EPIF Response to the Draft Guidelines on the use of Remote Customer On-boarding Solutions under Article 13(1)

March 2022

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.**

EPIF believes that this section, like the rest of the document, could aim for greater clarity. The use of plain language will help regulators and businesses understand what is expected. Throughout the document, the addition of material such as practical examples, short case studies, or examples of good and poor practice would help the reader understand the EBA's expectations.

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.**

Guidance about what we should consider when implementing remote onboarding is welcome.

Paragraph 10 could, if read literally, be interpreted to require all financial firms to create these policies and procedures even if they do not use remote onboarding. This is presumably not the intention. Small drafting changes could clarify this.

Policies and procedures relating to remote customer on boarding

The current wording of paragraph 10.c of the Guidelines may be understood to be that financial market entities should assess the adequacy of their remote onboarding solutions separately for each category of clients, products and services (based on the vulnerability of each category to AML/CFT risk). This seems to be a too excessive obligation, particularly in view of the fact that these entities are obliged under the AML regulations to conduct operations on the basis of general "risk-based approach". The current wording of paragraph 10.c implies the necessity to not only adjust the solutions used for remote onboarding to the level of the identified risk, but the provision goes further and forces obliged institutions to assess and adjust the solution per each element (component) of risk (clients, products or services).

Leaving the content of the paragraph in its current form will cause significant interpretation doubts at the stage of its application. The choice and range of tools used should correspond to the final risk category assigned to the client. Therefore, in order to align the requirements with the obligations under the existing AML regulations, it is recommended to narrow the content of the paragraph by making the applied solution dependent only on the level of AML/CFT risk identified in relation to the client, as follows:

> *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:*
>
> *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;*

For consistency, it is also recommended to modify paragraph 17 of the Guidelines as follows:

> *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***.

Additionally, the guidelines should consider allowing for a prioritization on the review of the highest ML/TF risks for business relationships in line with a proportionate assessment.

The pre-implementation assessment of the remote customer onboarding solution

According to the current wording of paragraph 15.e of the Guidelines, the scope of the pre-implementation assessment process should include at least 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. Such a requirement is too extensive and in practice it will be impossible to implement in its entirety. The dynamics of technological development in the field of financial services results in a geometric growth of new regulations in the area of financial services, supplemented by all kinds of "soft law" acts issued by competent authorities. As a result, financial entities must adapt their services and products to current requirements on an ongoing basis. It is not possible to determine the adaptability of a product to requirements that are unknown at the time the product is introduced, which is in fact what the current paragraph 15.e of the Guidelines requires. It is therefore recommended to remove this obligation as too far-reaching.

Trust services in accordance with Regulation (EU) 910/2014

As far as the *assurance level substantial* is concerned, the elements of technical specifications and procedures outlined in the Annex to Regulation (EU) 2015/1502 in terms of identity proofing and verification are high enough to consider that the pre-implementation assessment criteria set out in paragraph 15 to be appropriately met also for non-qualified trust services providing electronic identification means with the *assurance level substantial*. As guideline 4.5.48 indicates similarity in relation to reducing substantially the risk of impersonation, misuse or alteration of the identity between the level substantial or high in relation to trust services under the eIDAS Regulation, there is no justification to consider the assessment criteria in paragraph 15 to be appropriately met only when the solution includes just qualified trust services. In view of the above, it is suggested that paragraph 16 of the Guidelines should be amended as follows.

> *16. Financial sector operators should consider the assessment criteria in paragraph 15 to be appropriately met to the extent that the solution includes not only qualified trust services in accordance with Regulation (EU) 910/2014 (the "eIDAS Regulation"), but also non-qualified trust services provided that the assurance level of the electronic identification means they issue corresponds to the assurance level substantial.*

Sample testing

According to paragraph 21.iv of the Guidelines, financial sector operators should consider sample testing, as the means of carrying out the ongoing monitoring of the remote customer onboarding solutions. However, it is not specified what the

expectations are in this respect. Therefore, in order to avoid doubts at the stage of using this tool, it is necessary to specify how this method is to be carried out or to remove the clause.

EPIF welcomes and supports the proposed requirements around guideline 4.1.4. on ongoing monitoring of the remote customer onboarding solutions. However, EPIF would caution against a too prescriptive standarised 'one-size-fits' all approach for the ongoing monitoring requirements. We support the ability for obliged entities to apply their own risk-based approach in the administration of ongoing monitoring. A risk-based approach should permit company specific approaches in terms of frequency and process of monitoring that should lead to more effective and efficient ongoing monitoring. EPIF would urge that the final EBA guidelines should permit obliged entities to fulfill the ongoing monitoring obligations, with respect to frequency and process, in accordance with their own risk-based framework.

