EBA/CP/2021/40

BSG 2022 010

Deadline: 10 March 2022

BANKING STAKEHOLDER GROUP

EBA Consultation Paper: draft Guidelines on Remote Customer Onboarding under Article 13(1) of Directive (EU) 2015/849

EBA is consulting on draft guidelines on how sound, risk-sensitive initial customer due diligence can be carried out remotely, in the light of the Commission's request in its Digital Finance Strategy to ensure that there are not undue barriers to remote customer onboarding, increased demand for remote onboarding during the pandemic, and differences in practice between member states that EBA has identified in its preparatory work. The BSG is grateful for the opportunity to comment on these proposals.

The COVID-19 pandemic has indeed been a catalyst for further digitalisation. Consequently, expectations concerning both the convenience and high security for any online activity such as remotely opening a bank account or applying for a loan have matured. The BSG acknowledges therefore the importance of a proper onboarding process with better user experience while ensuring the same level of security as face-to-face onboarding processes. Expectations are high that the forthcoming European digital identity (Commission proposal for a regulation establishing a framework for a European Digital Identity) will make it possible to improve even further remote customer onboarding. In the meantime, it appears essential to provide clarity and convergence at EU level on what is, and what is not allowed in a remote and digital context.

Several guiding principles have informed our response to the consultation and it may be helpful to articulate these here:

- We consider that it is in the interests of both consumers and institutions to find solutions that enable remote customer onboarding given the potential it may bring for improved convenience, customer service, access for those with limited mobility and lower costs.

- We consider that the underlying responsibility for financial institutions in relation to the effectiveness of their AML controls remains the same, whether onboarding is conducted in person or remotely. As such, it is important to ensure that the guidelines recognize that decisions about any onboarding process, whether in-person or remote involve an assessment of risk and strategies

to manage it. In-person approaches to identity verification are not risk-free. Remote approaches should be held to the same, but not a higher standard.

- Procedures within a financial institution for determining, executing and recording choices about customer onboarding processes should be very similar whether the final result is an in-person, remote or hybrid approach. We consider that the important thing in each case is to be aware of the strengths and limitations of the techniques used, consider how limitations can be mitigated, and ensure that the overall result is sufficiently robust while still meeting the needs of customers. As such, we would expect guidelines on remote onboarding specifically to focus more on the assessment of different techniques available than on aspects of internal policies and procedures that should be equally applicable to in-person and remote customer on-boarding.

- We recognize that where effective e-ID schemes are available these play a significant role in reducing AML-related risks in customer on-boarding. In some Member States these are already widely used, even if not necessarily by non-nationals, and we hope this will in time be the case across the Union. However, in the meantime, we think it is important to make the most of other techniques that are available where e-ID is not and hope that the guidelines in their final form will support this outcome.

In our response, we have focused specifically on the AML checks which are required to be carried out as part of customer onboarding, and how those may operate remotely. However, it is important that EBA and competent authorities continue to consider the broader customer on-boarding process, including in digital environments where customer behavior and preferences may be different than in other contexts, and the wider customer protection implications of this.

Q1: 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.

Scope

We would ask EBA to clarify whether the guidelines also relate to the provisions in Art 13(5) of the AMLD on CDD for beneficiaries of investment-related life and other insurance and explain the reasoning either way.

It should be noted that during the course of the customer relationship, there may be additional situations in which the using of the remote channels may come to question (e.g. customer request new products, financial sector operator carries out ODD measures). In addition to the initial CDD (onboarding), clarification would be needed whether the Guideline is meant to provide guidance also in other situations (not only initial CDD).

Definitions

The digital identity definition does not personalise the user (e.g. customer). However, the "Digital Identity Issuer" definition refers to "the customer's identification". We therefore suggest changing the definition of "Digital Identity Issuer" to, for example, "the user's identification".

In the Draft Guideline, Impersonation Fraud Risk is defined as follows: "*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." However, it may not be only the customer who uses another person's details, but, for example, the customer's representative or another third party. We therefore suggest changing the word "customer" to an alternative such as "a person".

Wherever possible, definitions used in this section should be consistent with those used in existing or planned EU legislation, for example GDPR.

Q2: 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.

The BSG agrees that customer onboarding by financial institutions - whether remote or otherwise – should be governed by clear policies and procedures, and decisions about those processes informed by an assessment of the level of risk, and the effectiveness of the proposed approach at mitigating that risk, while also providing an appropriate service to customers.

However, we have two significant concerns about this section.

1) The procedural requirements are very prescriptive. It is not clear why this level of prescription is necessary to deal with issues specific to remote customer onboarding, how it is intended to relate to procedures for determining in-person CDD, and whether it allows for appropriate tailoring to risk given the range of institutions and activities in relation to which the guidelines will be used. We would suggest that it would be more beneficial to simplify this section and focus on what is specific to carrying out onboarding remotely – namely assessing and deciding how to ensure that the techniques used for remote onboarding are appropriately robust. Otherwise, there is a risk of imposing unnecessary cost and burden for little benefit.

