout the lifetime of the remote customer onboarding solution.

4.2 Acquisition of information

4.2.1 Identifying the customer

25. Where financial sector operators do not resort to digital identity issuers to identify the customer, as set out in Section 4.6 of these Guidelines, they should ensure that:

    a) the information obtained through the remote customer onboarding solution is up-to-date and adequate to meet the 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 images, video, sound and data are stored according to GDPR Regulation[18] and remain available to the financial sector operator;

    d) any technical shortcomings that might hinder the identification process, such as unexpected connection interruptions, are detected and investigated.

26. The identification proofs 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. The content and the quality of stored records, including pictures and videos, should be available in a readable format and allow for ex-post verifications.

4.2.2 Identifying Natural Persons

27. Financial sector operators should determine in their policies, as set out in Section 4.1.1 paragraph 10, the information they need to obtain in order to identify customers remotely. In addition, financial sector operators should define what information (i) is manually entered by the customer (ii) is automatically captured from the documentation provided by the customer and, (iii) is gathered using other internal or external sources.

28. Financial sector operators should have appropriate mechanisms in place to ensure the reliability of the information automatically retrieved, referred in the previous paragraph, and apply controls to address associated risks. This also includes situations where location

[18] Regulation (EU) 2016/679

data such as Internet Protocol (IP) addresses can be spoofed or services such as Virtual Private Networks (VPNs) used to obfuscate the location of the customer's device.

4.2.3 Identifying Legal Entities

29. Where financial sector operators remotely onboard customers that are legal entities, they should define in their policies and procedures, as set out in Section 4.1.1 paragraph 10, which category of legal entities it will onboard remotely, taking into account the level of ML/TF risk associated with that category.

30. Financial sector operators should ensure that the remote customer onboarding solution(s) has features to collect:

    a) all relevant data and documentation to identify and verify the legal person and to verify that the natural person they are dealing with is legally entitled to act on behalf of the legal entity;

    b) the information regarding the beneficial owners in accordance with provision 4.12 of the EBA Risk Factor Guidelines[19].

31. For the natural persons who are acting on behalf of legal persons, financial sector operators should apply the identification process described in the Section 4.2.2.

4.2.4 Nature and purpose of the business relationship

32. Financial sector operators should implement specific steps during the remote customer onboarding process to obtain information on the purpose and intended nature of the business relationship in accordance with the provision 4.38 of the EBA Risk Factor Guidelines. In particular, they should take risk-sensitive steps to gather information from their customers to identify the nature of their personal, professional or business activities and expected source of funds, and verify the accuracy of this information as necessary.

4.3 Document Authenticity & Integrity

33. Where the financial sector operators accept paper copies, photos or scans of paper-based documents in the course of remote customer onboarding without having the possibility to examine the original identification document, they should take steps to have sufficient assurance as to the reliability of the copy provided. This may include verifying:

    a) if the copy, photo or scan reproduces security features embedded in the original document and if the specifications of the original document that are being reproduced by the copy are valid and acceptable, in particular, type, size of

[19] EBA/GL/2021/02

characters and structure of the document, by comparing them with official databases, such as PRADO[20];

b) that no alteration of the personal data in the document has been attempted;

c) 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) that the copy, photo or scan of the identification document is of sufficient quality and definition so as to ensure that relevant information is unambiguous;

e) where applicable, that the picture of the customer embedded in the document was not replaced.

34. Where financial sector operators use features to automatically read information from documents, such as Optical Character Recognition (OCR) algorithms or Machine Readable Zone (MRZ) verifications, those tools should be sufficient to ensure that information is captured in an accurate and consistent manner.

35. In situations where the customer's own device allows the collection of relevant data, for example the data contained in the chip of a national identity card, financial sector operators should use this information to verify the consistency with other sources, such as the submitted data and other submitted documents.

36. Where available, during the verification process, financial sector operators should verify the security features embedded in the official document, if any, such as holograms, as a proof of their authenticity.

37. Financial sector operators should refer to para 4.10 of the EBA Risk factor Guidelines when accepting alternative documentation for the purposes of financial inclusion. This may include carry out additional controls or increase human intervention to verify the reliability of non-traditional forms of identity documentation.

4.4 Authenticity Checks

38. Remote customer onboarding solutions implemented by the financial sector operators should, as a minimum, allow them to verify the validity of official documents issued by a public authority as part of their remote verification process to ensure:

a) that the identity of the customer coincides with the person previously identified, in cases of natural persons;

[20] https://www.consilium.europa.eu/prado/en/prado-start-page.html

b) that the legal entity has the right to conclude contracts and it is established in its respective jurisdiction;

c) the natural person that represents a legal entity is entitled to act on behalf of such entity.

