European approach to remote customer onboarding solutions

Daniel Cookman
University College Dublin, Dublin, Ireland

Abstract

Purpose – This study aims to identify European positioning on the use of remote customer onboarding solutions in combating financial crime.

Design/methodology/approach – This study is a desktop research that examines European Banking Authority (EBA) policy statements relating to the use of innovative solutions in combating financial crime.

Findings – Technological advancements in biometric data and software tools provide a unique opportunity to address potential paper customer onboarding process deficiencies. Electronic remote customer onboarding solutions equip credit, financial institutions and investment firms with an alternative FTE cost-saving solution, in their pursuit of revenue generation. Whilst the EBA and Financial Action Task Force have provided approval for the utilisation of innovative solutions and AML technologies in combatting financial crime. Hesitancy remains on the ability of credit and financial institutions to use technological solutions as a "magic solution" in preventing the materialisation of money laundering/terrorist financing related risks. Analysis of policy suggests a gravitation towards the increased use of the aforementioned technologies in the interim.

Originality/value – Capitalisation of European banking authority.

Keywords Financial crime, European banking authority, Innovative solutions

Paper type General review

Introduction

There has been a significant increase in demand for remote onboarding from institutions and their customers. This trend was exacerbated by restrictions on movement in the context of the Coronavirus Disease Pandemic 2019 (COVID-19), which highlighted the importance of institutions having at their disposal reliable and effective means to meet their customer due diligence (CDD) obligations in this context. The European Banking Authority (EBA) considers it important for competent authorities and credit and financial institutions to understand the capabilities of these new remote solutions to onboard customers and make the most of the opportunities they offer. At the same time, to support their sound and responsible use, the EBA, from 2 October 2023, will require competent authorities and credit and financial institutions to be aware of guideline requirements relating to money laundering and terrorist financing (ML/TF) risks arising from the use of such tools and take steps to mitigate those risks effectively (European Banking Authority, 2023a, pp. 1–45).

Journal of Money Laundering Control
Vol. 26 No. 7, 2023
pp. 213-223
Emerald Publishing Limited
1368-5201
DOI 10.1108/JMLC-08-2023-0140

Innovative solutions: a question of effectiveness?

Innovative skills, methods and processes, as well as innovative ways to use established technology-based processes, can help regulators, supervisors and regulated entities overcome many of the identified AML/CFT challenges. Technology can facilitate data collection, processing and analysis and help actors identify and manage ML/TF risks more effectively and closer to real-time. Faster payments and transactions, more accurate identification systems, monitoring, record-keeping and information sharing between competent authorities and regulated entities also offer advantages. The increased use of digital solutions for AML/CFT based on artificial intelligence (AI) and its different subsets (machine learning and natural language processing) can potentially help to better identify risks and respond to, communicate with and monitor suspicious activity. At the public sector level, improved live (real-time) monitoring and information exchange with counterparts enable more informed oversight of regulated entities, helping to improve supervision (FATF 2023 "Opportunities and Challenges of New Technologies for AML/CFT", pp. 1–49).

At the private sector level, technology can improve risk assessments, onboarding practices, relationships with competent authorities, auditability, accountability and overall good governance. Whilst cost-saving, digital identity solutions can enable non-face-to-face customer identification/verification and updating of information. They can also improve customer authentication for more secure account access and strengthen identification and authentication when onboarding and transactions are conducted in person, promoting financial inclusion and combating money laundering, fraud, terrorist financing and other illicit financing activities. (FATF 2023 "Opportunities and Challenges of New Technologies for AML/CFT", p. 6).

