CONSULTATION PAPER

(CP-02-2020)

SUBJECT: **IMPROVING THE FACILITATION OF CUSTOMER DUE DILIGENCE WITH INNOVATIVE TECHNOLOGIES**

DATE OF ISSUE: 15 OCTOBER 2020

PURPOSE THIS CONSULTATION PAPER

This Consultation Paper (the "Consultation") helps enact effective consultation procedures with market participants and investors regarding proposed changes in the Cyprus Securities and Exchange Commission's ("CySEC") policy.

IMPORTANT WARNING

The submission of responses should be made **no later than 20 November 2020**. No extension will be given on an individual basis. Therefore, unless CySEC extends the submission period with a formal announcement, any responses received after the above date **will not be considered**.

INSTRUCTIONS FOR THE SUBMISSION OF RESPONSES

Interested parties may submit their responses to the CySEC Policy Department by email at policy@cysec.gov.cy.

The subject of the email should have the following form:

«*Consultation Paper (2020 - 02) – [insert the Name of Organisation, Legal or Natural Person submitting the comments or views]*»

In submitting your responses, you are requested to state whether you represent an organized group or a specific enterprise, or if you are an individual. In the case of organized groups, you are kindly requested to provide information on the number and nature of persons or enterprises you represent.

Please answer the questions in the order presented in this document be concise and provide your replies in a Word document.

CONTENT

1. INTRODUCTION AND BACKGROUND ANALYSIS

1.1. PURPOSE OF THIS CONSULTATION PAPER

1.1.1 The Cyprus Securities and Exchange Commission publishes this consultation paper ('the **CP**') in order to propose the amendment of the provisions of Annex IV of CySEC's Directive 144-2007-08 on The Prevention of Money Laundering and Terrorist Financing ('the **CySEC AMLD'**) as regards customer due diligence, within the meaning of Law 188 of 2007 on the Prevention and Suppression of Money Laundering and Terrorist Financing as in force ('the **AML Law**'), by means of innovative technological methods ('**Innovative Methods**').

1.1.2 The proposed amendment applies to those obliged entities, within the meaning of the AML Law, which fall under CySEC's supervision ('the **Obliged Entities'**)[1], whereas aims:

i. At allowing the use of additional Innovative Methods for the purposes of Paragraph 33(1)(d) of the CySEC AMLD; and

ii. At further facilitating the incorporation of Innovative Methods into the customer due diligence process, within the meaning of the AML Law ('the **CDD**') for identity verification purposes[2], in a prudent and a risk proportionate manner.

1.1.3 While the intention of the CP is to further facilitate the incorporation of innovative technologies by Obliged Entities into the customers' on-boarding process, as a corollary to such facilitation compliance with safeguards that are recommended in this CP will also be required and will have to be documented in a relevant risk assessment. The safeguards that Obliged Entities need to comply with, are the ones outlined in the ESAs Opinion[3] on the use of innovative solutions by credit and financial institutions in the customer due

[1] Such entities being presented in brief under section 2 of the CP 'Who this concerns'.

[2] Article 61(1)(a) of the AML Law.

[3] Available at: https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf

diligence process **(the "ESAs Opinion")** and in the FATF Guidance on Digital Identity[4] **(the "FATF Guidance")**. The application of CDD by means of (additional) Innovative Methods is intended to apply to the non-face to face ('NFTF') identification and verification of identity of natural persons (individuals). Non-face-to-face interactions are considered to occur remotely; meaning the parties are not in the same physical location and conduct activities by digital or other non-physically present means, such as mail or telephone[5]. The key feature of most commonly used innovative CDD solutions is that they enable the identification and verification of identity of individuals without them being required to live in close proximity to Obliged Entities to use their services, and do not have to be physically present for identification purposes

1.1.4 The reason for initiating a consultation on extending the use of innovative technological solutions in the context of CDD procedures is:

i. The significant technological progress that has been achieved in this field[6] which was further confirmed in the context of the work undertaken by the CySEC Innovation Hub (see here). Competent authorities are encouraged at the European level to support those developments, especially where they improve the effectiveness and efficiency of Obliged Entities' AML/CFT compliance[7];

ii. The fact that the number of NFTF customers is expected to rise significantly given the circumstances caused by the COVID-19 pandemic and the changes it brought; and

iii. The fact that the relevant provisions in the CySEC AMLD are currently limited as to the use of Innovative Methods in the field of CDD regarding NFTF identification and verification of identity of natural persons[8]. Despite the current restrictive approach of the CySEC AMLD, the statutory provisions in force, i.e. the primary rules, allow a more extended use of innovative technologies for CDD purposes, subject to the

[4]Available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

[5] Paragraph 87 of FATF Guidance.

[6] Paragraphs 3&5 of the EASs Opinion.

[7] Paragraph 23 of the ESAs Opinion.

[8] Namely limiting, in essence, such use to video-calls, as it emanates from Paragraph 33(1)(d) in conjunction with Annex IV Nr. 2 (iv) of the CySEC AMLD respectively.

requirement that it is data or information obtained from a reliable and independent source[9].

1.2. STRUCTURE OF THE CONSULTATION PAPER

1.2.1. Section 1 contains introductory and background information. Section 2 provides an analytical summary of the content of the ESAs Opinion and of the FATF Guidance.

1.2.2. The reason for such detailed presentation is that those two documents complement each other and both of them collectively further specify the abstract terms employed at the level of the AML Law: The ESAs Opinion provides more generic[10] information about Innovative Methods without delving into the technical details by providing an analysis about idiosyncratic risks (i.e. risks inherent in the technology used). Conversely, the FATF Guidance focuses on technological[11] risks regarding the digital ID systems for identity verification purposes with the aim of achieving the required '*assurance*'[12].

1.2.3. Thus, the ESAs Opinion highlights the factors that need to be considered when assessing:

- The adequacy of Obliged Entities' CDD measures where innovative solutions are used and the application of such measures by the said entities; and
- The controls in place that enable Obliged Entities to mitigate any risks associated with innovative solutions,

whereas the FATF Guidance focuses on the technological aspects[13], in order to achieve the required assurance level. The ultimate goal of this summary is to guide Obliged Entities

[9] Article 13(1) of the Directive 2015/849/EU ('the **EU AMLD'**)/61(1) of the AML Law.

[10] See for example the generic grouping of Innovative Methods under Paragraph 13 of the ESAs Opinion into Innovative Methods allowing verification of identity on the basis of traditional identity documents and secondly verification of customers' identity through other means, e.g. central identity documentation repositories known as KYC utilities. Regarding the risk factors to be considered, they are also generic and non-technical, namely those provided under Annex III of the AML Law and those viewed from an AML risk management framework perspective in general (see e.g. Paragraphs 15/16, 17b-d 18a and 22 of the ESAs Opinion).

[11] See for instance Section IV and Appendix A of the Guidance respectively.

[12] Paragraph 4 of the FATF Guidance: *'...Assurance levels measure the level of confidence in the reliability and independence of a digital ID system and its components*'.

[13] For instance, unlike the general grouping of the Innovative Methods under Paragraph 13 of the ESAs Opinion, Paragraph 32 of the FATF Guidance provides a detailed enumeration thereof. For the avoidance of doubt, where the FATF Guidance uses the term '*technology-neutral*' this means that no specific technology is endorsed and not that technological issues are not taken into consideration.

in familiarising themselves with CySEC's proposal and the corresponding regulator expectations.

1.2.4. The summary of the ESAs Opinion and of the FATF Guidance provided herein is therefore non-exhaustive and may not replace a thorough consideration of the aforesaid documents that should be undertaken by Obliged Entities where they wish to incorporate innovative solutions into their customer on-boarding process.

1.2.5. Annex 1 of the CP contains the proposed amendment of the CySEC AMLD and Annex 2 contains a standardised confirmation (to be submitted to CySEC) on the performance of a relevant risk assessment by Obliged Entities prior to the incorporation of innovative solutions into their customer on-boarding process.

1.3. WHO THIS CONCERNS

1.3.1. PERSONAL SCOPE

1.3.1.1. This CP is addressed to the Obliged Entities as these are more specifically determined by Article 2A in conjunction with Article 59(1)(b) of the AML Law respectively.

