JC 2017 81

23 January 2018

OPINION ON THE USE OF INNOVATIVE SOLUTIONS BY CREDIT AND FINANCIAL INSTITUTIONS IN THE CUSTOMER DUE DILIGENCE PROCESS

LEGAL BASIS

1. The competence of the European Supervisory Authorities' (ESA)'s (the European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority) to deliver an opinion is based on Article 29(1) (a) and Article 56 of Regulation (EU) No 1093/2010[1], Article 29(1) (a) and Article 56 of Regulation (EU) No 1094/2010,[2] and Article 56 of Regulation (EU) No 1095/2010[3], as anti-money laundering and countering the financing of terrorism (AML/CFT) relate to the ESAs' area of competence.

2. This Opinion is addressed to competent authorities as defined in point (ii) of Article 4(2) of Regulation (EU) No 1093/2010, point (ii) of Article 4(2) of Regulation (EU) No 1094/2010 and point (ii) of Article 4(3) of Regulation No 1995/2010.

BACKGROUND

3. Over the past few years, financial transactions and business relationships have become increasingly digitised, creating customer expectations of almost instantaneous access to, and delivery of, financial products and services. Consequently, firms are compelled to adapt their practices to stay competitive. While the move towards a more technologically driven

[1] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

[2] Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC.

[3] Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC.

financial services market presents many benefits, which include reduced costs, improved customer experience, increased speed of transactions, reduced account opening times and continuous access to services online, firms have to be mindful of the impact these changes might have on their money laundering and terrorist financing (ML/TF) risk exposure.

4. Innovation is not confined to new financial products and services. It also includes the development of new solutions to address specific compliance challenges, such as customer due diligence (CDD), which is central to the AML/CFT regime. Meeting CDD obligations can be challenging for firms, as this process is often associated with significant costs and customer inconvenience.

5. Additional challenges arise from the fact that in an increasingly digitised environment, where most services are accessible online, firms may have to move away from traditional face-to-face interactions to non-face-to-face online channels.

6. CDD therefore offers considerable scope for financial innovation that can improve the effectiveness and efficiency of AML/ CFT controls. Nevertheless, 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.

7. As European standard-setters responsible for fostering the consistent application of AML/CFT standards across the European Union the ESAs aim to promote the development of a common approach across Member States to the use of innovative solutions by firms in their CDD processes. The ESAs believe that a common approach will prevent regulatory arbitrage, create a level playing field and strengthen Europe's AML/CFT defences, while at the same time fostering the use of those innovations to make AML/CFT systems and controls more effective and efficient.

To this end, this Opinion:

- highlights the factors that the ESAs believe competent authorities should consider when:
  - assessing the adequacy of firms' CDD measures where innovative solutions are used and the application of such measures by firms; and

- assessing controls in place at firms that enable them to mitigate any risks associated with innovative solutions;

- aims to develop common regulatory understanding of the appropriate use of innovative solutions.

DEFINITIONS

8. For the purpose of this Opinion, the definitions contained in Directive (EU) 2015/849 and the following definitions shall apply:

'Firms' means credit institutions and financial institutions as defined in Article 3 (1) and (2) of Directive (EU) 2015/849.

'Competent authorities' means the authorities competent for ensuring firms' compliance with the requirements of Directive (EU) 2015/849 as incorporated into national legislation[4].

'Customer' means any person who enters into a business relationship or carries out an occasional transaction with firms.

LEGAL FRAMEWORK

9. The EU's AML/CFT framework is set out in Directive (EU) 2015/849,[5] which came into force on 26 June 2015, and Regulation (EU) 2015/847[6]. Directive (EU) 2015/849 provides that firms are required to assess ML/TF risks, and to put in place effective AML/CFT policies and procedures to mitigate these risks. The Directive requires that these policies and procedures include CDD measures, which consist of a duty to:

- identify the customer (and, where applicable, the beneficial owner and beneficiary) and verify the customer's (and beneficial owner's and beneficiary's) identity on the

[4] Article 4(2)(ii), Regulation (EU) No 1093/2010, Article 4(2)(ii), Regulation (EU) No 1094/2010, Article 4(3)(ii), Regulation (EU) No 1093/2010.