The EBA (European Banking Authority, 2023b, pp. 1–19) also provides a similar rationale to the Financial Action Task Force (FATF) on the usefulness of leveraging innovative solutions in combating financial crime-related risks (Financial Action Task Force, 2023). Identifying that where innovative solutions are designed to monitor business relationships and transactions, they often replace or supplement traditional transaction monitoring (which is based on preset rules, thresholds and patterns and can, at times, generate large numbers of possible hits) with a more tailored approach based on artificial intelligence, which often involves algorithms that process large volumes of information from multiple sources and in different languages. These solutions are continually learning from past cases and leveraging this learning to automatically investigate similar cases in future. If implemented properly, these innovations can potentially allow firms to (European Banking Authority, 2023b, pp. 5–6):

- assess risks associated with a business relationship instantly by reviewing large volumes of data and information from various internal sources (e.g. a customer's static data, account information, transaction history, engagement history) and external sources (e.g. politically exposed person (PEP) registers, company and beneficial ownership registers, online news and publications), including sources in different languages, and by augmenting that data with information protocol (IP) locations and device information;
- complement existing monitoring processes by making them more automated and thus allowing firms' staff to focus on the actual analysis of information;
- streamline their decision-making practices by receiving instant trigger alerts of possible suspicious transactions or changes in customers' risk status (e.g. a new PEP position or corruption allegations); and/or
- minimise false alerts.

As illustrated, supervisory authorities are complementary to innovative solutions. There is a firm understanding that electronic customer onboarding solutions equip credit and financial institutions with an FTE cost-saving solution in their pursuit of revenue generation, while providing an additional tool for combating financial crime-related risks. Although implementation of these solutions is not without risk, as identified by the EBA, there is a risk that innovation in this field, if ill understood or badly applied, may weaken firms' ML/TF safeguards and subsequently undermine the integrity of the markets in which they operate (European Banking Authority, 2023b, p. 2).

FATF provides a similar caveat in their reasoning that when innovative technologies are used responsibly and proportionally, innovative AML/CFT technologies can help identify risks and focus compliance efforts on existing and emerging challenges, but manual review and human input remain very important. For example, even in a technology-enabling regulatory environment, human actors must be relied upon to identify and assess any residual risks presented by new technologies and put in place appropriate mitigation measures. Combining the efficiency and accuracy of digital solutions, with the knowledge and analytical skills of human experts produces more robust systems that can effectively respond to AML/CFT requirements whilst being fully auditable and accountable (FATF 2023 "Opportunities and Challenges of New Technologies for AML/CFT", p. 5).

Remote customer onboarding solutions: policy and procedure considerations

Internal policies and procedures are central to managing regulatory risk relating to the pre-implementation, implementation and ongoing use of innovative solutions. Credit and financial institutions should be risk-sensitive, identifying the following (European Banking Authority, 2023a, p. 12):

- A general description of the solution credit and financial institutions has been put in place to collect, verify and record information throughout the remote customer onboarding process. This includes an explanation of the features and functioning of the solution.
- The situations where the remote customer onboarding solution can be used, taking into account the risk factors identified and assessed and the business-wide risk assessment, including a description of the categories of customers, products and services that are eligible for remote onboarding.
- Which steps are fully autonomised and which steps require human intervention.
- The controls in place to ensure that the first transaction with a newly onboarded customer is executed only once all initial CDD measures have been applied.
- A description of the induction and regular training programs to ensure staff awareness and up-to-date knowledge of the functioning of the remote customer onboarding solution, the associated risks and the remote customer onboarding policies and procedures aimed at mitigating such risks.

The AML/CFT Compliance Officer should, as part of their general duty to prepare policies and procedures to comply with the CDD requirements, make sure that remote customer onboarding policies and procedures are implemented effectively, reviewed regularly and amended where necessary. However, the management body of the credit and financial institution should approve remote customer onboarding policies and procedures and oversee their correct implementation (European Banking Authority, 2023a, p. 13).