1.3.1.2. Without prejudice to the Obliged Entities falling within CySEC's regulatory perimeter, the CP is also of interest to external developers (in case where the Innovative Method is developed externally, while the CDD itself is performed in-house by the Obliged Entity) or outsourcing providers (in cases where the Obliged Entity relies on a third-party provider to perform CDD through the Innovative Method), given the inherently technical nature of the Innovative Method[14]. Within this context of ideas and given that the risk-based approach recommended by the FATF Guidance:

- Relies on a set of open source, consensus-driven assurance frameworks and technical standards for digital ID systems[15]; and

[14] *As* per footnote 8 of the FATF Guidance: *'While the FATF Standards are only applicable to regulated entities (i.e. financial institutions, virtual asset service providers and designated non-financial businesses and professions), this Guidance is relevant background for digital ID service providers who provide service to regulated entities (for FATF purposes). Ultimately, the regulated entity is responsible for the meeting the FATF requirements.'*

[15] Paragraph 4 of the FATF Guidance

- The Guidance draws links between digital ID assurance frameworks and standards and the FATF's CDD requirements.[16]

It is thus recommended by the FATF Guidance that digital ID providers familiarise themselves with the applicable requirements[17], seek assurance testing[18] and Provide transparent information to Obliged Entities in respect of technical matters[19].

1.3.2. MATERIAL SCOPE

1.3.2.1. The material scope of this CP is limited to the NFTF identification and verification of the identity of an individual (natural person), as part of the CDD process as specifically required under Article 61(1)(a) and 61(1)(b) of the AML Law, namely to:

i. Identify the customer and verify the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

ii. Identify the beneficial owner and take reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is.

1.3.2.2. The scope of this CP does not include the cases provided under Article 61(1) (c)-(d) of the AML Law. This does not mean that the Innovative Methods considered herein, could not be potentially applied to such cases as well. However, such application might require different assessments and safeguards, which do not form part of the CP.

1.4. CURRENT STATE OF THINGS

1.4.1. The consultation initiated by means of this CP relates to the NFTF identification and verification of the identity of individuals, which are mainly involved with NFTF customers. NFTF customers were previously subject to Enhanced CDD until the transposition of the EU

[16] Paragraph 5 of the FATF Guidance

[17] Paragraph 28 of the FATF Guidance.

[18] Paragraph 29 of the FATF Guidance.

[19] Paragraph 30 of the FATF Guidance.

AMLD into Cypriot Law, as they were considered to be by definition of high-risk, requiring thus Enhanced CDD under the previous regime [20]. However, following the said transposition, NFTF customers '*without certain safeguards*' applying were classified as of '*potentially higher risk*' than physically present customers, but not by default as '*high-risk*', in order to be subjected in all cases to Enhanced CDD[21]. At the same time, the provisions of the EU AMLD and of the AML Law do not prohibit the use of innovative technologies for the performance of CDD tasks[22], since technology is not only linked to operations but also to compliance tools[23].

1.4.2. Nevertheless, although the use of Innovative Methods is allowed for CDD purposes as mentioned above [24] Paragraph 33(1)(d) of the CySEC AMLD [25] provides only for the possibility of performing at least one of the Enhanced Due Diligence Measures of Annex IV of the CySEC AMLD where the obliged entities collect copies of the relevant documents from their customers or where they perform electronic verification. Even though Annex IV of the CySEC AMLD provides an open-ended list of enhanced CDD measures, this list is considered to be exhaustive for the purposes of Paragraph 33(1)(d), limiting thus the options of obliged entities to a video call as regards Innovation Methods; to the exclusion[26] of any other possibility to use Innovative Methods for the purposes of Paragraph 33(1)(d)

---

[20] Article 13 of the repealed DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

[21] Annex III (2)(c) of the EU AMLD/AML Law; Paragraphs 11 and 20 of the of the ESAs Opinion; Paragraph 88 of the FATF Guidance.

[22] Article 13(1)(a) of the EU AMLD/Article 61(1)(a) of the AML Law adopting the broad definition of '*reliable data from an independent source*'. Given that the subject matter of this FATF Guidance is, in essence, the verification of identity by digital means, Paragraph 87 of the FATF Guidance provides in this respect: *'In the digital ID context, the requirement that digital "source documents, data or information" must be "reliable, independent" means that the digital ID system used to conduct CDD relies upon technology, adequate governance, processes and procedures that provide appropriate level of confidence that the system produces accurate results. This means that they have mitigation measures in place to prevent the types of [technological idiosyncratic] risks set out in Section IV.*'.

[23] Paragraph 4 of the ESAs Opinion.

[24] See also, in addition to the above, Paragraph 10 of the ESAs Opinion that: *'EU law does not specify what 'reliable and independent sources' are…. This means that, to the extent permitted by national legislation [as established], firms have some flexibility regarding the sources of information they use to meet their CDD obligations… EU law does not prevent the verification of the customer's identity on the basis of alternative reliable and independent…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*'.

[25] Paragraph 33(1)(d) of the CySEC AMLD

[26] The other methods laid down in Annex IV N2. of the CySEC AMLD are either a wire transfer, reception of a confirmation by a credit institution, telephone communication, communication via registered mail.

of the CySEC AMLD. This restrictive approach is intended to change subject to certain regulatory and technological safeguards provided for in the CP, which however will have to be considered in a relevant risk-assessment that has to be carried out by Obliged Entities.

1.5 RESULTS TO BE ACHIEVED

1.5.1. By means of the CP, CySEC aims to expand that part of the CDD that relates to the NFTF identification and verification of the identity of individuals by Obliged Entities by explicitly incorporating additional Innovative Methods without them being limited to video calls.

1.5.2. However, the implementation of such methods must be accompanied by relevant safeguards. Such safeguards must allow on a reasonable, consistent and demonstrable basis to sufficiently reduce the Money Laundering/Terrorist Financing (ML/TF) emanating from the introduction of (those additional) Innovative Methods to an acceptable and manageable level taking the technological, i.e. digitized nature of such methods into consideration. Furthermore, the said safeguards must be laid down in a risk assessment conducted by the Obliged Entities, which will take both regulatory requirements and technical issues, in particular idiosyncratic risk related with the introduction of the Innovative Method, into consideration. The said safeguards and, subsequently, the guidance for the purposes of their implementation, are also laid down in the CP. As to the additional Innovative Methods, whose introduction is contemplated herewith these are, without limitation, the contactless selfie[27], Big Data[28] and certificates from public[29] or private regulated bodies[30] produced by means of Distributed Ledger Technology (where available) or other tamper-proof and time stamped method.

[27] Paragraph 13 first bullet point of the ESAs Opinion.

[28] Paragraph 13 second bullet point of the ESAs Opinion.

[29] E.g. corporate certificates.

[30] E.g. bank references.

2. SUMMARY OF AND INTERPLAY BETWEEN THE ESAs OPINION AND THE FATF GUIDANCE

2.1. THE IMPORTANCE OF THE CONTENT OF THE ESAs OPINION AND OF THE FATF GUIDANCE FOR THE PURPOSES OF THE CP

2.1.1. The importance of the ESAs Opinion lies in recognizing the increasing importance of non-face-to-face interaction in view of the technological innovation[31]; and that it is addressed to competent authorities, in order for them to determine their regulatory expectations[32] as these are laid down as regards CySEC in the '*What we expect*' section of this CP. The FATF Guidance clarifies the meaning of abstract terms employed by the AMLD/AML Law in the context of Innovative, i.e. digitized, Methods, in particular the term '*reliable data and information*'[33] as well as technical details in relation thereto[34].

2.2. THE FINDINGS OF THE ESAs OPINION AND OF THE FATF GUIDANCE AS TO THE BENEFITS AND CHALLENGING POSED BY INNOVATIVE METHODS

2.2.1. Financial transactions and business relationships have become increasingly digitized, such digitalization presenting many benefits, which include reduced costs, improved customer experience, increased speed of transactions, reduced account opening times and continuous access to services online. However, Obliged Entities have, at the same time to be mindful of the impact these changes might have on their money laundering and terrorist financing (ML/TF) risk exposure[35]. Additional challenges arise from the fact that in an increasingly digitised environment, where most services are accessible online, Obliged Entities may have to move away from traditional face-to-face interactions to non-face-to-face online channels[36] (this phenomenon has been corroborated by the recent COVID-19 pandemic).