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.**

Currently, EPIF members are faced with different national requirements on acquisition of information, which makes operating inside the EU's single market more challenging.

(i) For instance, different rules regarding the acceptance of personal identification documents;
- some countries only permit IDs and passports,
- some countries accept driver licenses or residence permits,
- some countries require personal identification numbers/social security numbers to be collected.

All those mentioned documents might contain different information such as issuing or expiration dates.

(ii) In addition, countries have different document retention requirements for collected identification and other KYC documents, they can vary between 5, 7 or 10 years.

Therefore, **EPIF would welcome harmonisation or alignment on these (i) requirements, which would facilitate the use of unified KYC templates in conjunction with the similar (ii) retention policies.**

There is, throughout this document, an emphasis on video-ID and technologies that allow official documents to be seen remotely. There is a lot of detail about how this should be implemented. There is however, no text about other tools that are in widespread use in today's remote onboarding methods. For example, there is no mention of the use of database look-up services that provide information about customers from reliable independent sources (such as credit reference bureaux) and which can be used to cross-check other data.

Identifying the customer

The current paragraph 25.c of the Guidelines stipulates that financial sector operators should ensure that the images, video, sound and data are stored according to GDPR Regulation and remain available to the financial sector operator while identifying the customer. As a clarification to the provision, EPIF recommends to recognise that data can also include system logs or files that provide confirmation that specific data has been established (e.g. data aggregates or logs obtained from providers like Transparent Data or Bisnode).

Information to obtain in order to identify customers remotely

To avoid any ambiguity it is recommended to clarify the additional requirement set out in paragraph 27 *italics* by adding "where applicable" to make sure that it is up to the financial sector operators to determine the information they need to obtain in order to identify customers remotely provided that this is in line with the risk-based approach set out in the EBA's Guidelines on remote onboarding. In particular, obtaining a photo of an ID card or a video call should not be the only means of identification and identity verification. Thus, we recommend introducing an additional paragraph in Guideline 4.2 stating that a photo of an ID card or a video call are just two of the possible means that the financial services operator can take when identifying and verifying the customer's identity. This should be clearly laid down in the Guidelines. Otherwise, the Guidelines may create ambiguity regarding selecting means for customer identification and verification.

Identifying Natural Persons

According to paragraph 28 of the Guidelines, financial sector operators should have appropriate mechanisms in place to ensure the reliability of the information automatically retrieved, referred to in the previous paragraph and apply controls to address associated risks. This also includes situations where location 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. It is not sufficiently clear from the current content of the guideline what the EBA's expectations are in terms of the obligation to have mechanisms in place to ensure the reliability of customer location information and control measures, given the risk of spoofing (particularly on the subject of customer IP and VPNs). Examples of appropriate mechanisms could be specified in the EBA guidelines

This may lead to serious interpretation problems at the stage of application of the Guidelines. It is necessary to clarify the indicated provision or to remove it from the Guidelines.

Information on the purpose and intended nature of the business relationship

To ensure appropriate and proportionate regulation the requirement of implementing specific steps during the remote customer onboarding process to obtain information on the purpose and intended nature of the business relationship should be introduced depending on the services/products provided by the financial sector operators and their specificity. In regard to the transactions/products with low risk associated with the business relationship, e.g. low-value loans, it would be even more appropriate to waive this requirement.

EPIF also points out that Point 32 states: *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.* EPIF would welcome additional clarity through specific examples of what is meant by accuracy.

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.**

The overall impression of Guideline 4.3 is that collecting paper-based documents is obligatory in the course of remote customer onboarding. To avoid any ambiguity we recommend clarifying these provisions by adding "where applicable".

We note that a clarification is requested if this action should be focused on i) verifying the formal correctness of the document number, or ii) it is required to verify the actual existence of the document number through enquiry to official repositories or iii) the financial operators should implement an algorithm to re-calculate the document number and verify that the calculated number corresponds with the document ID number. If the action iii) is requested, it should be noted that this kind of activity will be quite onerous for the financial operators, so it will be preferable have a central repository to verify the document number correctness.

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.**

Paragraph 40 seems to require that video identification is necessary if high risk customers are onboarded remotely. This is based on our understanding of the current state of the technology realistically available for 'liveness' testing. If a business is using non-video remote onboarding methods, the expense of creating a channel just for a small group of customers means it is likely that these customers would instead be

turned away. The practical consequence of this would be politically exposed persons such as Members of Parliament (the main kind of high-risk customer many firms are likely to encounter) not being able to access many financial services via remote methods.