Remote customer onboarding solutions: pre-implementation assessment

European supervisory expectation relating to initial scoping exercises of potential use cases for the implementation of innovative customer onboarding technologies. Provide that financial and credit institutions when considering whether to adopt a new remote customer onboarding solution, credit and financial institutions should carry out a pre-implementation assessment of the remote customer onboarding solution. This assessment should set out the scope, steps and record-keeping requirements of the pre-implementation assessment in their policies and procedures, which should include at least (European Banking Authority, 2023a, p. 13):

- an assessment of the adequacy of the solution regarding the completeness and accuracy of the data and documents to be collected, as well as of the reliability and independence of the sources of information it uses;
- an assessment of the impact of the use of the remote customer onboarding solution on its business-wide risks, including ML/TF, operational, reputational and legal risks;
- the identification of possible mitigating measures and remedial actions for each risk identified in the assessment under the letter;
- tests to assess fraud risks, including impersonation fraud risks and other information and communications technology and security risks; and
- an end-to-end testing of the functioning of the solution targeting customer(s), product(s) and service(s) identified in the remote customer onboarding policies and procedures.

The conduction a pre-implementation assessment and satisfying competent authorities of that the aforementioned assessment has considered ML/TF and the appropriateness of the solution in light of types of customers, services, geographies, products and the wider integration considerations in light of the institutions internal control framework. Remain central to satisfying a competent authority of the business case for implementation of the solution (European Banking Authority, 2023a, p. 14).

Remote customer onboarding solutions: ongoing monitoring

The continuation of a proactive prioritisation of a risk-sensitive approach in using innovative customer onboarding solutions requires credit and financial institutions to ensure continuous monitoring of the innovative solution. This should comprise ensuring that the solution is operating within the envisaged key performance and key risk indicators. Preventative:, mitigative and corrective controls should complement internal policies and procedures. Internal documentary stipulations in conjunction with process and assurance controls should at least (European Banking Authority, 2023a, p. 14).

(1) capture the steps they will take to be satisfied with the ongoing quality, completeness, accuracy and adequacy of data collected during the remote customer onboarding process, which should be commensurate to the ML/TF risks to which the credit and financial institution is exposed;

(2) the scope and frequency of such regular reviews; and

(3) the circumstances that will trigger ad hoc reviews, which should include at least:

- changes to the ML/TF risk exposure of the credit and financial institution;
- deficiencies in the functioning of the solution detected in the course of monitoring, auditing or supervisory activities;

- a perceived increase in fraud attempts; and
- changes to the legal or regulatory framework.

Credit and financial institutions should set out in their procedures and processes remedial measures where a risk has materialised or where errors have been identified that have an impact on the efficiency and effectiveness of the general remote customer onboarding solution. These measures should include at least (European Banking Authority, 2023a, p. 15):

(1) review of all affected business relationships to assess whether sufficient initial CDD has been applied by the credit and financial institutions and prioritise those business relationships that carry the highest ML/TF risk;

(2) taking into account the information obtained in the above-mentioned review, an assessment of whether an affected business relationship should be:

- subject to additional due diligence measures;
- subject to limitations, such as limits on the volume of transaction, where permitted under national law, until such time as a review has taken place;
- terminated;
- reported to the FIU; and
- reclassified into a different risk category.

The continuation of a proactive prioritisation of a risk-sensitive approach to using innovative customer onboarding solutions also requires credit and financial institutions to consider the most effective way to monitor the ongoing adequacy and reliability of the remote customer onboarding solutions. They should consider one or more of, but not be limited to, the following means: (European Banking Authority, 2023a, p. 15).

- quality assurance testing;
- automated critical alerts and notifications;
- regular automated quality reports;
- sample testing; and
- manual reviews.

More generally, credit and financial institutions should be able to demonstrate to their competent authorities which reviews they carried out and the remedial steps they have taken to rectify any shortcomings identified throughout the lifetime of the remote customer onboarding solution (European Banking Authority, 2023a, p. 15).

Remote customer onboarding solutions: customer identification

Internal policies and procedures are central to managing regulatory risk relating to the pre-implementation, implementation and ongoing use of innovative solutions. They require credit and financial institutions to identify natural persons, legal entities and the nature and purpose of the business relationship. Prior to execution of business services. This should comprise at least the following information: (European Banking Authority, 2023a, pp. 16–19).