39. Where the remote customer onboarding solution involves the use of biometric data to verify the customer's identity, financial sector operators should make sure that the biometric data have enough uniqueness to be unequivocally referable to a single natural person. Financial sector operators should verify the unambiguous match between the biometric data indicated on the submitted identity document and the customer being onboarded.

40. Where the ML/TF risk associated with a business relationship is increased, financial sector operators should use remote verification processes that include liveness detection procedures examining whether the video, picture or other biometric data captured during the remote customer onboarding process belong to a living person present at the point of capture, or real-time videoconference.

41. In case of legal entities, financial sector operators should verify the identity and the information provided in the documents and attributes reviewed as part of the identification process, through a reliable and independent source of information such as public registers, where available.

42. 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 discontinued and redirected, where possible, to a face-to-face verification, in the same physical location.

43. Where financial sector operators use photograph(s) as a mean to verify the identity of the customer by comparing it with a picture(s) incorporated in an official document, they should:

a) ensure that the photograph(s) is taken under proper lighting conditions and that the required properties are captured with absolute clarity;

b) ensure that the photograph(s) is taken at the time the customer is performing the verification process. This may be achieved by using a dynamic photograph, multiple photo shots under different angles or another similar method;

c) perform liveness detection verifications, which may include procedures where a specific action from the customer to verify that he/she is present in the communication session or it can be based on the analysis of the received data and does not require an action by the customer;

d) in the absence of human verification, use strong and reliable algorithms to verify if the photograph(s) taken match with the pictures retrieved from the official document(s) belonging to the customer or representative.

44. Where financial sector operators use a video conference as a mean to verify the identity of the customer, 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 staff 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.

45. Where possible, financial sector operators should use remote customer onboarding solutions that include randomness in the sequence of actions to be performed by the customer for verification purposes. Where possible, financial sector operators should also provide random assignments to the employee responsible for the remote verification process to avoid collusion between the customer and the responsible employee.

46. In addition to the above, and where appropriate to the ML/TF risk presented by the business relationship, financial sector operators should use of one or more of the following controls:

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.

47. Where financial sector operators resort to digital identity issuers to identify and verify the customer, which are qualified trust services in accordance with Regulation (EU) No 910/2014, or to any other digital identity issuer regulated, recognised, approved or accepted by the relevant national authorities as referred to in Article 13(1)(a) of Directive (EU) 2015/849, paragraphs 38 to 45 should not be applied.

4.5 Use of Digital Identities

48. When using a digital identity other than by using qualified trust services in accordance with Regulation (EU) No 910/2014, financial sector operators should use a Digital Identity Issuer with a similar level of assurance as to the level substantial or high as in relation to trust services under Regulation (EU) No 910/2014, which are in particular, similar in relation to reducing substantially the risk of impersonation, misuse or alteration of the identity.

49. When using digital identities to perform the identification and verification process, financial sector operators should identify the risks involved in the authentication and set out in their policies and procedures specific mitigation measures especially with regard to impersonation fraud risks.

50. In order to assess whether to use a digital identity issuer other than relevant trust services in accordance with in Regulation (EU) No 910/2014 or those regulated, recognised, approved or accepted by the relevant national authorities to verify and identify their customers, financial sector operators should:

    a) determine the level of assurance based on the elements of technical specifications and procedures outlined in the Annex to Regulation (EU) 2015/1502[21];

    b) take adequate measures to understand the digital identity system based on its technical specifications, architecture and governance;

    c) determine the reliability and independence of the digital identity issuer.

51. Financial sector operators should ensure that when the customer is onboarded using their digital identity this occurs in a secure environment, and, where possible, strong authentication is applied when verifying their digital identity.

52. Financial sector operators should take steps to minimize the risk that the customer's identity is not the claimed identity, taking into account at a minimum the risk of lost, stolen,

[21] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

suspended, revoked or expired identity evidence, including, as appropriate, tools to detect and prevent the use of identity frauds.

53. When electronic certificates are used, financial sector operators should check if the certificates are valid and from a trusted source. In addition, the signed certificate should be used to sign any contract established with the customer. Any contract should be timestamped electronically as the proof of date when the contract is signed.

54. Financial sector operators should take steps to minimize the risk that the customer's identity is not the claimed identity, taking into account at a minimum the risk of lost, stolen, suspended, revoked or expired identity evidence.

55. Where the Digital Identity does not provide sufficient information to perform the identification and verification process, financial sector operators should take adequate measures to autonomously collect customer's additional data in order to adequately complete the process.