---

[31] Paragraph 5 of the Opinion

[32] Paragraph 7 of the ESAs Opinion

[33] See Paragraph 3 and 87 of the FATF Guidance respectively.

[34] See Section V and Annex A of the FATF Guidance respectively.

[35] Paragraph 3 of the ESAs Opinion.

[36] Paragraph 5 of the ESAs Opinion.

2.2.2. Nevertheless, the ESAs Opinion encourages competent authorities to support technological innovation in the CDD process of Obliged Entities[37] and that they build or increase (as the case may be) their in-house expertise[38], as meeting (conventional) CDD obligations can be challenging for Obliged Entities, since this process is often associated with significant costs and customer inconvenience[39]. The FATF Guidance explains the links between NFTF relationships and Innovative Methods, since '*Non-face-to-face interactions are considered to occur remotely—meaning the parties are not in the same physical location and conduct activities by digital or other non-physically-present means, such as mail or telephone*'[40].

2.2.3. Furthermore, the ESAs Opinion clarifies that innovation is not confined to new financial products and services only, but that it also includes development of new solutions to address specific compliance challenges, such as CDD[41] (e.g. the terms RegTech and Suptech that have emerged recently), whereas CDD offers considerable scope for financial innovation that can improve the effectiveness and efficiency of AML/ CFT controls; nevertheless, the ESAs Opinion highlights that there is a risk that innovation in this field, if ill understood or badly applied, may weaken Obliged Entities' ML/TF safeguards and subsequently, undermine the integrity of the markets in which they operate[42]. The said safeguards are the factors that CySEC should, as per the ESAs Opinion, consider when assessing the:

- Adequacy of the Obliged Entities' CDD measures where innovative solutions are used and the application of such measures by them; and
- Controls in place that enable Obliged Entities to mitigate any risks associated with Innovative Methods[43].

[37] Paragraph 23 of the ESAs Opinion.

[38] Paragraph 25 of the ESAs Opinion.

[39] Paragraph 4 of the ESAs Opinion.

[40] Paragraph 87 of the FATF Guidance.

[41] Paragraph 4 of the ESAs Opinion.

[42] Paragraph 6 of the ESAs Opinion. It is noted that this is the justification for CySEC's approach in this CP, namely that the insertion in the CySEC AMLD of additional Innovative Methods cannot take place, unless Obliged Entities have previously the required safeguards (described below herein) to CySEC's satisfaction.

[43] Paragraph 7 of the ESAs Opinion.

2.3. DATA FROM RELIABLE AND INDEPENDENT SOURCES IN THE DIGITAL ID CONTEXT

2.3.1. As mentioned above, the AML Law does not specify the term '*data from a reliable and independent source*'. This means that, to the extent permitted by national legislation, Obliged Entities have some flexibility regarding the sources of information they may use to meet their CDD obligations, as long as they 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[44]. However, given that the AMLD lays down minimum CDD requirements which can become more stringent [45] CySEC contemplates to allow the introduction of additional Innovative Methods, based on the aforesaid flexibility, subject to certain safeguards being observed. The said safeguards include **a risk assessment**, which shall take the risk factors laid down in the ESAs Opinion and the technical standards laid down in the FATF Guidance into consideration, both of them presented in summary form below herein.

2.3.2. Having regard to the previous paragraph, it is concluded that the AMLD/AML Law refers to '*reliable and independent documents, data and information*' as an alternative to documentary CDD, whereas the ESAs Opinion sets the framework for using Innovative Methods to this end. Within this context of ideas, the FATF Guidance goes a step further providing specific technical details, namely that: '*In the digital ID context, the requirement that digital "source documents, data or information" must be "reliable, independent" means that the digital ID system used to conduct CDD relies upon technology, adequate governance, processes and procedures that provide appropriate levels of confidence that the system produces accurate results*[46] *….and that they have mitigation measures in place to prevent the types of risks of digital ID systems*[47]*…. This means that there is an appropriate level of confidence (assurance) that the digital ID system works as it is supposed to and produces accurate results. It should also be adequately protected against internal or*

[44] Paragraph 10 of the ESAs Opinion.

[45] Paragraph 12 of the ESAs Opinion.

[46] Paragraph 3 of the FATF Guidance.

[47] Paragraph 84 of the FATF Guidance, whereas the relevant risks are laid down in Section IV of the FATF Guidance.

external manipulation or falsification, to fabricate and credential false identities or authenticate unauthorised users, including by cyberattack or insider malfeasance.[48]'.

2.3.3. It emanates from the above that the term '*assurance*' is a key term, which is very frequently employed in the FATF Guidance: '*Digital ID assurance frameworks and standards refer to the term "assurance" in describing the robustness of systems. Assurance levels are therefore useful for determining whether a given digital ID system is "reliable, independent" for AML/CFT purposes*'[49]. As it is further stated in the FATF Guidance:'*…digital ID systems that mitigate these risks in accordance with digital ID assurance frameworks and standards hold great promise for strengthening CDD and AML/CFT controls*'[50]. Thus, the risk-based determination of whether the digital ID system, i.e. the Innovative Method, is appropriately reliable and independent in light of the potential ML, TF, fraud, and other illicit financing risks, will be based on the digital ID's assurance levels[51].

2.3.4. The practical importance of NFTF identification and of transactions by means of reliable and independent digital ID systems with appropriate risk mitigation measures in place, is that it may present a standard level of risk, and may even be lower-risk where higher assurance levels are implemented and/or appropriate ML/TF risk control measures, such as product functionality limits and other measures are present[52] . Thus: *'If, as a matter of internal policy or practice, non-face-to-face business relationships or transactions are always classified as high-risk, [Obliged Entities should] consider reviewing and revising those policies to take into account that identification/verification measures that rely on reliable, independent digital ID systems, with appropriate risk-mitigation measures in place, may be standard risk, and may even be lower-risk*[53].' It is thus in the (business) interest of Obliged Entities to conduct their risk assessment also on the technical grounds mentioned in the FATF Guidance, with the aim to establish in the said assessment the required assurance level.

[48] Paragraph 138 of the FATF Guidance.

[49] Paragraph 81 of the FATF Guidance.

[50] Paragraph 10 of the FATF Guidance.

[51] Paragraph 139 of the FATF Guidance.

[52] Page 6 of the short version of the FATF Guidance, Paragraph 3 of the FATF Guidance and Paragraph 89 of the FATF Guidance.

[53] Paragraph 25 of the FATF Guidance.

2.4. FATF GUIDANCE ON DIGITAL ID SYSTEMS

2.4.1. Given its technical content, the FATF Guidance provides a list of some of the technologies used in the digital ID context, which even include artificial intelligence/machine learning (e.g. for determining validity of a government-issued ID)[54].

2.4.2. As to some of the benefits and ML/TF risks posed by digital ID systems, these are covered in detail under Section IV of the FATF Guidance, since identity proofing and/or authenticating individuals over an open communications network (i.e. the Internet), creates risks specific to digital ID systems – particularly in relation to cyberattacks and potential large-scale identity theft[55].

2.4.3. The FATF Guidance also provides a description of how digital ID systems generally operate[56] and an analysis of the three key components of digital ID systems[57], whereas a more detailed technical explanation thereupon takes place in Annex A of the FATF Guidance. As to those three key components, let it be said at this point that these are:

- Identity proofing and enrolment (essential characteristic);
- Authentication and identity lifecycle (essential characteristic); and
- Portability and interoperability mechanisms (optional characteristic).