[5] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 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.

[6] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

basis of documents, data or information obtained from 'reliable and independent sources';

- assess and, as appropriate, obtain information on the purpose and intended nature of the business relationship; and
- carry out on-going monitoring of business relationships and transactions.[7]

Similarly, Regulation (EU) 2015/847 requires that the accuracy of certain information accompanying fund transfers is verified on the basis of data, documentation or information from reliable and independent sources.

10. EU law[8] does not specify what 'reliable and independent sources' are. This means that, to the extent permitted by national legislation, firms have some flexibility regarding the sources of information they use to meet their CDD obligations. For example, while official documents such as passports (for natural persons) or certificates of incorporation (for legal persons) are largely relied upon by firms to verify their customers' identity, EU law does not prevent the verification of the customer's identity on the basis of alternative reliable and independent documents, data and information, as long as firms can demonstrate to their competent authority that the use of particular sources is commensurate with the ML/TF risks presented by the underlying business relationship.

11. Furthermore, EU law no longer designates situations where a customer is not physically present for identification purposes as high risk in all cases. Instead, Annex III to Directive (EU) 2015/849 lists non-face-to-face business relationships or transactions 'without certain safeguards' as 'potentially higher risk' in recognition of approaches to non-face-to-face verification of identity becoming more reliable.

12. However, since Directive (EU) 2015/849 lays down only minimum CDD requirements that firms must comply with, Member States have some flexibility in imposing more stringent standards through their national legislation where this is necessary in the light of the ML/TF risk.

[7] Article 13, Directive (EU) 2015/849.

[8] Directive (EU) 2015/849 and Regulation (EU) 2015/847.

TYPES OF INNOVATIVE SOLUTIONS CURRENTLY USED IN THE CDD PROCESS

13. When considering the use of innovative solutions in their customer identification and verification processes, firms are generally driven by the demand for improved customer experience and cost savings. Therefore, many of the innovative solutions currently used by firms contain features that address these demands and can be broadly grouped into two categories:

    - Firstly, there are innovative solutions that often involve non-face-to-face verification of customers' identity on the basis of traditional identity documents (e.g. a passport, a driving licence or a national identity card) through various portable devices such as smartphones; and

    - Secondly, there are innovative solutions that enable the verification of customers' identity through other means, e.g. central identity documentation repositories (often referred to as 'KYC utilities'). These repositories are generally set up as a joint venture or a co-operative between a number of firms, or as an outsourcing arrangement between a number of firms and an external provider, which may or may not be an obliged entity under Directive (EU) 2015/849. These repositories aim to streamline the collection and exchange of CDD data and documentation between participating firms and their customers, thereby avoiding the same information being requested repeatedly from the same customer.

14. Where innovative solutions are designed to monitor business relationships and transactions, they often replace or supplement traditional transaction monitoring (which is based on pre-set 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:

    - 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 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.

FACTORS TO BE CONSIDERED

15. In the ESAs' view, competent authorities should consider a number of factors when assessing the extent to which the use or intended use of innovative CDD solutions is adequate in the light of the ML/TF risk associated with individual business relationships and firms' business-wide risk profiles. These factors are technology-neutral and apply in addition to the customer, product, services, transaction, delivery channel and geographical risk factors[9] firms should consider when assessing the risks associated with their business relationships, in line with Article 8 of Directive (EU) 2015/849 and Risk Factors Guidelines[10]. In particular, competent authorities should consider:
    - oversight and control mechanisms;
    - the quality and adequacy of CDD measures;
    - the reliability of CDD measures;
    - delivery channel risks; and
    - geographical risks.

[9] Annex III, Directive (EU) 2015/ 849 and the ESAs' Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849.

[10] Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and firms should consider when assessing the money laundering and terrorist financing risk associated with individual business relationship and occasional transactions.