- is manually entered by the customer;
- is automatically captured from the documentation provided by the customer;
- is gathered using other internal or external sources;
- all relevant data and documentation to identify and verify the legal person;

- all relevant data and documentation to verify that the natural person acting on behalf of the legal person is legally entitled to act as such; and
- the information regarding the beneficial owners.

Where credit and financial institutions accept reproductions of an original document and do not examine the original document, they should take steps to ascertain that the reproduction is reliable. Credit and financial institutions should establish at least the following (European Banking Authority, 2023a, p. 18):

- if the reproduction includes security features embedded in the original document and if the specifications of the original document that are being reproduced are valid and acceptable, in particular, the type, size of characters and structure of the document, by comparing them with official databases;
- whether personal data has been altered or otherwise tampered with or, where applicable, whether the picture of the customer embedded in the document was not replaced;
- whether the integrity of the algorithm used to generate the unique identification number of the original document, in case the official document has been issued with a machine-readable zone (MRZ);
- whether the provided reproduction is of sufficient quality and definition so as to ensure that relevant information is unambiguous; and
- that the provided reproduction has not been displayed on a screen based on a photograph or scan of the original identity document.

Where credit and financial institutions use features to automatically read information from documents, such as optical character recognition algorithms or MRZ verifications, they should take the steps necessary to ensure that these tools capture information in an accurate and consistent manner. In situations where the device the customers use to prove their identity allows the collection of relevant data, for example, because the data is contained in the chip of a national identity card and it is technically feasible for credit and financial institutions to access this data, credit and financial institutions should consider using this information to verify its consistency with the information obtained through other sources, such as the submitted data or other documents submitted by the customer. Verifying the security features embedded in the official document, if any, such as holograms, can be used as a proof of their authenticity (European Banking Authority, 2023a, p. 18).

Matching customer identities as part of the verification process

Where the remote customer onboarding solution involves the use of biometric data defined as "personal data relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data, which is obtained and processed using technical means" (European Banking Authority, 2023a, p. 11), to verify the customer's identity, credit and financial institutions should make sure that the biometric data is sufficiently unique to be unequivocally linked to a single natural person. Credit and financial institutions should use strong and reliable algorithms to verify the match between the biometric data provided on the submitted identity document and the customer being onboarded. In situations where the solution does not provide the required level of confidence, additional controls should be applied. 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 interrupted, restarted or redirected to face-to-face verification. Remote customer onboarding solutions implemented by credit and financial institutions should, as a minimum, allow for the following as part of their verification process: (European Banking Authority, 2023a, p. 19).

- There is a match between the visible information of the natural person and the documentation provided.
- Where the customer is a legal entity, it is publicly registered, where applicable.
- Where the customer is a legal entity, the natural person who represents it is entitled to act on its behalf.

Where possible, credit and financial institutions should use remote customer onboarding solutions that include randomness in the sequence of actions to be performed by the customer for verification purposes to guard against risks such as the use of synthetic identities or coercion. Additionally, where possible, credit and financial institutions should also provide random assignments to the employee responsible for the remote verification process to avoid collusion between the customer and the responsible employee. Credit and financial institutions using unattended remote onboarding solutions, in which the customer does not interact with an employee to perform the verification process, should (European Banking Authority, 2023a, pp. 19–20):

- ensure that the quality of the image and audio is sufficient to allow the proper verification of the customer's identity and that reliable technological systems are used;
- foresee the participation of an employee who has sufficient knowledge of the applicable AML/CFT regulation and security aspects of remote verification and who is sufficiently trained to anticipate and prevent the intentional or deliberate use of deception techniques related to remote verification and to detect and react in case of their occurrence; and
- develop an interview guide defining the subsequent steps of the remote verification process as well as the actions required from the employee. The interview guide should include guidance on observing and identifying psychological factors or other features that might characterise suspicious behaviour during remote verification.