2.4.4. As to the risks at the identity proofing stage, these may result in digital IDs that are "*fake*" (i.e. obtained under false premises through an intentionally malicious act) and that can be used to facilitate illicit activities. These risks are mitigated by having an appropriate identity assurance level. Identity proofing risks are distinguished from authentication risks, where a legitimately issued digital ID has been compromised and its credentials or authenticators are under the control of an unauthorised person. These risks are mitigated by having an appropriate authentication assurance level[58]. Further guidance as to the technical aspects of digital ID systems and of the relevant risks posed can be found under Annex A and

[54] See Paragraph 32 of the FATF Guidance for a more detailed presentation of the technologies used in this context.

[55] Paragraph 10 of the FATF Guidance.

[56] Paragraph 57-60 of the FATF Guidance.

[57] Paragraphs 61-70 of the FATF Guidance.

[58] Paragraph 116 of the FATF Guidance.

Section IV of the FATF Guidance respectively. More specifically, identity proofing risks are laid down under Paragraphs 117-119 of the FATF Guidance, whereas authentication risks under paragraphs 120-130 thereof. As to broader issues presented by digital ID systems which may impact AML/CFT efforts, but cannot be considered as idiosyncratic risks, i.e. risks inherent, in the digital ID verification process, these are laid down under Paragraphs 132-137 of the FATF Guidance.

2.4.5. As to how to attain the required level of assurance, the FATF Guidance provides directions[59] in this respect: '*Section V is the crux of the Guidance and provides guidance for government authorities, regulated entities and other relevant parties on how to apply a risk-based approach to using digital ID systems for customer identification and verification…There are two elements of this approach:*

- *Understand the assurance levels of the digital ID system and*
- *Assess whether, given the assurance levels, the ID system is appropriately reliable [and] independent in light of the ML/TF risks*'[60].

A relevant flowchart to be considered by Obliged Entities is provided under Paragraph 9 of the FATF Guidance, whereas further analysis of the questions included in the flowchart[61] is provided under Paragraphs 141-153 of the FATF Guidance. Section II of the FATF Guidance[62] provides clarifications as to digital ID terminology and key features, so that Obliged Entities can understand the basic components of digital ID systems, particularly identity proofing and authentication, and how they apply[63].

[59] Paragraphs 7,9 with a relevant flowchart and 141ff of the FATF Guidance.

[60] Paragraph 7 of the FATF Guidance.

[61] Paragraphs 142-146 for the first question, namely Question One: 'Is the digital ID system authorised by government for use in CDD?' Paragraphs 147-151 as to 'Question Two: Do you know the relevant assurance level/s of the digital ID system?' and Paragraphs 152-153 as to Question Three: Is the digital ID system appropriate for the ML/TF risk situation?

[62] Paragraphs 48-75 of the FATF Guidance.

[63] Paragraph 22 of the FATF Guidance.

2.5. THE RISK FACTORS WHICH MUST BE CONSIDERED IN OBLIGED ENTITIES' RISK ASSESSMENT FOR THE INTRODUCTION OF INNOVATIVE METHODS

2.5.1. The ESAs Opinion provides for a number of factors that competent authorities, in the present case CySEC, should consider when assessing the extent to which the use or intended use of Innovative Methods is adequate in the light of the ML/TF risk associated with individual business relationships and the Obliged Entities' business-wide risk profiles, such factors being technology-neutral[64]. The said factors apply **in addition** to the risk factors set out in Annex III of the AML Law, and Part IV of the CySEC AMLD, which should be considered in the context of performing a risk assessment as per the provisions of Section 58A of the AML Law. Those additional risk factors inter alia include:

- Oversight and control mechanisms;
- The quality and adequacy of CDD measures;
- The reliability of CDD measures;
- Delivery channel risks; and
- Geographical risks[65].

2.5.2. A summary as to the assessment of those factors, as per the ESAs Opinion, is provided below herein. Obliged Entities must conclude that the introduction of an innovative technological method for CDD purposes is consistent with the entity's risk profile or in case of disruption that necessary continuity/recovery arrangements are in place. Obliged Entities must demonstrate that they have full understanding of the solution, including **at the level of senior management and of the AML/CFT Compliance Officer**. Such understanding encompasses in-house technical expertise as to the solution's development and implementation and as to continuity issues, including relevant contingency planning. The continuity objectives should aim to ensure proper functioning and troubleshooting, even in case of extreme failures and breakdowns or in case of termination of outsourcing arrangements.[66]

[64] Paragraph 15 of the ESAs Opinion

[65] Paragraph 15 of the ESAs Opinion.

[66] Paragraph 16 of the ESAs Opinion.

2.6. SUCCINCT OVERVIEW OF THE RISK FACTORS TO BE CONSIDERED IN THE OBLIGED ENTITIES' RISK ASSESSMENT

2.6.1. Oversight and control mechanisms shall apply to both in-house solutions and to solutions that have been outsourced to or developed (for internal use by the Obliged Entity) by an external technical provider[67]. The FATF Guidance provides for the technical criteria, in order to place reliance on the digital ID system of an eligible third party[68]. Furthermore, when competent authorities assess the adequacy of firms' governance and controls frameworks, the following will be taken into consideration and have thus must be addressed in the relevant risk assessment:

- Appropriateness of relevant risk management systems where Obliged Entities can demonstrate successful previous (stress) testing, in order to ensure full transition to the new CDD method[69];
- Where the innovative CDD solution has not been developed in-house, the Obliged Entity must demonstrate that it does not end up as a letter box entity[70];
- Ongoing monitoring arrangements and a three step remedial action, where weaknesses have been identified[71];
- In case of serious weaknesses the existence of a process to reconsider the solution introduced[72];
- Regular monitoring of data retention, i.e. of record-keeping requirements[73]
- High standards of data and IT security[74];
- GDPR compliance by means of evidencing a GDPR compliance review[75];
- The integrity[76] and training of the staff[77];

[67] Paragraph 17 of the ESAs Opinion in reliance of Article 17 AMLD/ Article 67 of the AML Law.

[68] Paragraph 96 of the FATF Guidance.

[69] Paragraph 17a of the ESAs Opinion.

[70] Paragraph 17b of the ESAs Opinion.

[71] Paragraph 17c of the ESAs Opinion.

[72] Paragraph 17d of the ESAs Opinion.

[73] Paragraph 17e of the ESAs Opinion.

[74] Paragraph 17f of the ESAs Opinion.

[75] Paragraph 17g of the ESAs Opinion.

[76] Paragraph 17h of the ESAs Opinion.

[77] Paragraph 17i of the ESAs Opinion.

- Consideration by Obliged Entities of any compliance and operational risks before commencing the use of an innovative CDD solution, including of any other risks associated with the solution in question[78]. This factor shall also be considered at the level of the external provider or delegate (as the case may be), as to their financial, operational and reputational soundness; and
- Third country rules in case of outsourcing that might prevent the obliged entity from meeting its AML obligations[79].

2.6.2. As to the quality and adequacy of CDD measures, Obliged Entities should be able to demonstrate that the innovative solution is sufficiently reliable and commensurate with the level of ML/TF risks presented[80] and consider the following factors:

- That sufficient controls are in place to ensure that a business relationship commences only once all CDD measures being commensurate with the ML/TF risk have been applied. The final decision lies always with the Obliged Entity[81].
- That an oversight framework is in place that may include, among other things, regular assurance testing, ongoing compliance monitoring and reviews by the Internal Audit function or even by the external auditor and inspections to the third party provider (if applicable)[82]; and
- That controls are in place to ensure that documentation, data and information gathered during the customer on-boarding process through innovative solutions remain accurate and up to date[83].

2.6.3. As to the reliability of CDD measures, this encompasses issues of validity and authenticity in cases of data, documentation and information obtained in respect of customers through Innovative Methods[84]. Where persons are required to transmit their ID documentation, data or information via video conferences, mobile phone apps or other digital means:

---

[78] Paragraph 17j of the ESAs Opinion.

[79] Paragraph 17k of the ESAs Opinion.

[80] Paragraph 18 of the FATF Guidance.

[81] Paragraph 18a of the ESAs Opinion.

[82] Paragraph 18b of the ESAs Opinion, whereas Paragraph 18c thereof refers to the ongoing monitoring of the business relationship with the customer.

[83] Paragraph 18d of the ESAs Opinion.