16. In addition to the above factors, when firms make use of or intend to make use of innovative solutions for CDD purposes, competent authorities should take into account the potential impact that this may have on firms' overall risk profiles. To adequately oversee and gain reasonable assurances that the innovative CDD solution is and will be operating appropriately and to prepare for situations should the solution breaks down or fails, firms should have a full and thorough understanding of its features. To ensure this, competent authorities should consider in particular whether or not the firm has sufficient in-house expertise, in addition to any external expert advice, to guarantee the implementation and use of the innovative solution as well as to ensure the continuation of services should the innovative solution suffer irreparable system failure or the termination of a business relationship between the firm and an external provider of the solution (where it is not developed in-house). This includes the assessment of:

    - whether or not firms have appropriate technical skills to oversee the development and proper implementation of innovative solutions, particularly where these solution are developed or used by a third party (where reliance is placed on such third party in line with Article 25 of Directive (EU) 2015/849) or an external provider;
    - whether or not the senior management and the compliance officer have appropriate understanding of the innovative solution; and
    - whether or not firms have proper contingency plans in place.

OVERSIGHT AND CONTROLS MECHANISMS

17. There are various ways in which firms can utilise innovative CDD solutions as part of their CDD process and Directive (EU) 2015/849 does not prevent the use of such solutions where proper safeguards have been put in place to mitigate any ML/TF risks. Most commonly, these solutions are:

    - developed in-house;
    - provided by an external provider;
    - used by a third party where the firm places reliance on such third party in line with Article 25 of Directive (EU) 2015/849; or

- used by an external provider to which the firm has outsourced its CDD processes[11].

However, the options available to firms may be limited by national legislation in their Member State. Notwithstanding the means chosen to employ innovative CDD solutions, the responsibility for meeting the AML/ CFT obligations remains with the firms. The ESAs therefore believe that the competent authorities should consider, in addition to the firms' risk assessment[12], at least the factors set out below when assessing the adequacy of firms' governance and controls frameworks in the context of their decision to use the innovative CDD solutions for AML/ CFT compliance purposes:

a. Does the innovative solution's design and service offering includes appropriate risk management systems that are compatible with products and services offered by firms, especially when the solution is not developed in-house? Before introducing an innovative solution in their CDD process, the ESAs believe that firms should carry out a full assessment of the solution to ensure that it has undergone proper testing and to establish whether or not the solution allows the application of CDD measures in line with firms' AML/CFT policies and procedures and applicable AML/ CFT law. Where the assessment results are inconclusive, firms should maintain their traditional systems parallel to the innovative solution for as long as they have full confidence in the new solution. The assessment should be provided to the competent authorities on request. The ESAs consider it necessary for the compliance and/or risk officer to be involved in this assessment, especially in circumstances where firms are considering a number of external providers, and at all implementation stages thereafter.

b. Do firms retain sufficient decision-making powers, specifically in respect of changes proposed to the innovative solution, the on-boarding process or the applicable CDD measures? The ESAs expect the competent authorities to ensure that firms have a written arrangement in place (where the innovative solution has not been developed in-house) detailing the roles and responsibilities of each party as well as providing guarantees that the firm should be informed of, and have decision-making powers over, any changes proposed to the innovative solution or the CDD measures and processes.

[11] Recital 36 and Article 29 of Directive (EU) 2015/849.

[12] Article 8 of Directive (EU) 2015/849.

c. Is a process in place that would ensure continuous monitoring of the innovative solution's effectiveness? The ESAs believe that firms should ensure that the innovative solution is regularly assessed and that any errors and weaknesses identified as a result of such assessment are corrected without delay. Where weaknesses related to the customer on-boarding process have been identified, this should trigger:

   - a review of all affected business relationships, to assess whether sufficient CDD has been applied in line with firms' policies and procedures;
   - an assessment, after the weaknesses have been corrected and adequate CDD has been applied, of whether, based on the new information, any affected business relationships can be maintained or should be terminated, and/or the execution of transactions related to such business relationships should be stopped; and
   - an assessment of whether or not a Suspicious Transaction Report (STR) should be raised.

d. Where firms have identified serious weaknesses in the innovative solution or systematic errors related to the use of the innovative solution, in addition to the above steps, the ESAs believe that they should also re-evaluate:

   - whether or not the level of reliability of the innovative CDD solution is justifiable against the level of ML/TF risks presented by their customers and business relationships;
   - the need for any improvements to the innovative CDD solution; and
   - the continuation of the use of the solution.

