loqr

Empowering Digital Lives

March 7th, 2022

Suggestions and Comments to EBA's Draft Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849

EBA | EUROPEAN BANKING AUTHORITY

The Draft Guidelines on the use of Remote Customer Onboarding Solutions issued by the European Banking Authority represents an important and significant step to achieve legal certainty and broader financial inclusion in Europe, balancing it with the integrity of the financial system.

As part of our vision of empowering digital lives, LOQR analyzed the proposal and here we present some suggestions and comments to the public consultation.

We believe that cooperation and transparency are important fundaments of building a broad, solid, and safe digital financial inclusion, so we hereby authorize the disclosure of our comments and suggestions.

General context

Considering the increasing risks of money laundering (around 2.7% of global GDP[1]), terrorist financing, corruption (~US$20-40 billion/year in bribes received[2]), money mulling, smurfing, impersonation attempts, and other types of frauds, financial crimes, as well as other criminal activities via digital and online platforms, LOQR understands that the most advanced available technology tools should be used to ensure a safe and efficient experience for both clients and financial institutions in what concerns to customer's remote onboarding.

The development of identity verification technologies is going through a fast-paced changing. Despite the remarkable advances in the field, none of the existing tools can provide 100% accuracy. For this reason, the combination of different mechanisms can mitigate the risks mentioned above while more accurate and advanced solutions are created, developed, and implemented.

We truly believe that one important step for digital financial inclusion is building a trust relationship with the new customers. For a variety of reasons, some people still do not fully trust digital solutions and avoid using these services believing that the traditional methods are more reliable to avoid frauds.

Some digital solutions failed to provide the security that was expected, and it did not contribute to building a sense of reliability on the systems. Providing more strict regulatory aspects may increase the remote onboarding process length, but on the other hand, it may prevent events that could harm the reputation of Financial Sector Operators (FSOs) and the system itself, slowing down the digital financial inclusion.

In this sense, having more strict guidelines regarding technological aspects, such as the use of Optical Character Recognition (OCR), Machine Readable Zone (MRZ), advanced safety features of the documents accepted, liveness, face match, digital IDs, among others, would be more adequate to the goals of creating a safer digital environment without creating an excessive burden to FSOs and to customers.

Answers to EBA's questions

QUESTION 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.

1. We understand that documents accepted for the purpose of remote onboarding should mandatorily have MRZ (as the regulation in Germany, for example) or have advanced safety features (e.g., as required by the regulation in Portugal). This measure can reduce the chance of fraud or adulteration, enhancing the security of the process.

   In situations where the client is not able to provide a document with such features, a possible solution is to complement the onboarding file with another official document (containing a photo) to double check the authenticity of the data provided: e.g., driver's license, professional association ID (in the countries where it is accepted as an official document), among others.

2. Related to the paragraph 37, if it is not possible to provide any document with MRZ or advanced safety features, the client should have their risk level raised and further steps of verification should be applied, namely real time videoconference with a human operator, in which is possible to ask the customer to show and move the document to the camera, to mitigate the risks of use of fake, modified, or fraudulent documents.

3. To reduce the risks of the use of fraudulently or illegally obtained pictures, copies, or digitalization of IDs, we strongly suggest that the onboarding cannot be done using uploads of files from the customer's device. The pictures of the document must be taken in real time using the app, the website or the platform used by the FSO for the onboarding.

QUESTION 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.

1. Considering the risks of the digital onboarding and the importance of maintaining the integrity of the financial system, liveness detection and face match technologies should be used in all onboarding processes, not only in the increased ML/TF risk ones. The necessity of applying these technologies arises from various reasons:

a) The Rationale 8 of the Draft Guidelines indicates that ML/TF risks "*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*". The use of liveness and face match tools can be an additional barrier to eventual verification gaps, as well as mentioned in the Rationale 15, with the need to apply sound processes to mitigate the impersonation fraud

risks. Liveness and other Machine Learning/AI can add value to Identification and Verification of the customers by performing micro expression analysis, anti-spoofing checks, fake image detection, and human face attributes analysis[3].

b) If the client is unknown or not well-known by the FSOs, having a low risk profile does not necessarily mean that the behavior of the client will not increase ML/TF risks to the FSO after the onboarding. Especially in cases of money mulling, smurfing, and terrorist financing, criminals choose intermediaries of low-risk transactional profile to try to dissimulate and disguise the flow of funds obtained from illegal/illicit activities or to criminal activities. In TF, the characteristics of the funds transferred is usually related to small amounts that can take time to trigger system alerts.

   A low-risk client can quickly shift to high-risk. If the funds reach the destination, especially in TF, the practical consequences can be severe.

c) Face match and liveness detection do not interfere in the user experience: as they are automated, these tools do not complicate any further the customer's experience – they do not exclude or harden the financial inclusion.

d) Though these technologies may not be 100% accurate, as mentioned in the section of cost/benefit analysis, they can create an extra security layer that, when in doubt, can be confirmed by the human intervention.

