## Response to the EBA's Consultation on Remote Customer Onboarding Guidelines

The European Fintech Association (EFA) welcomes the opportunity to participate in the European Banking Authority's (EBA) consultation on its draft Guidelines on the use of remote customer onboarding solutions. Overall, the guidelines provide an important step in the right direction along with the currently negotiated European Framework on Digital Identification (eIDAS) as well as the Anti-Money Laundering (AML) package. The EFA believes that several aspects need to be properly addressed by European regulators to create an efficient and effective pan-European digital market for businesses and consumers.

As highlighted in the EFA's position paper on the upcoming AML Regulation, we strongly support the EU-wide harmonization of digital identification methods, as it could remove significant cross-border barriers faced by European fintechs when onboarding customers. Moreover, it is critical to remove any gold plating on a national level and foster an interoperable environment that enables fintechs to have broader market access, and offer European consumers a more seamless and inclusive customer journey.

From the vast experience of the EFA members in the remote and digital onboarding of customers some clarifications are still very much needed in the following areas:

- **Basic definitions:** these need to be clear and straightforward to avoid national regulators adopting different approaches as is currently the case. For example, the definition of Digital Identity Issuer currently includes those market players providing the digital identity (issuers) and those who provide the authentication or verification method (third parties). The EFA would like to highlight this issue, since currently it is repeated across different Regulations, Directives, Delegated Acts and Guidelines. The proposed guidelines run the risk of overburdening certain market players that rely on others for the identification and verification.
- **Remote identification methods:** The EFA would welcome a distinction between potential methods of remote identification.The Guidelines should separate in a clearer way and subsequently tackle authority and integrity according to each of the following cases: remote identification that does not involve a live check (videoconference) with no examination of the original document, remote identification with examination of the original documents and other procedures. This would also streamline the approach taken by national regulators.
- **Outsourcing activities:** The EFA fully understands that this regulation will have to closely integrate with the AML package, and therefore calls on the European legislators to take a consolidated approach to the outsourcing of activities, to avoid burdening small players and to apply a "same risk, same rules" approach. This is of special relevance for the flourishing market of FinTechs that develop very specific activities in the AML space, specializing on elements of the Customer Due Diligence process. To create a level-playing field between the homegrown European FinTech industry and foreign BigTech, the businesses need to be able to cooperate with each other to provide one joint solution. In the specific topic of these guidelines, this is achieved through the outsourcing of the services to highly specialized third companies.
- **Third-party reliance:** There should be a full introduction to this section explaining the difference between reliance and outsourcing to make it clearer for the user, considering the scenario where it is carried out by an intragroup company. The Guidelines should spell out the initial CDD requirements under the EBA Risk Factor Guidelines instead of referencing the guidelines to make it easier for the user.

The EFA remains available for further enquiries regarding its response to this consultation and looks forward to future engagements and opportunities to interact with European regulators.

The EFA provided its detailed response with suggestions to the EBA (available in the Annex).

**Annex: EFA Response to EBA's Consultation on Remote Customer Onboarding Guidelines**

| EBA Question | DRAFT EFA RESPONSE |
|---|---|
| **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.** | • The definitions provided here are unclear: for example, the definition of "digital identity" includes the term "material or immaterial unit", which does not shed much light. Obscure language is used such as "dactyloscopic data" rather than "fingerprints".<br><br>• It would be beneficial if the definitions were clearer and provided examples of what a particular document/requirement is or where to find it out quickly i.e. other legislation such as the EBA Risk Factor Guidance). This document is 'Guidelines' drafted to assist financial institutions to comply so procedural explanations would be very helpful.<br><br>• Definitions like PRADO, MRZ and other IT technology terms should be clearly defined for more efficient reference purposes. The use of appendices providing such additional information would be helpful re: clear/detailed definitions and legislative references.<br><br>• It would also be helpful to have additional information added throughout the document where other legislation is referenced such as the difference between initial CDD and full CDD which is mentioned several times. e.g., the term ' initial CDD' be defined in this document to again avoid having to reference other legislation.<br><br>• **2 Paragraph 9**: The current definition of Digital Identity Issuer risks complicating the single market for remote onboarding service providers in the EU. There is a distinction between an Issuer of a |