e. Are controls in place to ensure that firms are meeting their data retention requirements, regardless of the type of innovative solution? The ESAs believe that competent authorities should ensure that firms keep all necessary records that enable them to determine the receipt date and applicable retention period for the documentation, information and data received as part of the CDD process through innovative solutions. The ESAs consider that this could be achieved by carrying out regular monitoring of data stored in-house or externally, and by testing the agreed retention periods. On request from the competent authorities, firms should be able to provide copies of records held without delay.

f. Are controls in place to prevent any data security and privacy breaches? The ESAs consider that competent authorities should ensure that firms have effective controls in place to

demonstrate that high standards of data and IT security are adhered to, including where data storage has been outsourced to a cloud service provider.

g. Have sufficient safeguards been put in place by firms to ensure that the use of innovative solutions as part of their customer identification and verification processes does not lead to a breach of data protection legislation or other relevant legislation? In the ESAs' view, firms should confirm to their competent authorities that they have examined and addressed any possible data protection or other legal implications, and have put in place additional safeguards, if required, especially where CDD documentation is gathered in a central repository maintained by an external provider.

h. Are sufficient controls in place to ensure that staff conducting the identity verification of customers through innovative solutions are not colluding with criminals? This is not a unique factor applicable only to innovative solutions. Nerveless, it is an important one and the ESAs believe that competent authorities should ensure that there are controls in place to reduce the risk of collusion through pre-employment screening, random allocation of customers or screening of employee communications.

i. Are sufficient controls in place to ensure that staff using the innovative solutions are sufficiently trained? It is the ESA's expectation that competent authorities ensure that all relevant staff employed by firms, and also staff at the external provider, are provided with regular training which specifically focuses on the practical application of the innovative solution and its technical abilities as well as on the detection and escalation of potentially suspicious transactions arising from the use of the innovative solution. Such training should be provided in addition to ongoing general AML/ CFT training.

j. Are there any compliance and operational risks that should be considered by firms before commencing the use of an innovative CDD solution? In addition to ML/TF risks assessed in line with Article 8 of Directive (EU) 2015/849, the ESAs consider that competent authorities should also ensure that firms have identified and assessed other risks associated with the innovative solution and also the external provider (where the solution is not developed in-house). All such risks should be reflected in their business-wide risk assessment, and proper contingency plans should be put in place to ensure continuity of services. For example, where the innovative solution has been provided or developed by an external provider which is in its infancy, firms should assess risks arising from a possible failure of that provider due to bankruptcy or lack of funding, or irreparable system failure, or the likelihood

of the innovative solution becoming obsolete and the transferability of data in such a scenario.

k. Are there laws that do not permit information sharing between the external provider of the innovative solution and the firm, and/or between the external provider and the competent authority where these external providers are based in third countries? Firms are solely responsible for meeting their AML/CFT obligations regardless of the external provider's location. Therefore where firms are unable to meet their AML/CFT obligations because of legal obstacles in third countries where their external providers are located and where such obstacles cannot be overcome, firms should not engage with such external providers.

QUALITY AND ADEQUACY OF CDD MEASURES

18. Article 13(4) of Directive (EU) 2015/849 requires firms to demonstrate to their competent authority that the extent of CDD measures is commensurate with the ML/TF risks they have identified. This means that, based on their analysis of the innovative solution's characteristics and the assessment of ML/TF risks linked to their customers and business relationships, firms should be able to demonstrate to their competent authorities that the innovative solution is sufficiently reliable and commensurate with the level of ML/TF risks presented. Furthermore, the ESAs believe that competent authorities should also consider the following factors.

a. Are sufficient controls in place to ensure that a business relationship with a customer commences only once all CDD measures commensurate with the ML/TF risk have been applied? The final decision regarding the commencement of a new business relationship, including the acceptance of a high-risk customer and the formal approval of a business relationship with a PEP, lies solely with firms, as they remain accountable for the adequate and proper application of CDD measures which, at times, may need to be supplement with additional measures. This is particularly relevant when the identification and verification of customers are carried out through innovative solutions by external providers or third parties.