4.6 Reliance on third parties and outsourcing

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

56. Where financial sector operators rely on third parties in accordance with Chapter II, Section 4 of Directive (EU) 2015/849 to meet the initial CDD requirements, they should in addition to the EBA Risk Factor Guidelines[22], in particular to guidelines 2.20 to 2.21 and 4.32 and 4.37 of those Guidelines, 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, or equivalent, to, those laid down in the financial sector operator's own CDD policies and procedures;

    b) ensure the continuity of the business relationships established between the customer and the financial sector operator to guard against events that might reveal shortcomings on the remote customer onboarding process carried out by the third party.

57. The use of digital identities issued by third parties to perform the initial CDD process in full or in parts, should not be considered as reliance under this Section, however, financial sector operators should apply, in particular, Section 4.5 of these Guidelines.

[22] EBA/GL/2021/02

4.6.2 Outsourcing of CDD

58. Where financial sector operators outsource all or parts of the remote customer onboarding to an ourtsourcing provider, as referred to in Article 29 of Directive (EU) 2015/849, financial sector operators should apply - in addition to the EBA Risk Factor Guidelines, in particular to guidelines 2.20 to 2.21 and 4.32 and 4.37 of those Guidelines, and, in addition to EBA Guidelines on Outsourcing[23] where applicable -, before and during the business relationship with the outsourcing provider, the following measures, the extent of which should be adjusted on a risk-sensitive basis:

    a) ensure that the financial sector operator's remote customer onboarding policies and procedures are effectively implemented by the outsourcing provider 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 outsourcing provider is suitable to perform the remote customer onboarding process. This may address, but is not limited to, the assessment of staff training, technology fitness and propriety and data governance, at the outsourcing provider;

    c) ensure that the outsourcing provider request the agreement of the financial sector operators on any proposed changes of the remote customer onboarding process or any modification made to the solution provided by the outsourcing provider.

59. Where the outsourcing provider stores customer's data, including, but not limited to, photography, videos and documents, during the remote onboarding process, financial sector operators should ensure that:

    a) only necessary customer's data is collected and stored 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.

60. The use of digital identities to perform the initial CDD process in full or in parts, should not be considered as outsourcing under this Section, however, financial sector operators should apply, in particular, Section 4.5 of these Guidelines.

4.7 ICT and security risk management

61. Financial sector operators should identify and manage their ICT and security risks related to the use of the remote customer onboarding process, including where financial sector

[23] EBA Guidelines on outsourcing arrangements.docx (europa.eu)

operators rely on third parties or where the service is outsourced, including to group entities.

62. In addition to complying with requirements set out in the applicable EBA Guidelines on ICT and security risk management [24], financial sector operators should use secure communication channels to interact with the customer during the remote customer onboarding process. Secure protocols and strong and widely recognised encryption techniques should be used to safeguard the confidentiality, authenticity and integrity of the exchanged data at rest and in transit.

63. Financial sector operators should provide a secure access point for starting the remote customer onboarding process. The use of a qualified website authentication certificate provides higher authenticity to the website where the customer can initiate the remote customer onboarding process. The customer or representative should be informed about all applicable security measures to ensure a secure use of the system.

64. Where a multi-purpose device is used to perform the remote customer onboarding process, a secure environment should be provided for the deployment and usage of the software code on the side of the customer, where applicable. A security mechanism should be used to ensure the integrity of the software code and the confidentiality and authenticity of sensitive data.

[24] EBA/GL/2019/04

5. Accompanying documents

5.1 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 financial sector operators 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 financial sector operators 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

A. Problem identification

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

In cases where FSOs 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 FSOs.

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 financial sector operator 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 financial sector operators, 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 financial sector operators, 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 market[25]. This allows the FSO 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

[25] 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 FSO	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 financial sector operators 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 FSOs can take into account the assessments conducted under the eID solutions notified under eIDAS. In this regard, when resorting to certified digital identity issuer, financial sector operators should take into account the assessment already performed by the national competent authority.

3. Verification Process: Liveness detection

A. Problem identification

When FSOs are not using digital identities, the guidelines set out how financial sector operators 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 financial sector operators do not resort to live videoconference, financial sector operators 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 AML high risk cases only

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 2nd option requires the use of liveness detection only in high ML/TF risk cases when financial sector operators do not resort to digital identity issuers to identify and verify the customer. 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 liveliness detection in high risk cases only (Option 2). It is important to define criteria for situations 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. Digital identities

A. Problem identification

The digital representation of a person and their attributes and credentials to authenticate and proceed with the Remote Customer On-boarding process (digital identity) is a key topic in the remote on-boarding context considering the associated benefits for customers and firms, such as the interoperability and the possibility to enhance the CDD process.

The 5th AML Directive amends the 4th AML Directive to explicitly recognize eID under eIDAS as a valid solution to identify customers, and, more importantly, as a way to secure non face-to-face business relationships.