2) We are concerned that there appears to be an assumption that a higher standard needs to be met before remote onboarding is justified relative to in-person onboarding. We think it is important to recognise that there will always be risk in any onboarding process and judgements to be made about how to manage them. Specifically, we are concerned that the drafting proposed in 4.1.3 (18) is too strong: there will always be vulnerabilities, just as there are with in-person checks, so requiring an operator to 'mitigate any vulnerabilities' before using remote means is too onerous a test and likely to disincentivize adoption of remote methods and reduce access for customers.

Q3: Do you have any comments on 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.

This section of the draft guideline is less detailed and less helpful to financial institutions as regards the types of acceptable innovative technologies and acceptable forms of digital documentation, of which both were part of the original EU Commission request. This is understandable given the very differing situations across the EU. However, financial institutions would welcome clearer guidance of what is acceptable and not when onboarding a customer remotely for ID&V purposes.

Different countries set different requirements for recordkeeping of KYC information and the required level of detail varies. We therefore suggest modifying paragraph 26 to clarify that the records required

to be retained may not necessarily include pictures and videos, but where they do we agree these need to be available in readable format and allow for ex-post verification. This could be achieved by adding ”including **where applicable** pictures and videos”.

It would be helpful if 4.2.2 could be amended to reflect the fact that natural persons may also have representatives. (We note that natural persons who represent legal persons are covered in paragraph 31.)

It would be helpful to consider and clarify whether any adjustments are needed/permissible for PSP business models which do not involve the opening of a customer account.

Q4: Do you have any comments on Guideline 4.3 ‘Document Authenticity and 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.

We recognise that there can be risks to the authenticity of documents verified remotely and we therefore welcome the inclusion in these Guidelines of factors that can be used to mitigate these risks where ‘physical’ documents need to be used remotely as proof of identity. However, we would also ask EBA to consider whether reference could be made to other technologies for creating, communicating and receiving/reading official ‘certification’ which, where available, may reduce the need for reliance on scanning of documents.

We welcome the cross-reference to techniques which can be used to facilitate onboarding in a way that assists financial inclusion.

We also have the following specific points:

- Paragraph 33: we suggest to change the word in the sentence “This may include verifying” into e.g. “ensuring”, “examining” or “reviewing” so that the requirement is not confused with the verification obligation of the AML legislation and add additional requirements to the financial sector operators;

- Paragraph 33 a): it would be helpful to clarify what happens in situations in which the information cannot be compared with official databases in the absence of such databases;

- Paragraph 33 b): the document may include information that is not necessary for the CDD purposes and may include e.g. personal data that is not necessary. Therefore, it should be allowed to redact some part of the document when the redaction is assessed to have an acceptable reason and does not relate to the specific data relied on for the AML assessment.

We would welcome clarification in this section of how document integrity checks could be proportionately reduced in cases where simplified due diligence is permissible.

Q5: Do you have any comments on 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.

The BSG would like to highlight that for private corporates verifying validity of official documents issued by a public authority by checking against public registers as e.g. indicated in paragraphs 38 and 41 is problematic, not to say impossible, as regards nationals and corporates in other countries. The identification part will hopefully change in a positive direction with the recent EU Digital Identity proposal. However, the lack of access to relevant registries and data bases in another country remains.

We take the view that also national governments need to provide documents that are sufficiently verifiable and reliable in order for financial sector operators to fulfil the minimum requirements.

Regarding paragraph 38(c), we wish to highlight that assurance of representation (mandate or entitlement to act) is subject to variations across local jurisdictions, depending on the situation and specific role at hand (i.e. general agents or lawyers). We thus suggest that any mandate or entitlement to act may be assured in accordance with common practices and rules of the jurisdiction in question.

Paragraph 39 concerns the use of biometric data. The BSG would welcome more technical support on how to do this remotely.

Regarding the use of biometrics in addition to video identification, we note that the Portuguese legal framework requires (regardless of the level of risk) financial institutions to have a person, in real time, validating the client's identity. In terms of level playing field this is not very helpful, as it is an extra cost that banks have to support if they want to offer new remote onboarding solutions.

National experiences - Portugal

Under the legal and regulatory framework in force [cf. Law No. 83/2017, of August 18 (Law no. 83/2017), Bank of Portugal Notice no. 2/2018, of 26 September (Notice no. 2/2018) and Circular Letter No. 44/2020, of July 7, 2020 (Circular Letter No. 44/2020)], there are only two digital onboarding methods available in Portugal:

1) via Digital Mobile Key (CMD)
Onboarding via CMD is, of course, only accessible to CMD adherents. In spite of the growth of the adhesions to the CMD, the penetration levels of the solution are still limited. This might be because it is not very user-friendly and several steps have to be followed.

2) via videoconference
Onboarding via videoconference implies scheduling a video call, the presence of a certified operator and compliance with a set of technical requirements (e.g., carrying out in real time and without interruptions or pauses, adequate sound and image quality, in order to allow the identification of the security elements and characteristics of the documents of identification). In the current scenario, such a universe of requirements do not allow availability (24/7), scalability and it increases operating costs associated with opening an account.