b. Are controls in place to ensure the quality of the CDD measures applied and also the quality of data and information used or collected when carrying out CDD through innovative solutions, including on-going and transaction monitoring? The ESAs believe that competent authorities should ensure that firms fully oversee their CDD process on an on-going basis, regardless of whether the CDD is carried out internally or externally by third parties or

external providers. Such an oversight framework may include, among other things, regular assurance testing, ongoing compliance monitoring and reviews by the Internal Audit function. Competent authorities may also require that assessment of the innovative solution be included in the scope of the existing regular external audit review, or request that an ad hoc external audit review be carried out on the innovative solution to ensure its proper implementation. However, this should be commensurate with the nature, scale and complexity of firms' business and ML/TF risks associated with the sector. Where the innovative solution is not developed in-house or the CDD process is carried out by an external party, such reviews may be supported by on-site visits to ensure that the solution is functioning properly in practice. Where any issues are identified, appropriate reporting and governance should be in place to ensure its timely escalation, along with the suitability of the innovative CDD solution being subject to review and discussion on a regular basis.

c. With regard to innovative solutions for ongoing monitoring purposes, are controls in place to ensure that innovative solutions are operating effectively and efficiently? The ESAs consider it pertinent for the competent authorities to ensure that firms have considered the following factors:
   - Can the innovative solution be integrated with firms' existing workflows and legacy systems? The ESAs believe that the innovative solution should be fully integrated with current and legacy systems used by firms and should have full access to all available information on their customers across multiple accounts (current and historical) and networks.
   - Are firms able to determine and assess what data and information sources are used in the on-going monitoring process? Where firms are relying on innovative solutions to perform ongoing monitoring of customer relationships, in the ESAs' view, they should be able to demonstrate to their competent authorities their understanding of data and information sources used in this process. For example, where information comes from government databases or registers, such information may be considered sufficiently reliable and form part of customers' ML/TF risk assessment, as well as be taken into account in other decisions relating to business relationships. In comparison, for example, information obtained from newspapers or blogs may be considered less reliable; however, it may serve as a trigger for further investigations and information gathering.
   - Is the innovative solution able to develop a sufficiently informed view of which transactions should be considered potentially suspicious or unusual? Generally, such views are developed on the basis of historical data and patterns, and particularly

transactions that have been reported to the Financial Intelligence Unit (FIU). Therefore, the level of data completeness may play an important role in generating more precise monitoring results. However, this may prove to be challenging and, in the absence of any feedback from the FIUs, firms may need to consider using other sources of information when developing potentially suspicious transaction patterns.

- Do innovative solutions used by firms enable them to develop a holistic view of their customers' profiles, including their transactions, and identify linkages between customers, entities, payments, etc.? This could be achieved by simultaneously linking customers' transaction patterns with static data held in firms' databases and information gathered from other multiple data sources, e.g. government registers, device/ machine fingerprinting, online news and publications, social media (to the extent permitted by national legislation) and public databases and registers.

d. Are controls in place to ensure that documentation, data and information gathered during the customer on-boarding process through innovative solutions remains accurate and up to date? Firms remain responsible for the application of on-going CDD measures related to their customers, regardless of the means used to apply these measures or whether they have been applied internally or by external parties.

RELIABILITY OF CDD MEASURES

19. It is important that firms have regard to the validity and authenticity of data, documentation and information obtained in respect of their customers through innovative solutions at on-boarding or during the business relationship. Where customers are required to transmit their ID documentation, data or information via video conferences, mobile phone apps or other digital means, the ESAs believe that competent authorities should ensure that firms have considered at least the factors set out below.

a. Is there a risk that the customer's image visible on the screen is being tampered with during the transmission? The ESAs believe that competent authorities should ensure that firms have sufficiently robust controls in place to prevent or reduce such risk. These controls may include some or all of the following:

- a feature whereby a customer is required to have a live chat with an administrator who has received specialised training in how to identify possible suspicious or unusual behaviour or image inconsistencies;

- a built-in computer application that automatically identifies and verifies a person from a digital image or a video source (e.g. biometric facial recognition);

- a requirement for a screen to be adequately illuminated when taking a person's photograph or recording a video during the identity verification process;

- a built-in security feature that can detect images that are or have been tampered with (e.g. facial morphing) whereby such images appear pixelated or blurred.