EPIF believes that a clarification is needed in order to be clear:

- If this kind of assessment is needed for all the increased risk of business relationships or just in case of increased risk resulting in a "high" score;
- Which are the liveness detection processes that could be implemented to perform this kind of assessment.

We note that the guidelines are quite strict on the need for a face to face verification in the same physical location. EPIF suggests drafting a more proportionate alternative in case remote customer onboarding is to be discontinued and redirected. In practice it could be difficult to have it in the same physical location.

Liveness detection solutions

Paragraph 40 of the Guidelines provides for an obligation to apply solutions based on liveness detection when establishing relationsips with high-risk customers. This obligation may be overly burdensome for financial market entities and even unfeasible for smaller entities. To take account of this suggestion, paragraph 40 should be clarified by using the term 'in particular' as indicated below. For small entities, it is proposed to include the possibility to verify the identity of a high-risk customer by carrying out a verification of two proofs of identity (e.g. an ID and a passport).

> *40. Where the ML/TF risk associated with a business relationship is increased, financial sector operators should* ***in particular*** *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.* ***In particularly justified cases resulting from limited structure and capacity, financial market operators may rely on the verification of two identity documents (e.g. an ID and a passport).***

Moreover, it should be noted that remote verification processes that include liveness detection procedures should not be used in every situation where the ML/TF risk associated with a business relationship is increased. Such a requirement would be much more justified for impersonation fraud risks. For ML/FT risk this requirement seems to be too much as gathering additional documents/statements/data should be sufficient. In other words, any measures (the catalogue shouldn't be a closed list) need to be taken according to the level of risk.

Insufficiency of the evidence

The Guidelines in paragraph 42 provide only one solution in case of insufficient evidence being a source of ambiguity or uncertainty in the remote onboarding process. In order to enable completion of the onboarding process, it is recommended to add an alternative solution in the form of a possibility to switch to a video-verification channel when connecting online with the customer. Such a solution is applied by the national competent authorities, e.g. Polish Financial Supervisory Authority. In view of the above, paragraph 42 should have the following wording:

> *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* ***or in an online channel allowing contact with the person carrying out the physical verification****.*

Randomness of remote customer onboarding solutions

The Guidelines provide in paragraph 45 for recommendations on the randomisation of sequences of actions "to the extent possible for the financial market operator" - the vagueness of this wording may raise concerns at the stage of application of the Guidelines when there is a requirement to apply randomisation under mandatory regulations. Therefore, EPIF suggests changing this wording to "in particular".

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

Repealing the application of paragraphs 38 to 45 to non-qualified trust services providers

Paragraphs 38 to 45 should not only be applied where financial sector operators resort to digital identity issuers to identify and verify the customer, which are qualified trust services in accordance with the eIDAS Regulation, or to any other digital identity issuer regulated, recognised, approved or accepted by the relevant national authorities. It should also be applied to non-qualified trust services provided that the assurance level of the electronic identification means they issue corresponds to the assurance level substantial.

It cannot be forgotten that digital identity issuer regulated, recognised, approved or accepted by the relevant national authorities can issue electronic identification means with the assurance levels low, substantial and/or high. Therefore, pursuant to paragraph 47 where financial sector operators resort to digital identity issuer regulated, recognised, approved or accepted by the relevant national authorities that issues electronic identification means with the assurance levels low, paragraphs 38 to 45 should not be applied. If so, such an exclusion should also apply to non-qualified trust services provided that the assurance level of the electronic identification means corresponds to the assurance level substantial.

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.**

As digital identities are managed at national level in the European Union, companies follow Member States laws and guidance on digital identities. That said, the EBA's final Guidelines on the use of Remote Customer Onboarding Solutions should take into account the evolving regulatory and legal framework at European level around digital identity.

In the context of digital identities, EPIF welcomes the current legislative review of the Regulation No 910/2014 establishing a framework for a European Digital Identity. EPIF sees the eID as an additional tool for AML/CFT as well as CDD regulation and KYC. We also support the idea of an unique identifier that would be attached to the identified persons across borders.

If the EBA were to take a role in 'certifying' the adequacy of different digital identity issuers' approaches (when no national framework has) this would lead to substantial system-wide efficiency savings against a situation where each individual financial sector operator does their own assurance checks. We suggest the extra burdens this would place on the EBA would be relatively modest against the savings. Innovation and growth would also be fostered by the legal 'safe harbour' such certification would provide.