The EBA requires credit and financial institutions to identify preventative, mitigative and corrective controls. The aforementioned should complement internal policies and procedures by increasing the reliability of the verification process. These controls or measures may include, but are not limited to, the following (European Banking Authority, 2023a, p. 20):

- 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.
- Send a randomly generated passcode to the customer to confirm their presence during the remote verification process. The passcode should be a single-use and time-limited code.

- Capture biometric data to compare them with data collected through other independent and reliable sources.
- Telephone contacts with the customer.
- Direct mailing (both electronic and postal) to the customer.

Remote customer onboarding solutions: third-party outsourcing

The continuation of a proactive prioritisation of a risk-sensitive approach in using third-party vendors requires credit and financial institutions to ensure continuous monitoring of the innovative solution. This should comprise ensuring that the solution is operating within the envisaged key performance and key risk indicators. Preventative, mitigative and corrective controls should complement internal policies and procedures. Internal documentary stipulations, in conjunction to process and assurance controls, should determine which remote customer onboarding functions and activities will be carried out or performed by the credit and financial institution, by third parties or by another outsourced service provider. Credit and financial institutions should also apply the following criteria (European Banking Authority, 2023a, p. 21):

- Take the steps necessary to be satisfied that the third party's own CDD remote customer onboarding processes and procedures and the information and data they collect in this context are sufficient and consistent.
- Ensure the continuity of the business relationships established between the customer and the credit and financial institution to guard against events that might reveal shortcomings in the remote customer onboarding process carried out by the third party.

In instances where credit and financial institutions outsource all or parts of the remote customer onboarding process to an outsourced service provider, where applicable, before and during the business relationship with the outsourced service provider, the following measures should be taken, the extent of which should be adjusted on a risk-sensitive basis (European Banking Authority, 2023a, p. 22):

(1) Ensure that the outsourced service provider effectively implements and complies with the credit and financial institution's remote customer onboarding policies and procedures in accordance with the outsourcing agreement. This should be achieved through regular reporting, ongoing monitoring, on-site visits or sample testing.

(2) Carry out assessments to ensure that the outsourced service provider is sufficiently equipped and able to perform the remote customer onboarding process. Assessments may include, but are not limited to, the assessment of staff training, technology fitness and data governance at the outsourced service provider.

(3) Ensure that the outsourced service provider informs the credit and financial institutions of any proposed changes to the remote customer onboarding process, or any modification made to the solution provided by the outsourced service provider.

(4) Where the outsourced service provider stores customer data, including, but not limited to, photography, videos and documents, during the remote onboarding process, credit and financial institutions should ensure that:

(5) only necessary customers' data is collected and stored in line with a clearly defined retention period;

(6) access to the data is strictly limited and registered; and

(7) appropriate security measures are implemented to ensure that the stored data is protected.

Remote customer onboarding solutions: trust services and national identification processes

The EBA envisages instances whereby credit and financial institutions may use relevant trust services and electronic identification processes regulated, recognised, approved or accepted by the relevant national authorities. Their expectation is for credit and financial institutions to conduct an assessment detailing an examination of the solution in light of EBA requirements. Providing rationale as to the preventative, mitigative and corrective control measures implemented to mitigate any relevant risks arising from utilisation of the solution. Specifically considering the following scenarios (European Banking Authority, 2023a, p. 23):

- the risks involved in the authentication and set out in their policies and procedures specific mitigation measures, especially with regard to impersonation fraud risks;
- the risk that the customers' identity is not the claimed identity; and
- the risk of lost, stolen, suspended, revoked or expired identity evidence, including, as appropriate, tools to detect and prevent the use of identity frauds.

Remote customer onboarding solutions: national hesitation?

Case (ECLI:EN:CBB:2022:707, 2023) provides an illustration of a pre-EBA/GL/2022/15 challenge to elements of the use of innovative remote customer onboarding solutions from a Netherlands perspective. More generally, the challenge concerned matters relating to: (a) policies, procedures and measures relating to risk profile and transaction patterns; (b) the transaction monitoring system; and (c) CDD (ECLI:EN:CBB:2022:707, 2023, para 1.3).