b. Is there a risk that an ID document displayed on the screen by a customer during the transmission belongs to another but similar-looking person? The ESAs consider that firms should ensure that the innovative CDD solution contains built-in features that enable it to identify any discrepancies, or that staff responsible for the identify verification during the transmission have been trained to spot situations where the person on the screen looks different from the person on the ID document.

c. Are controls in place to ensure that identity documents produced during the transmission have not been altered (i.e. changes made to data in a genuine document), counterfeited (i.e. reproduction of an identity document) or recycled (i.e. creation of a fraudulent identity document using materials from legitimate documents)? The ESAs believe that firms should have sufficient controls in place to prevent or reduce the risk of these breaches, which may include one or more of the following:

- built-in features which enable them to detect fraudulent documents on the basis of the documents' security features (i.e. watermarks, biographical data, photographs, lamination, UV-sensitive ink lines) and the location of various elements in the document (i.e. optical character recognition);

- features that compare the security features ingrained in the identity document presented during the transmission with a template of the same document held in the firms' internal identity document database;

- limiting the type of acceptable identity documents to those that contain:

  – high security features or biometric data including finger prints and a facial image (e.g. e-passports and e-ID);

- a qualified electronic signature created in line with standards set in Regulation (EU) No 910/2014 (especially relevant where a customer is a legal person);

- a feature that links the innovative solution with trade registers or other reliable data sources such as the company registration office database; or

- a feature that adjoins the innovative solution with the government-established CDD data repository or the notified e-ID scheme as defined in Regulation (EU) No 910/2014, if the scheme's assurance level is classified as substantial;

- where the verification is not based on a government-issued identity document, to the extent permitted by national law and commensurate with the ML/ TF risk, features that allow firms to verify the information received from their customers against a combination of multiple reliable and independent sources (including, but not limited to, government registers and databases), which can be supplemented with data mining and social network analysis, IP address analysis, and location or device analysis.

d. Are controls in place to ensure that most potentially suspicious transactions have been identified? Where innovative solutions are used in the transaction monitoring process, the ESAs believe that adequate steps should be taken by firms to gauge the quality of the outputs and alerts generated by the system, and compare these with the quality of existing approaches. Firms should be able to demonstrate their understanding of the transaction monitoring process and explain it to the competent authorities.

e. Where innovative solutions are used to assess ML/ TF risks associated with a business relationship, are all available data and information used in this process, and are they considered reliable? To ensure that firms have developed a holistic view of the ML/TF risks presented by a particular business relationship, the ESAs believe that competent authorities should assess whether or not data necessary to carry out the risk assessment are pulled from multiple reliable and independent sources, which may be in different languages, and may include data from the customer's account profile and web login activity, government- or third-party-issued watch-lists, online news and publications, social media, and public databases.

DELIVERY CHANNEL RISKS

20. Directive (EU) 2015/849 considers that non-face-to-face business relationships or transactions without sufficient safeguards are potentially higher risk than face-to-face business relationships. Therefore, there is an expectation that firms carry out an assessment of ML/TF risks associated with non-face-to-face business relationships and the extent to which the use of innovative solutions can address, or might further exacerbate, those risks. As part of this process, the ESAs think that competent authorities should ensure that at least the factors set out below have been considered by firms.

a. Is there a risk that potential customers who are on-boarded via the innovative CDD solution are not who they claim to be as they are impersonating another person or using another person's personal data or identity documents (i.e. identity fraud)? There is an expectation that firms should be able to demonstrate to their competent authorities that they have assessed the availability and effectiveness of safeguards that could mitigate these risks. Such safeguards may include the verification of a customer's identity on the basis of a notified e-ID scheme, as defined in Regulation (EU) No 910/2014, where the scheme's assurance level is classified as high, or a combination of other checks that ensure the information obtained during the transmission can be linked to a particular customer, for example:

- the verification of a customer's identity based on multiple factors and data sources, for example, where the customer's personal information is verified on the basis of a government-issued photographic document, combined with information obtained during the live chat with an administrator and information obtained from the government or other reliable and independent sources and databases;
- built-in features that allow firms to detect their customers' native language based on their written communications with them;
- a requirement that all CDD documentation contains a qualified electronic signature created in line with standards set in the Regulation (EU) No 910/2014;
- verifying a customer's identity on the basis of more traditional processes such as sending a letter to the customer's verified home address.

b. Is there a risk that a customer could be intimidated, threatened or under duress during the transmission of the identity verification? In the ESAs view, firms should have strong controls

in place to identify possible coercion, which may include a built-in technical feature in the innovative solution or a feature whereby a customer is required to have a live chat with an administrator who is well trained to spot any abnormalities in the customer's behaviour, which may assist in identifying situations where the customer is behaving suspiciously (e.g. psychological profiling).