Use of strong customer authentication

The Guidelines provides in paragraph 51 for strong customer authentication "where possible" when verifying identity. Leaving the paragraph in the current wording may cause doubts in case there is a requirement for strong customer authentication resulting from mandatory regulations. Additionally, it will be problematic to use strong customer authentication when the financial entity does not know the identity of the customer. Therefore, it is desirable to remove the reference to the use of strong customer authentication from paragraph 51 of the Guidelines. In case the above suggestion will not be approved, EPIF suggests changing the wording of point 51 to:

> *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~~ ***in particularly justified cases****, strong authentication is applied when verifying their digital identity.*

Inconsistency of paragraphs

In the text of the Guidelines, paragraphs 52 and 54 are practically identical (in paragraph 52 only the part highlighted below is added). Paragraph 52 specifies obligations of financial sector operators, but leaves space for interpretation ("as appropriate") as to the choice of appropriate measures to minimize the risk that the customer's identity is not the one declared. EPIF therefore proposes removing paragraph 54.

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

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.~~*

Verification of certificates

According to paragraph 53 of the Guidelines financial sector operators should check if the certificates are valid and from a trusted source when electronic certificates are used. EPIF suggests deleting the second part of this paragraph, i.e. '*In addition, the signed certificate should be used to sign any contract established with the customer. Any contract should be time stamped electronically as the proof of date when the contract is signed*.'.

The Guidelines set common EU standards on the steps financial sector operators should follow when choosing remote customer onboarding tools to comply effectively with their CDD obligations. Thus, the additional requirements for signing contracts with the customers shouldn't fall within the scope of these Guidelines. Moreover, when electronic certificates are used, the signed certificate should not be the only "tool" that is allowed to sign every contract established with the customer. Under Article 3(10) of the eIDAS Regulation 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. Article 25.1 of the eIDAS Regulation stipulates that an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures. Therefore, the requirement of using the signed certificate to sign any contract established with the customer precludes the financial sector operator with the possibility of signing the contract with a simple electronic signature which is permitted under the eIDAS Regulation or by agreeing to the Terms & Conditions by using a particular checkbox

or button. Introducing such a requirement would not let the financial sector operators benefit from the opportunities that the eIDAS Regulation and existing solutions in concluding remoted agreements have given as far as simplifying the of signing contracts.

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.**

Outsourcing of CDD

In scope of the content of paragraph 58, it should be noted that recourse to Article 29 of Directive (EU) 2015/849 seems to be incorrect. Guidelines 4.6.2. deals with the outsourcing of CDD in general, whereas paragraph 58 refers to an outsourcing service provider or agent being a part of the obliged entity. Therefore, the wording of this paragraph should be adjusted appropriately.

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.**

EPIF generally agrees with guideline 4.7. as set out by the EBA. However, in relation to paragraph 64 and the security for 'multi-purpose device' EPIF would like the EBA to consider the following.

For EPIF members a mobile device falls within the category of a 'multi-purpose device'. Notwithstanding that companies remain responsible for their part of the ICT security, companies do not have the ability to affect a customer's 'multi-purpose device' to provide a secure environment. Therefore, EPIF would urge the EBA to reflect these aspects in their final guidelines.

ICT and security risk management

Paragraph 61 of the Guidelines stipulates that 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 operators rely on third parties or where the service is outsourced, including to group entities. The significance of this obligation is not disputed, while group entities should be excluded from the scope of this guideline as outsourcing within the same group enables a higher level of control over the outsourced function. Thus, intra group outsourcing is less risky than outsourcing to an external entity.

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 190 authorised payment institutions and other non-bank payment providers as our members offering services in every part of Europe. **EPIF** thus represents roughly one third of all authorized Payment Institutions ("PI") in Europe. All of our members operate online. Our diverse membership includes a broad range of business models, including:

- Three-party Card Network Schemes
- E-Money Providers
- E-Payment Service Providers and Gateways
- Money Transfer Operators
- Acquirers
- Digital Wallets
- FX Payment Providers and Operators
- Payment Processing Services
- Card Issuers
- Independent Card Processors
- Third Party Providers
- Payment Collectors

EPIF seeks to represent the voice of the PI industry and the non-bank payment sector with EU institutions, policy-makers and stakeholders. We aim to play a constructive role in shaping and developing market conditions for payments in a modern and constantly evolving environment. It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

We wish to be seen as a provider for efficient payments in that single market and it is our aim to increase payment product diversification and innovation tailored to the needs of payment users (e.g. via mobile and internet).