| | |
|---|---|
| | Digital Identity (ie eID service providers under eIDAS) and a business providing verification/authentication services for the purposes of onboarding. This distinction should be reflected in the EBA guidelines to avoid any confusion. European legislative tools (including Regulations, Directives, Delegated Acts and Guidelines) should have consistent definitions to avoid fragmentation in the application of rules, and to provide legal certainty to market participants (ie third party onboarding service providers, financial institutions, consumers).<br><br>● The concept of 'material/immaterial' is unclearly defined. This should be further elaborated at least by providing some examples of what is meant by this (e.g., a private key, digital ID tokens, smart ID cards with embedded smart chips). |
| **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.** | ● **Section 10(c)** could pose practical challenges, as we cannot know in which risk category to place a customer until after we have begun onboarding them and have found out more information about the customer: firms will often be well into the onboarding process before having enough information about a customer to determine how that customer fits into our customer risk models.<br><br>● We fully appreciate that this consultation relates to the remote customer onboarding solution but it would be beneficial to also include the actual information required to IDV customers instead of referring to other legislation/guidance. E.g. e.g. 10 (d to f) wants banks to create policies and procedures which include the types of documents that are admissible (d) but not actually what those documents are. It would be more beneficial, if all this information is combined or described, as the user currently needs to refer to the |

| | |
|---|---|
| | EBA Risk Factors guidance and reflect all this information into the policies/procedures for the solution.<br><br>● **Paragraph 16:** Qualified Trust Services - referenced in Regulation (EU) 910/2014 - this information should be added to an appendix for the purpose of easy reference.<br><br>● **Paragraph 18: '**Sufficient assurance / adequately manage' - The EFA is of the view that is important to clarify how these terms would be defined. It would be better to state that the system launch should only happen post an audit or sign off by Quality Assurance. These terms could be defined as meaning 'that no identified weaknesses, additional risks, or systematic errors have been identified from extensive Quality Assurance testing or any issues identified have been remediated and are now deemed adequate.<br><br>● **Paragraph 21:** Ongoing monitoring examples could be more detailed to provide more information for the user e.g. what exactly are automated critical alerts and notifications; what is expected from a manual review; which is the approach or aim to be followed for the regular automated quality reports?<br><br>● **Paragraph 23: '**reliability and adequacy of the solution regarding fully automated remote customer solution', could be quantifiable or provide more context in regard to the user.<br><br>● **Comment to 4.1.3:** Currently, It is not clear whether this requirement would apply for operators that rely on other operators for identification and verification. From what the EFA is aware, obliged entities may rely on identification and verification carried out by another obliged entity when certain preconditions are observed. If such preconditions are met (e.g., the obliged entity is comfortable |

| | |
|---|---|
| | that they may rely), then it would create an unnecessary burden and render the "reliance" concept "purpose" a bit more to the side of "obsolete".<br><br>a. In addition to that, the guidelines should provide an "exit" of the requirement to create a "pre-implementation assessment" to the operators that already have established and proven/audited remote identification solutions as to avoid unnecessary burden (outsourcing guidelines already cover these).<br><br>● **4.1 Paragraph 16:** As well as directly referencing qualified trust providers, the guidelines should also allow for financial service providers to consider service providers that have received a certification through a national conformity assessment body under the eIDAS Regulation (which are not considered qualified trust service providers) to still appropriately meet the criteria in paragraph 15**.**<br><br>● Service providers having received equivalent certification under the eIDAS Regulation or the AML Directive uphold the same standards, and should therefore not have to prove their process requirements through yet another series of criteria. If this is not the case, paragraph 15 should also stipulate that once one Member State recognises that a service provider meets all the criteria set out in the paragraph, this should be mutually recognised across the Union, so as to not mandate that service providers provide the same proof every time they choose to expand their service to a new marketplace within the EU.<br><br>● We support the Risk Based CDD taken in 10(c) however we would call for more clarity on what is meant by 'solution'. In addition, the scope |

| | |
|---|---|
| | of section c is very broad and would recommend removing 'products and services' as customer onboarding is specific to the customers and including all 3 makes it a risk assessment as opposed to a customer onboarding question.<br><br>● **Additional consideration:** With regards to Section 4.1.3 on Pre-implementation Assessment, will existing policies/processes be grandfathered from this? |
| **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.** | ● The EFA is of the view that the scope of the guideline could be further narrowed to provide clarity and cover situations where documents are being remotely verified or where a digital identity is verified under the EU's formal e-ID framework. Currently, the Guidelines are not addressing methods, such as the use of trusted database providers, as these services are a valid part of the remote onboarding processes.<br><br>● **(4.2.1 & 4.2.2)** Concerning customers vs Natural persons , differences would need to be defined or explained better.<br><br>● **Paragraph 25:** 'digital identity issuers' - further information required on what this is and how they operate etc - unless described elsewhere.<br><br>● **Paragraph 25:** 'Initial customer due diligence' - Guidelines would need to further define and explain which criteria are required to consider it "adequate" as mentioned in (a). |