   There is also an opportunity to apply these technologies as a way of improving its developments linked to artificial intelligence and machine learning, leveraging it by its constant use.

e) The Paragraph 39 determines that biometric data collected by the FSO needs to be unique and unequivocally related to a single natural person, matching it with the ID submitted and the customer being onboarded. Considering the impersonation fraud risks and the more sophisticated and dynamic fraud methods, to achieve the goal presented in that target, it is important to use the leverage of new technologies and tools.

   For this reason, we understand that the Paragraph 40, by stating that liveness detection should be used only in cases of increased ML/TF risks, is not in line with the fundamental reasons of the Draft Guidelines and the ultimate purpose of it.

2. Also related to the Paragraph 40, we understand that the use of liveness detection during a real-time videoconference should not be necessary, as during this process, a human operator is interacting with the customer and is able to verify if he/she is a real person. In the situations where the self-interview is used, however, liveness detection and face match tools should be used to ensure the identity of the client to be onboarded.

3. To assure the customer is not using filters or any other methods to dissimulate his/her identity, it should be recommended to establish a direct link/connection between the device of the client and the servers of the FSO, both for real-time videoconferences and for self-interviews.

4. Only real-time recorded videos should be accepted for the purpose of self-interview, forbidding the submission or upload of previously recorded videos on the remote onboarding platforms.

5. The Paragraph 44, a) is not clear when it refers to the use of "*reliable technological systems*". Does it refer to the quality of the video itself, to the

tools used to identify the customer, or to another aspect? Can you please clarify it?

6. Regarding the OTP (one-time passcode) mentioned on the Paragraph 46, b), to increase the level of security of this step, we suggest the inclusion of two requirements:

    i. The customer should have a limit of three attempts to type the OTP sent.
    ii. In cases of videoconferences, the OTP should be sent during the interview and should be typed by the customer in real-time, without informing the numbers to the operator.

7. The Paragraph 47 states that the authenticity check rules contained in the paragraphs 38-45 should not be applied when the FSO resort to digital identity issuers to identify and verify the customer.

    We believe that the use of digital IDs and resorting to regulated, recognized, approved, or accepted digital identity issuers by the relevant national authorities should reduce the requirements for remote onboarding to avoid double work and to create a friendly customer experience – enhancing, then, inclusion to the financial system. However, this rule should be applied with caution not to replace important KYC steps. The way Paragraph 47 is written may lead to an understanding of loosen requirements that can bring higher risks – for example, not collecting relevant data of the customer: pictures, videos, among others.

    The writing of the paragraph is also not in line with the exposed cost/benefit analysis exposed in the case 2, which the option preferred was to allow 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*".

    The collection of biometric and/or non-biometric data (namely photos and videos), is an important tool to unequivocally identify and verify the customer and his/her intention to be take part in the remote onboarding process, and that their digital identity is not being used by other person to open an account. Collecting pictures and videos also can help to assess if the person is under coercion or if the customer has full mental capacity. Furthermore, resorting to digital IDs do not exclude other possible risks related to the customer that can impact the FSO and the financial system.

QUESTION 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.

1. We believe the paragraphs 52 and 54 should be merged, as their content is almost identical.

Conclusions

We understand the importance of the Draft Guidelines Public Consultation to achieve a faster, more democratic, and efficient financial inclusion, and to assure a safer financial system.

A clearer and more standardized European regulatory framework about Remote Customer Onboarding may create opportunities to reduce costs, raise efficiency and improve the services offered to companies and individuals.

However, these points can only be achieved if the safety of the system is enhanced, so there are no setbacks. Our comments and suggestions are based on it and on the premise that there are several technologies available to be chosen by FSOs and they can be used to improve security without overloading the FSOs or the customers.

We praise this Public Consultation and the new possibilities the future Guidelines will bring.

About LOQR©

LOQR is the **leading AI-powered journeys-as-a-service provider** for financial institutions. **We enable organizations to offer B2B2C and B2B journeys** through our journey builder platform, such as **remote account opening**, **customer data update**, **remote access recovery**, and other value-added services as an integrated digital channel.

Through a **fully compliant journey builder platform**, banks and other players offer digital onboarding experiences fully aligned with their customers' expectations. **We anticipate and update regulatory changes** over time, assuring that our clients meet local and global compliance regulations, and our extensive know-how allows us to continuously fine-tune our journeys to guarantee the most efficient and convenient solutions.
Through AI (Artificial Intelligence) with ML (Machine Learning) proprietary techniques, we increase the overall security and KYC/AML accuracy while reducing our clients' costs and increasing their ROI.

To know more about LOQR© and our journey builder platform, don't hesitate to get in touch with us at sales@loqr.io.