[84] Paragraph 19 of the ESAs Opinion.

- Controls must be in place to prevent the risk that the person's image visible on the screen is being tampered with during the transmission[85];
- Controls must be in place to address the risk of discrepancies between the person on the screen and the person to whom the relevant identity document belongs[86];
- Controls need to be in place to ensure that identity documents produced during the transmission have not been processed (processing to be understood in a broad sense)[87]
- An assessment should take place whether or not data necessary to carry out the CDD 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[88].

2.6.4. As to delivery channel risks, the factors set out below should be at least considered by Obliged Entities:

- Risk of identity fraud and that Obliged Entities have assessed the availability and effectiveness of safeguards that could mitigate these risks, whereas examples of relevant safeguards are provided[89];
- Risk of undue influence (intimidated, threat or duress) during the transmission of the identity verification[90]; whereas
- The FATF Guidance[91] provides further input with additional technical safeguards that could be taken into consideration: '*For example, regulated entities could utilise safeguards built into digital ID systems to prevent fraud (i.e. monitoring authentication events to detect systematic misuse of digital IDs to access accounts, including through lost, compromised, stolen, or sold digital ID credentials/authenticators) to feed into systems to conduct ongoing due diligence on the business relationship and to monitor, detect and report suspicious transactions to authorities*'.

[85] Paragraph 19a of the ESAs Opinion where also relevant examples are provided.

[86] Paragraph 19b of the ESAs Opinion.

[87] Paragraph 19c of the ESAs Opinion also providing for relevant measures, whereas Paragraph 19d thereof refers to ongoing monitoring.

[88] Paragraph 19e of the ESAs Opinion.

[89] Paragraph 20a of the ESAs Opinion.

[90] Paragraph 20b of the ESAs Opinion.

[91] Paragraph 26 of the FATF Guidance.

2.6.5. As to the consideration of geographical risks, i.e. the risks emanating from the nature of the NFTF relationship, it must be assessed whether a person in another jurisdiction uses the Obliged Entity for ML/TF purposes[92]. Therefore, competent authorities should satisfy themselves and, subsequently, Obliged Entities should establish in the risk assessment, required under the CP, that Obliged Entities:

- Are able to assess the geographical risks, including through controls that capture the persons' location (e.g. through device fingerprinting or GPS data on mobile phones), in order to establish if they are based in a jurisdiction associated with higher ML/TF risks; and,
- Have practices in place to assess the reasons why customers from other jurisdictions are using their services[93].

3. CYSEC'S PROPOSAL/EXPECTATIONS AND ADDITIONAL REQUIREMENTS AND CONSIDERATIONS

3.1. WHAT WE PROPOSE

3.1.1. As initially established, both the AMLD and the AML Law allow the introduction of Innovative Methods in the CDD process for the purposes of identifying and verifying the identity of a natural person by means of a Digital ID; provided it can be demonstrated to CySEC that the said process is based on '*data and information from a reliable and independent source'*. Furthermore, the FATF Guidance provides technical insights, including insights into technical risks, regarding to establish reliability and independence in the Digital ID context, whereas the ESAs Opinion provides for the relevant risk factors that need to be considered from an AML risk management perspective. At the same time the current provisions of the CySEC AMLD, namely Paragraph 33(1)(d) thereof, provides only for the possibility of performing at least one of the Enhanced Due Diligence Measures of Annex IV of the CySEC AMLD where the obliged entities collect copies of the relevant documents from their customers or where they perform electronic verification. Even though Annex IV of the CySEC AMLD provides an open-ended list of enhanced CDD measures, this list is considered to be exhaustive for the purposes of Paragraph 33(1)(d), limiting thus the options of obliged entities to a video call as regards Innovation Methods;

[92] Paragraph 22 of the ESAs Opinion.

[93] Paragraph 22 of the ESAs Opinion.

to the exclusion[94] of any other possibility to use Innovative Methods for the purposes of Paragraph 33(1)(d) of the CySEC AMLD.

3.1.2. Having regard to the current approach of the CySEC AMLD, whereas the number of Obliged Entities' interactions with NFTF individuals is expected to rise, both for reasons associated with the technological progress and the COVID19 Pandemic, CySEC proposes the amendment of the CySEC AMLD.

3.1.3. The proposed amendment encompasses the amendment of Annex IV of the CySEC AMLD by explicitly incorporating the possibility of using such innovative methods, subject to certain conditions, whereas the suggested (amended) wording is appended to the CP as Annex I thereof. The amendment aims at expanding the use of Innovative Methods for the purposes of conducting CDD as to the NFTF identification and verification of the identity of individuals, provided such methods can sufficiently reduce the Ml/TF risks on a reasonable, consistent and demonstrable basis, such risks being also understood as the idiosyncratic risks inherent in the technology employed in the context of the Innovative Method, but also the risks relevant to the specific customer.

3.1.4. As to how this reasonable, consistent and demonstrable basis, in other words the required assurance level will be achieved, Obliged Entities will have to carry out a risk assessment, which will have to take the points provided under section 3.2 below herein into consideration.

Question 1: Do you agree with CySEC's proposal to amend the CySEC AMLD by explicitly incorporating the possibility of using innovative methods for the purposes of conducting CDD as to the NFTF identification and verification of the identity of individuals (natural persons)?

Questions 2: Do you agree that the use of such innovative methods should be subject to a risk assessment based on which it is rendered that the ML/TF risks are being addressed on a reasonable, consistent and demonstrable basis?

[94] The other methods laid down in Annex IV N2. of the CySEC AMLD are either a wire transfer, reception of a confirmation by a credit institution, telephone communication, communication via registered mail.

3.2. WHAT WE EXPECT/REQUIRE

3.2.1. Those Obliged Entities that intend to make use of the amended wording of the CySEC AMLD and to avail of additional Innovative Methods, for the NFTF identifying and verifying the identity of individuals, will have to carry out the risk assessment mentioned in this CP. The said assessment must take place on the basis of a risk-based approach, in accordance with Article 8 AMLD/58A AML Law and Part IV of CySEC AMLD and include in its content the assessment of the risk factors mentioned in the ESAs Opinion by also taking the content of the FATF Guidance (including the steps for technical implementation of the Innovative Method), into consideration and the content of CySEC's Circular C399[95] on Financial Action Task Force (FATF) COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses. The said assessment shall take place for each Innovative Method in question, in case where the Obliged Entity intends to make use of more than one.

3.2.2. It is stressed and clarified that the succinct analysis on the content and interplay between the ESAs Opinion and FATF Guidance contained herein, is provided solely for facilitating the consideration of these documents by the Obliged Entities and may not substitute a thorough review of the entire content of the aforesaid documents, which should be undertaken by the Obliged Entities before incorporating innovative methods into their CDD procedures.

3.2.3. CySEC does not to intend to set an explicit limit on the level of assets to be deposited and the size of transactions involved for an Obliged Entity to be able to use an innovative identification method. However, such a limit is expected to be set by the Obliged Entity in question on a risk basis, taking into consideration all relevant risks, including the risks of impersonation and fraud[96]. Such limit is expected to vary per risk category and on a case by case basis, depending on the particular risks involved and on whether a combination of Innovative CDD methods were used or were complemented with non-innovative/non-

[95] Available at: https://www.cysec.gov.cy/CMSPages/GetFile.aspx?guid=853fbd7e-cd2b-4e1f-b918-8fc9738bf280

[96] In accordance with Paragraph 33 of the ESAs 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 financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions.

https://www.cysec.gov.cy/CMSPages/GetFile.aspx?guid=b8e01bf6-f366-402a-bb0c-937ecbc06587

electronic CDD methods. In combining and/or complementing a CDD method Obliged Entities may for example:

- Use Data Sources Triangulation Service Providers to verify the documents and/or information provided by the customer;
- Triangulate the evidence provided by the customer, by gathering and analysing additional data, such as geolocation, verifiable phone numbers, etc.

The level of assets to be deposited and the size of transactions involved per CDD method (including per combination of CDD methods) and per customer risk category should also be part of the relevant risk assessment. The risk assessment should also prescribe the additional CDD measures that will be undertaken on a cases by case basis per type of risk identified.