However, the provisions in Article 13(1)(a) of the AMLD, which refers to 'any other secure, remote or electronic identification process regulated, recognised, approved or accepted by relevant national authorities' could be interpreted in different ways.

B. Policy objectives

These guidelines aim to create a common understanding of these provisions, while ensuring a secure and remote way of identification of customers

C. Options considered

Option 1: The Digital Identity Issuer under the eIDAS regulation

Option 2: Digital Identity Issuers identified by the designated national competent authorities

Option 3: Digital Identity Issuers determined by the firms themselves, subject to certain conditions that would be set out in the guidelines.

D. Cost-benefit analysis

Under Option 1, the Digital Identity Issuer should be considered as "*an independent and reliable source"* only if it was recognised by the national regulators under the eIDAS regulation[26]. Adopted in 2014, it provides the basis for cross-border electronic identification, authentication and website certification within the EU. eIDAS-based eIDs offer the possibility of a strong authentication of users (both natural and legal persons), based on ID information endorsed by governmental authorities across EU. Under eIDAS, a qualified electronic signature issued by a trusted service provider established in one EU member is valid throughout the Union. This approach is most reliable as it ensures a centralised and uniform approach to identifying such issuers. Already about 60% of Europeans can benefit from the current system.[27]Although the signature part of eIDAS has worked well, the broader eID part of the scheme to trust each other's credentials needs improvement. For example, there is no requirement for Member States to develop a national digital ID and to make it interoperable with the ones of other Member States, which leads to high discrepancies between countries.

While eIDAS regulates the acknowledgement of eIDs across borders, it does not harmonize the approach to certification of trusted service providers, but rather sets a minimum harmonization. This aspect therefore differs significantly across MSs. Many governments have felt little incentive to expand resources, given tight budgets and varying priorities. Almost all progress concerns government services, and the private sector mostly has not embarked on the project as was expected. [28]

[26] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN

[27] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

[28] CEPS (2020), "Europe's Digital Identification Opportunity", accessed at: https://www.ceps.eu/wp-content/uploads/2020/06/TFR_Europe-Digital-Identification-Opportunity.pdf

Moreover, the digital identities under the eIDAS were not designed with the private sector, and specifically financial sector in mind, and currently the attributes covered there under the minimum harmonization, are not sufficient for CDD processes as required under AMLD.

In its latest eGovernment benchmark[29], the European Commission noted the online availability of digital public services to foreign users or in a cross-border scenario is lagging behind expectations. One of the key obstacles for the cross-border use of digital public services are problems with access to procedures requiring authentication. Foreign national eIDs are accepted for only 9% of the services that citizens can access with a domestic eID. This indicates that the cross-border acceptance of eIDs still requires investments by the EU27+.

Due to these drawbacks, Option 1 should be targeted as a solution in the long-term, as it is expected that that the harmonization under the European Digital Identity (EUD) EU Digital Identity initiative will finally solve the problems on fragmentation. In the meantime, however, a more flexible approach may be desirable.

Under Option 2, the designated national competent (AML) authorities would be responsible for identifying those Digital Identity Issuers that could be used by the FSOs to perform the verification and identification process (even when not complying eIDAS Regulation). This approach is more flexible compared to Option 1, however it also puts a big burden on the regulators and requires specific expertise that very often the regulators do not have.

Finally, under Option 3, the FSOs would have the ability to determine themselves, whether a Digital Identity Issuer independent and reliable to support the initial CDD process, subject to certain conditions that would be set out in the guidelines. Under this scenario, FSOs would be responsible for demonstrating to their competent authority that the digital identity solution used is appropriate and sufficient to ensure the FSO's compliance with its AML/CFT obligations.

E. Preferred option

EBA staff consider that the third solution (Option 3: Digital Identity Issuers determined by the FSOs themselves, subject to certain conditions that would be set out in the guidelines) is in line with the risk-based approach.

[29] https://digital-strategy.ec.europa.eu/en/library/egovernment-benchmark-2020-egovernment-works-people

5.2 Overview of questions for consultation

1. Do you have any comments on the section 'Subject matter, scope and definitions'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

2. Do you have any comments on Guideline 4.1 'Internal policies and procedures'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

3. Do you have any comments on the Guideline 4.2 'Acquisition of Information'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

4. Do you have any comments on the Guideline 4.3 'Document Authenticity & Integrity'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

5. Do you have any comments on the Guideline 4.4 'Authenticity Checks'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

6. Do you have any comments on the Guideline 4.5 'Digital Identities'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

7. Do you have any comments on the Guideline 4.6 'Reliance on third parties and outsourcing'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

8. Do you have any comments on the Guideline 4.7 'ICT and security risk management'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.