| | |
|---|---|
| | • **Paragraph 26:** Clearly Define 'Identification Proofs'.<br><br>• **Paragraph 28** 'appropriate mechanisms' - more examples or best practice would be helpful. It discusses IP and VPN re: location which again are technical terms which could be further detailed with additional guidance / information or references in an appendix.<br><br>• **(4.2.3)** -The consultation paper could detail the minimum standards/best practice expected instead of referencing the EBA Risk Factor Guidelines (or add such information at the end for ease of use).<br><br>• **(4.2.4)** Nature and purpose of a customer relationship should be also obtained in the Initial Customer Due Diligence.<br><br>• **4.2.1**: The EFA would recommend expanding the tile to specify to what the guidelines are referring to: "Identifying the customer without the use of digital identity issuer".<br><br>• **4.2.4:** We would recommend removing "assessment of the purpose and intent of the business relationship" from the guidelines. It could generate some misunderstanding as to what this specific CDD measure consists of. Operators might deem necessary to collect this information in all cases (derisking). Explanations about the scope of each CDD measure (e.g., identification, verification, assessment of the purpose and intent of the business relationship) should be avoided. Remote identification is part of "identification" and "verification". |

| | |
|---|---|
| **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.** | • This section discusses the remote authentication of physical documents. Please can you clarify whether "the original identity documents" (in Paragraph 33) means just official photo-ID such as a passport, or whether it also covers other documentary evidence gathered as part of customer due diligence exercises (e.g. utility bills to provide evidence of address).<br><br>• **Paragraph 33a:** Security features could be more detailed –on industry best practice or similar guidance.<br><br>• **Paragraph 33a to e:** Additional information, training, guidance, or industry best practice would be helpful.<br><br>• **4.3:** A distinction between the potential methods of remote identification would be welcome. The guidelines could separate in a clearer way and subsequently tackle authenticity and integrity according to each case:<br>a. Remote identification that does not involve a live check (videoconference) – no examination of the original document;<br>b. Remote identification with examination of the original document;<br>c. others (e.g. digital identity perhaps)<br><br>• **4.3 Paragraph 33:** On the authenticity of document copies, begins with stating that steps to verify authenticity of such copies "may include." The main motivation behind these guidelines is to provide increased harmonisation across the continent. Phrases such as "may include" are exactly what leads to differing interpretations of the |

| | |
|---|---|
| | rules by national competent authorities (ie one authority may requires all steps under 4.3. paragraph 33 for a copy to be reliable, whilst others may only require one). We would argue for a risk-based distinction of the various steps, which would set out what steps are required depending on what risks are involved.<br><br>• This appears to be an overly prescriptive requirement and quite onerous. We would suggest this provision is further qualified by specifying that such data is not required to be collected in every instance but rather can optionally be collected – where technically possible – for verification through an additional source. |
| **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 39:** This suggests matches between biometric data on a document (e.g. a photo) and the person should be verified to ensure the match is unambiguous. This suggests manual re-verification in every case. A more proportionate approach would be more suitable, in order for manual checks to take place on a sample basis.<br><br>• **Paragraph 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. Thisparagraph suggests that, ultimately, face-to-face verification is more effective and preferred to digital identification. Rather, if there's a concern, this should trigger a stronger control such as a video conference or liveness element to strengthen the identification process. |

| | |
|---|---|
| | • **Paragraph 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:<br><br>a. ensure that the photograph(s) is taken under proper lighting conditions and that the required properties are captured with absolute clarity;<br><br>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;<br><br>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;<br><br>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.<br><br>• **Paragraph 45**: Recommends that randomness is added to the sequence of events presented to the customer when they are being onboarded. It would be helpful to understand what risk this measure seeks to address. |

| | |
|---|---|
| | • **Paragraph 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:<br><br>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;<br><br>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;<br><br>c. capture biometric data to compare them with data collected through other independent and reliable sources;<br><br>d. telephone contacts with the customer;<br><br>e. direct mailing (both electronic and postal) to the customer.<br><br>• **Paragraph 39:** 'Biometric data' should be defined with examples (via artificial intelligence system of facial recognition, by an employee, etc.) as well as to indicate further details on how the verification shall be carried out in order to detect unambiguous matches.<br><br>• **Paragraph 40:** 'Where the ML/TF risk associated with a business relationship is increased' should be clarified in terms of its meaning. |