Our proposed approach might provide more flexibility to firms to design their risk mitigation policy. However, at the same time, that would mean a higher degree of responsibility and accountability not only for the Obliged Entities but also for the natural persons involved. It is also clarified that the source of funds should be thoroughly evaluated and verified.

3.2.4. The outcome of the assessment must justify the Introduction of the Innovative Method on **a reasonable, consistent and demonstrable basis** and should be re-evaluated on an ongoing basis.

3.2.5. The persons within an Obliged Entity that are responsible for the selection, including the documented justification in the risk assessment mentioned herein, implementation and monitoring of the Innovative Method(s), are **the Board of Directors, the AML/CFT Compliance Officer**. The **Internal Auditor** will be responsible for independently auditing the risk assessment and the practical application of the selected Innovative Method(s) and where deficiencies are identified to be immediately rectified. For the purposes of this CP all of the aforesaid persons within the meaning of the CySEC AMLD will be called "the **Responsible Persons**". The said persons must ensure that the required risk assessment is updated, where required, and that it is kept at all times available for inspection by CySEC.

3.2.6. Furthermore, those Obliged Entities that intend to make use of the amended wording of the CySEC AMLD must notify CySEC in advance of their intention, specify the (additional) Innovative Method(s) to be used and provide the attestation appended to the CP as Annex II. The said attestation must be duly signed by all Responsible Persons, who confirm that the introduction of the Innovative Method(s) in question was deemed duly justified on a reasonable, consistent and demonstrable basis, for the customers intended to be used and for the level of assets to be deposited and the size of transactions involved.

Question 3: Do you agree that the risk assessment performed pursuant to Section 58A of the AML Law should, in addition to the risk factors set out in Annex III and Part IV of the CySEC AMLD, inter alia, include the risk factors mentioned in the ESAs Opinion by also taking the content of the FATF Guidance (including the steps for technical implementation of the Innovative Method), into consideration and the content of CySEC's Circular C399?

Questions 4: Do you agree with CySEC's intention to refrain from setting an explicit limit in relation to the level of assets to be deposited and the size of transactions involved for an Obliged Entity to be able to use an innovative identification method, provided that such limits will be set by the Obliged Entities in the content of their risk assessment per risk category and be further reviewed on a case by case basis?

Question 5: Do you agree with CySEC's intention to require the submission of a standardized attestation duly signed by all Responsible Persons, confirming that the introduction of the Innovative Method(s) in question was (were) deemed duly justified on a reasonable, consistent and demonstrable basis, for the customers intended to be used and for the level of assets to be deposited or the size of transactions involved, prior the use of such innovative method?

3.3. ADDITIONAL CONSIDERATIONS AND PRACTICAL GUIDANCE

3.3.1. THE RATIONALE UNDERPINNING THE ADDITIONAL CONSIDERATIONS AND THE PRACTICAL GUIDANCE

3.3.1.1. In view of the fact that the NFTF identification and verification of the identity of individuals by means of selfie verification and video calls are the most frequent and prominent among the good practices we have encountered in the context of the activities of the CySEC

Innovation Hub, we would like to provide herewith some practical guidance on their implementation.

3.3.1.2. More specifically, there are, as a matter of common market practice, two prevailing methods for effecting the NFTF identification and verification of the identity of individuals:

i. A video conference offering the highest possible reliability credentials with the participation of a properly trained employee of the Obliged Entity; and,
ii. An automated process initiated by the individual taking a dynamic real-time selfie.

3.3.1.3. Within the context of the aforesaid methods, the acceptable documents for the identification of natural persons are those having advanced safety features, in particular a (biometric) passport or a (biometric) ID.

3.3.1.4. Obliged Entities shall ensure that the electronic NFTF identification process remains reliable, by making use, to the extent possible, of multiple and alternative sources of information.

3.3.1.5. Obliged entities should also be in a position to shield themselves against spoofing[97] and deep-fake synthetic media[98].

3.3.1.6. Obliged entities must therefore be in a position to confirm (cumulatively) that they are dealing with:

i. A real person (i.e. with a real human being);
ii. The right person (i.e. the rightful holder of the identification document); and
iii. A (real) person which is authenticating themselves at the present time.

[97] Malicious parties impersonating another device or user.

[98] Synthetic media in which a person is replaced with someone else's likeness.

3.3.2. THE MINIMUM CONTENT OF THE ELECTRONIC NFTF IDENTIFICATION PROCEDURE BY MEANS OF DYNAMIC SELFIE AND/OR VIDEO-CALL

3.3.2.1. As to the content of the NFTF electronic identification procedure by means of dynamic selfie and/or video-call, such procedure must be approved by the Obliged Entity's Board and must as a minimum include:

i. An analytical description of the various stages of the electronic NFTF identification procedure per method applied; and of the organizational, technical and procedural measures taken to ensure a reliable identification and verification of the identity of natural persons, the management of the relevant risks and compliance with the requirements laid down in the CP;
ii. A procedure for activating additional measures and safeguards, in cases where the Obliged Entity is not satisfied with regard the validity of an identification document or with the conclusion about a natural person's identity;
iii. A procedure for recording and monitoring any divergences/discrepancies between the electronic NFTF identification procedure for as it has been approved by the BoD and its actual implementation; and,
iv. Criteria for determining what is considered as a not acceptable risk and, where applicable, for the subsequent termination of the electronic NFTF identification procedure in question.

3.3.2.2. It is clarified and stressed that the above procedure does not constitute a risk assessment. A risk assessment should be undertaken by the Obliged Entity in question in any case, as per the content of this CP.

3.3.3. PRACTICAL IMPLEMENTATION THE ELECTRONIC NFTF IDENTIFICATION PROCEDURE BY MEANS OF DYNAMIC SELFIE AND/OR VIDEO-CALL

3.3.3.1. As to the practical implementation of the electronic NFTF identification procedure as such, Obliged Entities must irrespectively of the specific method applied:

i. Apply safe communication techniques between the Obliged Entity and the natural person in question, in order to ensure the integrity and confidentiality of the information transmitted;

ii. Ensure that the electronic NFTF identification procedure in question takes place in real time and without interruption and that no data, which may have been created by the natural person in question prior to the commencement of the said procedure no matter how, will be accepted;

iii. Ensure that the natural person whose identity is verified via electronic means is the rightful holder of identification document (i.e. is the right person) and that they (the Obliged Entities in question) are not subject to spoofing or deep-fake media attacks.

iv. Ensure that photos and videos taken during the electronic NFTF identification procedure are of such quality that, both the natural person in question as well as the details included in the identification document of the said person, are totally identifiable and undisputable. In addition, Obliged Entities must ensure that during the electronic NFTF identification procedure appropriate lighting conditions are in place, that the natural person in question keeps the recommended distance from the camera, that his/her face is not covered or not clearly visible and that the depiction of this person's characteristics is generally achieved beyond any reasonable doubt;

v. Ensure that all data received is digitally recorded and that a relevant record is kept, including the results of the controls carried out during the various stages of the electronic NFTF identification procedure, such recording being adequately protected against any attempts to alter its content. As to the data mentioned in the previous sentence, it may include any photo or video taken during the electronic NFTF identification procedure should be kept available for supervisory Audit; and

vi. Ensure that the electronic NFTF identification procedure takes, at all times, place through the use of one and only device.

3.3.3.2. For the purposes of the electronic NFTF identification procedure, identification documents can be accepted, provided these are included in the PRADO - Public Register of Authentic travel and identity Documents of the European Council and of the Council of the European Union and bear:

i. Photo and signature of their holder;

ii. Machine Readable Zone-MRZ; and,

iii. Another two advanced visual safety features from those described in detail in the PRADO.

3.3.3.3. Obliged Entities shall in the course of the electronic NFTF identification procedure and irrespectively of the method applied:

i. Take under suitable lighting conditions photos/screenshots clearly depicting:
    a. The natural person's face from different angles, e.g. profile and en face, using techniques demonstrating that the natural person in question is '*live*' during the process (i.e. liveness, for instance eyes open/eyes shut, Head moving to different directions); and,
    b. That particular side of the identification document containing the photo, the signature and the identity details of the natural person in question, so that the control can be adjusted to the standards and the features of the relevant document.
ii. Carry out controls of the biometric characteristics of the natural person in question in relation to the photo in the relevant identification document by means of a specific software; and,
iii. Require the natural person in question to register the unique code number the person receives by email or SMS in its mobile phone.