GEOGRAPHICAL RISKS

21. The key feature of most commonly used innovative CDD solutions is that they enable firms to on-board customers remotely and verify their identity via the internet, regardless of customers' location or distance from the firm. This means that customers are no longer required to live in close proximity to firms to use their services, and do not have to be physically present for the identification purposes.

22. With the EU-wide availability of financial services being more common and explicitly supported by the European Commission[13], firms have to remain mindful of the risk that a customer may be looking to access financial services in another Member State for ML/TF purposes.[14] Therefore, the ESAs believe that competent authorities should satisfy themselves of:

- firms' ability to assess geographical risks presented by a business relationship, including through controls firms may have in place that capture their customers' location (e.g. through device fingerprinting or GPS data on mobile phones) to establish if they are based in a jurisdiction associated with higher ML/TF risks; and

- whether or not firms have practices in place to assess the reasons why customers from other jurisdictions are using their services.

[13] See, for example, Regulation (EU) No 910/2014 (eIDAS Regulation), which aims to provide a legal framework to ensure that an e-ID issued in one member state should be accepted for the purposes of identity verification in another member state, among other things; or Directive 2014/92/EU on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features, which entitles all consumers resident in the EU to a basic payments account, in any Member State, irrespective of where they are based.

[14] Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and firms should consider when assessing the money laundering and terrorist financing risk associated with individual business relationship and occasional transactions.

CONCLUSIONS

23. The ESAs consider that innovations and technological developments in financial services can potentially improve the efficiency and robustness of these services while also presenting many other benefits to firms and their customers. Therefore, the ESAs encourage competent authorities to support those developments, especially where they improve the effectiveness and efficiency of firms' AML/CFT compliance.

24. However, the ESAs are mindful that firms and competent authorities need to be aware not only of the benefits but also of the risks and challenges presented by these innovative solutions. It is important that firms can demonstrate to their competent authorities that they have identified, assessed and mitigated all relevant risks before introducing the innovative solution in their CDD process.

25. To foster innovation in financial services, the ESAs believe that there should be a common approach across the Member States, which can be achieved by:

- competent authorities working together and exchanging information and experiences with their counterparts in other Member States;
- competent authorities setting clear regulatory expectations for firms on how they can ensure compliance with their AML/CFT obligations while utilising technological innovations for CDD purposes;
- competent authorities working together with firms and providers of innovative CDD solutions as well as specialist teams from within the competent authority, if needed, to increase their knowledge and understanding on how these solutions can enhance firms' AML/CFT compliance, and why they are not necessarily an obstacle to the AML/ CFT supervision process - the ESAs consider the lack of understanding on behalf of competent authorities not to be a sufficient reason for preventing innovations and technologies from being used by firms to meet their AML/ CFT compliance obligations;
- competent authorities working together with firms to increase their awareness of ML/ TF risks presented by innovative solutions and technologies and also of benefits presented by good AML/ CFT compliance, while not favouring any particular innovative solution or technology;

- competent authorities fostering an environment in which firms inform them of innovative solutions they intend to use - while such notifications would not result in an express approval of a particular solution, the competent authority, to the extent permitted by the national legislation, may decide to take part in this process, especially where the solution will be used by a number of firms and its failure may result in repercussions for the financial services sector (for example, where a repository of identity documentation is being set up by a number of firms, competent authorities may decide to take part in this process from an early stage, as the failure of such a repository may have a negative impact on a large number of customers).

26. The ESAs are committed to working with competent authorities and providing relevant training, where required, and to issuing updated guidance on risk factors associated with innovative technologies and solutions.