From the perspective of utilisation of remote customer onboarding solutions, "Bunq", an online bank, tries to use technological knowledge to improve and innovate its processes. (ECLI:EN:CBB:2022:707, 2023, para 4.11). More specifically, an argument provided by Bunq accepted by the Dutch Multiple Chamber (ECLI:EN:CBB:2022:707, 2023, para 8.63) was that the relevant national expectation in Article 3, second paragraph, introductory sentence and point (c) of the Wwft did not prescribe how CDD is to be carried out, but that obtaining information about the purpose and intended nature of the business relationship must enable an institution to assess any risks that the provision of services to a customer entails. This Dutch illustration identifies that from a national supervisory evaluation perspective, in the event that national legislative provisions do not expressly preclude the use of remote customer onboarding innovative solutions, an arguable case will remain available to an institution that the utilisation of remote onboarding solutions is legal and appropriate.

Article 13(1)(a) of Directive (EU) 2015/849 (Directive (EU) 2015/849 of the European Parliament and Council of May 2015 on the prevention of the use of the financial system

for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70 EC (p. 19) identifies that identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification can be approved or accepted by relevant national authorities.

The inception of this article details a clear EBA and FATF preference (subject to the implementation of appropriate control measures to regulate the pre-assessment and ongoing monitoring of ML/TF risks associated with the utilisation of remote customer onboarding innovative solutions) for leveraging current and emerging AML/CTF technologies. Generally speaking, national competent authorities are unlikely in light of the aforementioned policy statements. To introduce blanket bans on the use of said solutions. Rather, their task will most likely remain to carry out internal suitability assessments of individual service providers solutions in light of the evaluation of individual institutions ability to implement these solutions in mitigation of ML/TF risks. Consolidating macroprudential data, to identify the success of remote customer onboarding solutions; and more generally innovative solutions in combating ML/TF risks. From a supervisory data evaluation standpoint, we are currently at the inception period of the examination of the successful ability of innovative solutions to combat financial crime risks. It is clear that while policy has moved to acceptance of these solutions. Acceptance and continued use of these solutions are contingent on the ability of individual institutions to satisfy national competent authorities that the potential negative implications of solution implementation are mitigated appropriately through internal preventative, mitigative and corrective controls. Therefore, hesitancy remains on the ability of credit and financial institutions to use technological solutions as a "magic solution" in preventing the materialisation of ML/TF related risks.

Conclusion

Technological advancements in biometric data and software tools provide a unique opportunity to address potential paper customer onboarding process deficiencies. Electronic remote customer onboarding solutions equip credit, financial institutions and investment firms with an alternative FTE cost-saving solution in their pursuit of revenue generation. While the EBA and FATF have provided approval for the utilisation of innovative solutions and AML technologies in combating financial crime, hesitancy remains on the ability of credit and financial institutions to use technological solutions as a "magic solution" in preventing the materialisation of ML/TF-related risks. An analysis of policy suggests a gravitation towards the increased use of the aforementioned technologies in the interim.

Conflict of interest and data availability statement agreement

I Daniel Cookman agree to abide by and conform with the terms and conditions of the Journal of Money Laundering Control's conflict of interest and data availability policies and statements and to policies relating as they pertain to the submission of my journal article titled:

"*EUROPEAN APPROCH TO REMOTE CUSTOMER ONBOARDING SOLUTIONS*"

Dated:

30 August 2023

Signed:

Daniel Cookman,

Principal Owner,

EVHC Consulting Ltd,

LL.M.

References

ECLI:EN:CBB:2022:707 (2023).

European Banking Authority (2023a), "Final report guidelines on the use of remote customer onboarding solutions under article 13(1) of directive (EU) 2015/849", EBA/GL/2022/15, pp. 1-45.

European Banking Authority (2023b), "Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process", JC 2017 81, pp. 1-19.

Financial Action Task Force (2023), "Opportunities and Challenges of New Technologies for AML/CFT", pp. 1-49.

Corresponding author
Daniel Cookman can be contacted at: dannycookman@gmail.com