3.3.3.4. In case where Obliged Entities apply the electronic NFTF identification procedure by means of a Video-call, they must in addition to the above:

i. Require the natural person in question to place his/her finger in front of the safety features of his/her identification document or move his/her hand in front of his/her face; and,
ii. Carry out controls in order to identify any suspicious behavior of the natural person in question, which may imply that this person is under the influence of narcotic or other substances or compulsion or eventually under a mental or physical disorder.

3.3.4. REQUIREMENTS ON THE OBLIGED ENTITIES' STAFF PARTICIPATING IN ELECTRONIC NFTF IDENTIFICATION PROCEDURE

3.3.4.1. Obliged Entities shall ensure that the electronic NFTF identification procedure is carried out by appropriate and duly trained staff, which has been vested with necessary resources and specialized technical means for the seamless and safe implementation of the procedure in question.

3.3.4.2. The training of the relevant staff shall comprise of the practical implementation of the technological solution in question and of its functional capabilities. It must also comprise of the safety features of those identification documents considered acceptable, including

the methods usually employed in order to forge or alter these, of the requirements laid down in the CP as well as of the identification of unusual or suspicious transactions and the transmission of relevant reports, in accordance with the Obliged Entity's internal procedures. The required training, which has to be provided over and above of the general AML/CTF training required under the applicable framework, shall take place before the assumption of the relevant duties by the staff in question and must repeated at regular time intervals.

3.3.4.3. In addition, Obliged Entities shall ensure through appropriate procedures that the staff carrying out the NFTF identification and verification of the identity of natural persons by means of any technological solution chosen, does not co-operate with persons involved in illegal activities. Such procedures must include the control on the suitability of the staff in question prior to their employment and such staff's regular assessment thereafter; furthermore, the random assignment to the staff in question of requests for electronic NFTF identification procedure, in order to minimize the possibility of manipulating the relevant process, as well as sample checks of the staff's communication with other natural persons during or after the performance of the electronic NFTF identification procedure.

3.3.4.4. In case where Obliged Entities apply the electronic NFTF identification procedure by means of videoconference, they must ensure that the staff performing such procedures is seated in a specially configured room of restricted and controlled access.

Question 6: Do you agree with the additional considerations and Practical Guidance?

Question 7: Do you have any suggestions for specific additional safeguards that should be set in the form of practical Guidance or otherwise?

Question 8: Do you have any other comments?

ANNEX I - PROPOSED CYSEC AMENDED AML DIRECTIVE AND UNOFFICIAL TRANSLATION

ΟΔΗΓΙΑ ΤΟΥ 2020 ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΚΕΦΑΛΑΙΑΓΟΡΑΣ (Αρ. 2) ΓΙΑ ΤΗΝ ΠΑΡΕΜΠΟΔΙΣΗ ΚΑΙ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΗΣ ΝΟΜΙΜΟΠΟΙΗΣΗΣ ΕΣΟΔΩΝ ΑΠΟ ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ		
(Τροποποιητική της Οδηγίας για Την Παρεμπόδιση και Καταπολέμηση της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες)		
Ν. 188(Ι)/2007 Ν. 58(Ι)/2010 Ν. 80(Ι)/2012 Ν. 192(Ι)/2012 Ν. 101(Ι)/2013 Ν. 184(Ι)/2014 Ν. 18(Ι)/2016 Ν. 13(Ι)/2018 Ν. 158(Ι)/2018 Ν. 81(Ι)/2019 Ν. 58(Ι)/2016.	Η Επιτροπή Κεφαλαιαγοράς Κύπρου, ασκώντας τις εξουσίες που της παρέχονται δυνάμει του Άρθρου 59 του περί της Παρεμπόδισης και Καταπολέμησης της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες Νόμου του 2007 και του Άρθρου 3 του περί Εφαρμογής των Διατάξεων των Ψηφισμάτων ή Αποφάσεων του Συμβουλίου Ασφαλείας του ΟΗΕ (Κυρώσεις) και των Αποφάσεων και Κανονισμών του Συμβουλίου της Ευρωπαϊκής Ένωσης (Περιοριστικά Μέτρα) Νόμου του 2016, εκδίδει την ακόλουθη Οδηγία:	
Συνοπτικός τίτλος. Κ.Δ.Π. 157/2019 Κ.Δ.Π. 125/2020	1.	Η παρούσα Οδηγία θα αναφέρεται ως η Οδηγία του 2020 (Αρ.2) για την Παρεμπόδιση και Καταπολέμηση της Νομιμοποίησης Εσοδών από Παράνομες Δραστηριότητες, η οποία τροποποιεί την Οδηγία για την Παρεμπόδιση και Καταπολέμηση της Νομιμοποίησης Εσοδών από Παράνομες Δραστηριότητες.
Τροποποίηση της παραγράφου 2.	2.	Η παράγραφος 2 της Οδηγίας για Την Παρεμπόδιση και Καταπολέμηση της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες τροποποιείται με την προσθήκη, στην κατάλληλη αλφαβητική σειρά, του ακόλουθου νέου όρου και του ορισμού του: ««τυποποιημένη βεβαίωση» σημαίνει το Έντυπο 188-2007-01 το οποίο εκδίδεται από την Επιτροπή Κεφαλαιαγοράς, και δημοσιεύεται στο διαδικτυακό της τόπο·».
Τροποποίηση του Τέταρτου Παραρτήματος.	3.	Το Τέταρτο Παράρτημα της Οδηγίας για Την Παρεμπόδιση και Καταπολέμηση της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες τροποποιείται με την αντικατάσταση της παραγράφου (iv) του σημείου 2 αυτού, με την ακόλουθη νέα παράγραφο: «iv. Ένα ή συνδυασμό περισσότερων καινοτόμων μεθόδων για την εξ' αποστάσεως εξακρίβωση και επαλήθευση της ταυτότητας φυσικών προσώπων, περιλαμβανομένων και χωρίς περιορισμού, της εξακρίβωσης ταυτότητας μέσω της λήψης δυναμικού αυτοπορτρέτου σε πραγματικό χρόνο (dynamic real time selfie) και της εξακρίβωσης ταυτότητας μέσω βιντεοκλήσης (video call), νοουμένου ότι πληρούνται σωρευτικά τα ακόλουθα: α. Η χρήση τέτοιων μεθόδων γίνεται σε μία βάση κινδύνου σε σχέση με τους σχετικούς πελάτες, το μέγεθος των περιουσιακών στοιχείων που θα κατατεθούν και το μέγεθος των συναλλαγών που αφορούν· β. Έχει προηγηθεί στη βάση του Μέρους IV διεξοδική αξιολόγηση των κινδύνων που ανακύπτουν από τη χρήση τέτοιων μεθόδων και σε σχέση με τους τρόπους μετριασμού των εν λόγω κινδύνων, η οποία επικαιροποιείται σε συνεχή βάση και σύμφωνα με την οποία οι εν λόγω καινοτόμοι μέθοδοι μπορούν σε μία εύλογη, συνεπή και ευαπόδεικτη βάση να μειώσουν επαρκώς τον κίνδυνο νομιμοποίησης εσόδων από παράνομες δραστηριότητες, περιλαμβανομένου του κινδύνου πλαστοπροσωπίας και απάτης· γ. Οι υπόχρεες οντότητες που προτίθενται να κάνουν χρήση καινοτόμων μεθόδων, έχουν ενημερώσει την Επιτροπή Κεφαλαιαγοράς εκ των προτέρων, προσδιορίζοντας τις μεθόδους αυτές και έχουν υποβάλει την τυποποιημένη βεβαίωση, δεόντως συμπληρωμένη και υπογεγραμμένη από όλα τα αρμόδια πρόσωπα που καθορίζονται σε αυτή·

		δ. Η χρήση των εν λόγω καινοτόμων μεθόδων γίνεται σύμφωνα με τις σχετικές κατευθυντήριες γραμμές και τις βέλτιστες πρακτικές που δημοσιεύει η Επιτροπή Κεφαλαιαγοράς.».
Έναρξη ισχύος.	4.	Η παρούσα Οδηγία ισχύει από τη δημοσίευσή της στην Επίσημη Εφημερίδα της Δημοκρατίας.