This reality in Portugal contrasts with the base-line option guideline contained in the EBA's proposed guidelines on remote onboarding (page 31-32) and principle-rule contained in §40 of the proposed GLs under consultation and which establishes "liveness detection" as an alternative method.

Furthermore, there are other methods in the European digital space, that are considered in these guidelines, that provide a more convenient customer journey, namely:

- Validation of identity a posteriori: Currently, some of the banks that operate in Portugal under the passporting regime use an onboarding process that involves the validation of the customer's identity a posteriori. The solution in question involves mobile phone verification, filling in customer data (name,

date of birth and address), email verification, capturing the photo on the front and back of the ID document and capturing a selfie. Subsequently, the client's identity is verified. The mechanism for proving the customer's identity is based on validating the capture of the identification card (both sides) and the customer's facial image (as proof of life). This mechanism, in addition to allowing the extraction of data from the citizen's card, validates its authenticity, namely if the photo matches the customer's facial image, among other validations.

- Real-time Identity Validation: Liveness detection, an anti-spoofing technology, and facial detection are examples of other solutions that have been adopted in banking onboarding processes in other geographies to automate the customer's identity verification mechanism, with a high level of quality of identification.

From the point of view of competition and innovation, the current legislative and regulatory reality places banks operating in Portugal under the passporting regime in a more favorable position, as they are able to offer a more frictionless account opening experience and, at the same time, are able to capture efficiency benefits. The processes adopted by these operators when opening an account at a distance have the following advantages compared to the processes that can be used by Portuguese banks (i) faster and simpler, (ii) less personal data requested, without a pre-contractual phase, no obligation to open documents, no scroll-down, no video call for ID confirmation (only photo ID and selfie), no digital signature.

It is therefore important to evolve towards establishing a technologically neutral regulatory framework that provides a level playing field for all banks in the European space.

As far as the consumer is concerned, the new solutions increase the range of alternatives and improve the user experience by simplifying the process and shortening the journey time.

Paragraph 40 prescribes certain measures "where the ML/TF risk associated with a business relationship is *increased*", which leaves room for interpretation. Existing AML/CFT legislation applies the terms lower and higher ML/TF risk, subject to 'simplified' and 'enhanced' measures respectively, but it is common for financial institutions to have medium or normal risk as well. Increased risk may be interpreted as all situations except in lower ML/TF risk or situations or only in situation of higher ML/TF risk. We thus suggest to use the term 'enhanced' to clarify the scope.

Paragraph 44(c) mandates financial institutions to "*develop an interview guide defining the subsequent steps of the remote verification process as well as the actions required from the employee" which "should include guidance on observing and identifying psychological factors or other features that might characterise suspicious behaviour during remote verification."* This adds to the already burdensome requirements in this guideline and by national competent authorities and seems overly cumbersome also in combination with 44(b) which mandates staff to be sufficiently trained on the same issues. As currently drafted, paragraph 44(c) does not appear to reflect the requirement proposed in paragraph 45 to include an element of randomness in the sequence of actions.

Regarding paragraph 46, the BSG proposes to add "*or similar measure*" to give sufficient flexibility in the controls to be applied.

We would welcome clarification in this section of how the authenticity checks could be proportionately reduced in cases where simplified due diligence is permissible.

Q6: Do you have any comments on 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.

As regards the use of Digital Identities, the BSG notes that even with nationally acceptable Digital Identities, not all national competent authorities consider them as sufficient and thus require additional measures to be performed. In combination with the substantial requirements on policies and procedures, remote onboarding of customers will not be encouraged.

In Portugal there is a fully operational mobile eID solution, Chave Movel Digital which allows for authentication. It is one of the technological means that has to be made available to customers for the identification and due diligence procedures associated with the establishment of a business relationship, as in the procedures for updating the identification. However, the reality is that it is a technology that is currently not widely used by society. This means that it is important to allow for other techniques to be used for remote onboarding alongside mobile eID solutions at least until uptake of e-ID, which currently varies significantly across member states, is consistently higher.

Q7: Do you have any comments on 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.

The BSG has no specific comments on this section. However, we note that the proposed guideline adds to the already existing complexity in regulatory requirements as regards reliance and outsourcing. Clarification would be needed to understand why the use of digital identities should not be considered as outsourcing as set out in the paragraph 60.

Q8: Do you have any comments on 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.

The BSG fully agrees that ICT and security risk is of the utmost importance, also in situations of remote customer onboarding. However, it should be noted that the possibility to provide a secure communication channel and a secure access point usually is only available when a customer is onboarded in a fully digital mode as they identify themselves with a reliable and verifiable digital identity. In situations of audio contact with the bank i.e. the future customer contacts the bank on phone, it is not possible to provide a secure communication channel and a secure access point as these are available to existing customers and customers that are onboarded digitally. To onboard customers solely via audio would also increase the risk of fraud as the fraudster could be the one in contact with the banks' contact centre and the prospective customer could be lured to use e.g. their digital ID simultaneously.