| | |
|---|---|
| | • **Paragraph 40:** Needs to be reconsidered whether the 'Liveness Detection procedures' need its own section again with guidance, best practice etc.<br><br>• **Paragraph 43:** This section provides more granular details of what is actually required or the way to assess which could be reflected throughout the whole document with topics such as 'initial customer due diligence' etc.<br><br>• **Paragraph 45:** The whole section requires further information/guidance to help describe what the Guidelines actually expect financial firms to do with respect to 'randomness in the sequence of actions' - further information/guidance required.<br><br>• **Paragraph** (46c) - Biometrics data - needs to be defined better to provide clarity on what it captures (e.g. fingerprints etc.)<br><br>• **Paragraph 46d: 'telephone contacts with the customer' should be further defined.**<br><br>• **Paragraph 47 'Qualified Trust Services' -** This point would benefit from further practical details on what is required by financial firms, rather than referencing other legislation.<br><br>• **4.4 paragraph 38a:** The term "person previously identified" does not make much sense. Probably a typo.<br><br>• **4.4 paragraph 46:** Typo. "Should make use of one or more". In addition to that, "one or more" is ambiguous, and should be clarified in terms of what option operators should take. Perhaps "at least one" would be a better wording. |

| | |
|---|---|
| | • **4.4 paragraph 42:** On insufficient quality of evidence being provided. The EFA is of the view that the necessary move to a physical location should be a last resort. The guidelines should allow for repeated attempts of remote customer onboarding with other pieces of evidence as well as a face-to-face verification over videoconference. Only after repeated attempts and the virtual face-to-face prove unable to alleviate the 'uncertainty and ambiguity' should the customer be required to have a face-to-face in the same physical location.<br><br>• **4.4 paragraph 43a:** Requires "absolute clarity" in photographs taken as a means to verify one's identity. We would argue to make this language more precise, "the required properties are captured with the necessary clarity to allow the proper verification of the customer's identity." as is the case in paragraph 44(a).<br><br>• **4.4 paragraph 43c:** Appears to require liveness detection verifications as part of any instance of photograph-based onboarding. This is not appropriate as it does not take a technology neutral approach, fails to take into account solutions which are widely used in the market and work effectively, and is disproportionate in terms of what it seeks to achieve. As underlined in paragraph 40 in the same page of the consultation, liveness detection should be left for cases where ML/TF risks are higher, rather than be necessary for all photograph-based onboarding processes.<br><br>• **4.4 paragraph 43d:** The EFA strongly welcomes the allowance of strong and reliable algorithms completing verification instead of the need for human verification. Nevertheless, we do still require clarity on what the wording "in the absence of human verification" means. Does this mean that operators can choose AI over humans to verify |

| | |
|---|---|
| | without issues, or is this only allowed where humans cannot do so for particular reasons? We assume this would be the former, and if so, we would recommend that this be clarified in text to avoid misinterpretations at the national level.<br><br>• **4.4 paragraph 44(b/c):** The EFA believes that staff knowledge may not be required in each and every videoconference if a trained AI is overseeing physical and psychological reactions during the videoconference, whilst the employee holding the interview will also be provided with the guide.<br><br>• **4.4 paragraph 45**: Again, this section, does not appear to take a technology neutral approach. Similar to our comments about paragraph 43(c), fails to take into account solutions which are widely used in the market and work effectively, and is disproportionate in terms of what it seeks to achieve. For example, there are solutions on the market that work extremely effectively without the need for randomness such as document and biometric checks.<br><br>• **Paragraph 38b:** This could be quite onerous and from our understanding this requirement doesn't currently exist under AML regulations.<br><br>• **Paragraph 44c and 45:** These paragraphs are overly prescriptive and call for a more flexible approach allowing for the implementation of risk-based measures**.**<br><br>• **Paragraph 46:** The list in para 46 is overly prescriptive and limited in scope, and 4AMLD and the EBA guidelines on ML/RF risk allow the use of a wider range of controls. these measures must be risk based |