SECOND DIRECTIVE OF 2020 OF THE CYPRUS SECURITIES AND EXCHANGE COMMISSION (No 2) FOR THE PREVENTION AND SUPPRESSION OF MONEY LAUNDERING ACTIVITIES		
(Amending the Directive of the Cyprus Securities and Exchange Commission for the Prevention and Suppression of Money Laundering and Terrorist Financing)		
L. 188(I)/2007 L. 58(I)/2010 L. 80(I)/2012 L. 192(I)/2012 L. 101(I)/2013 L. 184(I)/2014 L. 18(I)/2016 L. 13(I)/2018 L. 158(I)/2018 L. 81(I)/2019 L. 58(I)/2016.	The Cyprus Securities and Exchange Commission, in accordance with the powers vested in it by virtue of section 59 of the Prevention and Suppression of Money Laundering Activities Law of 2007 and section 3 of the Implementation of the Provisions of the United Nations Security Council Resolutions or Decisions (Sanctions) and the European Union Council Decisions and Regulations (Restrictive Measures) Law of 2016, issues the following Directive:	
Short Title. R.A.D. 157/2019 R.A.D. 125/2020	1.	The present Directive shall be cited as the Directive of 2020 (No. 2) for the Prevention and Suppression of Money Laundering Activities, amending the Directive for the Prevention and Suppression of Money Laundering Activities.
Amendment to Paragraph 2.	2.	Paragraph 2 of The Directive for the Prevention and Suppression of Money Laundering Activities is amended by adding, in the proper alphabetical order, the following new term and its definition:
		««standardised confirmation» means Form 188-2007-01 issued by the Cyprus Securities and Exchange Commission, and published on its website·».
Amendment to the Fourth Appendix	3.	The Fourth Appendix of The Directive for the Prevention and Suppression of Money Laundering Activities is amended by substituting paragraph (iv) of point 2 thereof, with the following new paragraph: « iv. An innovative method or a combination thereof for the non-face-to-face identification and verification of the identity of natural persons, including without limitation identity verification by means of taking a dynamic real time selfie, and/or of a real time video call, provided that the following conditions are cumulatively fulfilled: a. The use of such methods takes place on a risk-based approach as regards the relevant customers and the level of assets to be deposited and the size of transactions involved· b. A detailed assessment of the risks emanating from the use of such methods and of the measures employed to mitigate such risks has taken place in advance in accordance with of Part IV, whereas such assessment is updated on an ongoing basis and it allows on a reasonable, consistent and demonstrable basis to conclude that the money laundering risks, including the risks of identity theft, impersonation and identity fraud, are sufficiently reduced · c. The Obliged Entities intending to make use of such innovative methods have informed the Cyprus Securities and Exchange Commission in advance by defining

		the methods to be used and by submitting the standardized attestation duly completed and signed by all relevant persons specified for therein· d. The use of such innovative methods takes place in accordance with the relevant best practices and guidelines published by the Cyprus Securities and Exchange Commission.»..
Entry into force	4.	The present Directive shall enter into force as of is publication in the Official Gazette of the Republic.

ANNEX II - STANDARDIZED ATTESTATION

FORM 188-2007-01: STANDARDISED ATTESTATION BY OBLIGED ENTITIES IN RELATION TO THE INTRODUCTION OF INNOVATIVE TECHNOLOGICAL METHODS AS PER PARAGRAPH 2(iv) OF ANNEX FOUR OF CySEC DIRECTIVE FOR THE PREVENTION AND SUPPRESSION OF MONEY LAUNDERING AND TERRORIST FINANCING

A.(1) STANDARDISED ATTESTATION

In accordance with Paragraph 2(iv) of Annex Four of CySEC Directive for the Prevention and Suppression of Money Laundering and Terrorist Terrorism Financing the persons referred to in sections A.(2) below herein confirm the following:

1. [insert the name of the Obliged Entity] is a**:**

Table 1

Please fill-in the table accordingly.

TYPE OF OBLIGED ENTITY	
CIF	☐
ASP	☐
UCITS Management Company	☐
Internally managed UCITS	☐
AIFM	☐
Internally managed AIF	☐
Internally managed AIFLNP	☐
Company with sole purpose the management of AIFLNP	☐

2. [insert the name of the Obliged Entity] intends to use the innovative technological method(s) referred to in Table 2.1:

Table 2.1

Complete this table by indicating the innovative technological method(s) introduced pursuant to Paragraph 2(iv) of Annex Four of CySEC Directive for the Prevention and

Suppression of Money Laundering and Terrorist Financing for performing Customer Due Diligence ("CDD") with regard to non-face to face ('NFTF') identification and verification of identity of natural persons (individuals).

	Innovative Technological Method(s)
1.	
2.	
3.	

Table 2.2

Complete this table by checking the appropriate boxes. A Form will be considered as duly completed only where all boxes are checked.

1.	It is herewith confirmed that the entity referred to in Section 1 of this Form has undertaken a Risk Assessment in accordance with Article 58A of Law 188(I)/2007 and with Section IV of CySEC Directive for the Prevention and Suppression of Money Laundering and Terrorist Financing (including any relevant ESAs and FATF Guidelines) based on which it was deemed on a reasonable, demonstrable and consistent basis that the innovative technological CDD methods referred to in Table 2.1 could sufficiently address the ML/TF risks, including but not limited to, the risk of impersonation and fraud via spoofing or deep-fake synthetic media or otherwise.	☐
2.	It is herewith confirmed that a specific limit was set on the level of assets to be deposited and the size of transactions involved per each method referred to in Table 2.1 and/or on a combination thereof, in accordance with the risk assessment referred to in this Table directly above and that such limit was deemed to be reasonable and prudent for the risks involved and where necessary that additional measures will be taken on a risk basis.	☐
3.	It is herewith confirmed that when using the methods referred to in Table 2.1 the entity referred to in Section 1 of this Form complies with any relevant guidelines and best practices issued by CySEC from time to time.	☐
4.	It is herewith confirmed that the AML/CFT policy and risk management and procedures manual of the entity referred to in Section 1 of this Form has been amended in order to include the relevant designated internal practice, measures, procedures and controls in relation to the innovative technological methods referred to in Table 2.1 of this Form.	☐

Apart from checking the appropriate box, you may not otherwise add, erase or alter any of the content Table 2.2.

A.(2) Persons confirming the accuracy of the statement of section A.(1) above

Table 3

(1)	(2)	(3)	(4)
Function	**Names**	**Signature**	**Date**
Executive Directors	**[Insert the full names of the Executive Directors here]**	**[The Executive Directors should confirm by signing next to their name]**	
non-Executive Directors	**[Insert the full names of the non-Executive Directors]**	**[The non - Executive Directors should confirm by signing next to their name]**	
Internal Auditor	**[Insert the full name of the Internal Auditor]**	**[The Internal Auditor should confirm by signing next to their name]**	
Head of the AML/CFT Compliance Function	**[Insert the full name of the Head of the AML Compliance Function]**	**[The Head of the AML Compliance Function should confirm by signing next to their name]**	

The aforementioned statement must be confirmed and signed by all of the persons performing the functions referred to in column 1 of Table 3 directly above and must be submitted via email at aml@cysec.gov.cy.

In case that a person performs multiple functions, they should insert their name in each of the above boxes corresponding to the respective function and confirm by signing next to their name in each box.

Failure to provide a duly completed and signed confirmation will result in the Obliged Entity being in breach of the requirements of Paragraph 33(1)(d) and thus not allowed to avail of the CDD possibilities under Paragraph 33(1)(d).

The provision of false or misleading information may jeopardise the fitness and probity of the persons referred to in Table 3.