| | |
|---|---|
| | rather than an obligation to pick one of a combination of 5 specific controls. |
| **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.** | • **Paragraph 48:** The language in Paragraph 48 is very convoluted. It is difficult to understand its meaning, therefore further clarification is required.<br>• **'Digital Identities' -** define, guidance, best practice - provide more information instead of referencing other legislation would be helpful.<br>• **Paragraph 50a -** The guidelines could provide details on what is required from the Annex to Regulation (EU) 2015/1502 instead of referencing the regulation.<br>• **Section 4.5:** Tells the user details of what is expected but not how it could be performed to meet the requirements. Guidelines should provide the user with best practice, guidance etc to help them meet the requirements.<br>• **Paragraph 51**: 'Define and provide further guidance within the Guidelines for Secure environment'<br>• **Paragraph 53:** Define and provide further guidance within the Guidelines for Trusted Source.<br>• **Paragraph 55:** 'Define and provide further guidance within the Guidelines for Adequate Measures'. |

| | |
|---|---|
| | • Service providers that are "regulated, recognised, approved, or accepted by the relevant national authorities", should be recognised as such throughout the EU. |
| **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.** | • There should be a full introduction to this section explaining the difference between reliance and outsourcing to make it clearer for the user, considering the scenario where it is carried out by an intragroup company.<br><br>• The section should spell out the initial CDD requirements under the EBA Risk Factor Guidelines instead of referencing the guidelines to make it easier for the user.<br><br>• **Paragraph 57**: Needs to be explained better as to what is required - difficult to understand.<br><br>• **Paragraph 58b**: The definition of what is suitable needs to be included. Examples are helpful but essentially it is up to the financial institution to define what 'suitable' actually means in context with staff training, technology fitness etc'. The financial institutions view of 'suitable' could be different to that of a regulator or auditor. |

| | |
|---|---|
| | • **Paragraph 60:** More information is required, as currently the text is confusing as to what this actually means regarding 'Digital Identities and not Outsourcing'.<br><br>• **4.6 Paragraph 56a:** No guidelines on the "steps necessary". "sufficient/consistent/equivalent" do not provide clarity when national KYC requirements do not match. This could jeopardize reliance since an operator could claim that the third-party's policies do not match with those of the operator. Moreover, cases of reliance and outsourcing are distinct. In reliance circumstances, other institutions might not be willing to share their policies and procedures. In the scope of outsourcing these might be easier to retrieve from vendors.<br><br>• **4.6 Paragraph 56b**: Clarification is needed on this paragraph means and entails.<br><br>• **4.6.2 Paragraph 58a:** Requirement that vendors implement the operator's policies and procedures may jeopardize the offering of remote identification services. Policies and procedures might be very different according to the operators and according to the jurisdictions.<br><br>• **Paragraphs 57 and 60:** This could be included in the beginning of the section to make it clearer.<br><br>• **4.6.2 paragraph 59(b):** The phrasing "access to the data is strictly limited and registered;" may prevent the development of future data consortiums for the purposes of AML, which would in fact improve existing systems and reduce fraud. Paragraph 59 is indeed not needed, as it duplicates existing horizontal legislation, in particular GDPR. Duplication of legislation is unnecessary and adds additional |

| | |
|---|---|
| | complexity and burden to all parties without adding any value and, as such, it should be removed.<br><br>● **Section 4.6:** Furthermore, section 4.6 also would merit from providing guidance at the national level with regards to sub-outsourcing. Overall, we consider that the upcoming AML Regulation's Article 40 will improve the current landscape and lead to a more harmonised application of outsourcing rules. Nevertheless, neither Article 40, nor these guidelines encompass sub-outsourcing. To effectively harmonise the EU outsourcing regime and create further certainty for CDD service providers, a common approach to sub-outsourcing should also be included within the guidelines.<br><br>a. This is especially important as tech businesses/startups in the AML space tend to specialise on specific elements of the CDD process (ie remote customer onboarding). To effectively compete with Big Tech and established players, such businesses need to be able to cooperate with other businesses to provide one joint solution. In the area of eKYC and CDD this is achieved in many instances through sub-outsourcing of the services which an outsourced company is not specialised in. This allows for businesses to remain specialised and to develop higher-end solutions, whilst remaining competitive in the wider CDD marketplace by being sub-outsourced.<br><br>● We would therefore recommend for the inclusion of a paragraph that clarifies how sub-outsourcing should be allowed as long as certain criteria are met (ie this has been agreed upon between the outsourced party and the operator, regular reviews/monitoring can still occur, etc.) |

| | |
|---|---|
| **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.** | • **Paragraph 62:** Add what is required from the EBA Guidelines instead of referencing.<br>• **Paragraph 63:** 'Define secure access point' - very technical section difficult to understand unless you work in IT.<br>• **Paragraph 64:** Define 'Multipurpose device'. |