POLICY STATEMENT

(PS-01-2024)

SUBJECT: POLICY STATEMENT ON THE ENHANCEMENT OF THE NON-FACE-TO-FACE CUSTOMER ONBOARDING PROCESS WITH ELECTRONIC METHODS

DATE OF ISSUE: 6 AUGUST 2024

PURPOSE OF THE PUBLICATION

The Cyprus Securities and Exchange Commission (the 'CySEC'), publishes this Policy Statement in order to inform Obliged Entities and their counterparties based in Cyprus, for the further facilitation, establishment and incorporation of electronic methods and technologies in the process of remote Customer Due Diligence.

Queries in relation to the content of this Policy Statement may be addressed to the Policy Department of CySEC at policy@cysec.gov.cy.

CONTENT

GLOSSARY OF TERMS

AI means Artificial Intelligence.

AML/CFT Law means The Prevention and Suppression of Money Laundering and Terrorist Financing Law 188 of 2007 as in force from time to time.

AML/CFT Compliance Officer means the Anti-money Laundering/Countering Terrorist Financing Compliance Officer of an Obliged Entity, within the meaning of Section 69 of the AML/CFT Law.

AML/CFT means Anti-Money Laundering/Countering Terrorist Financing.

BoD means Board of Directors of an Obliged Entity.

CASP means Crypto Asset Services Providers, within the meaning of Section 2(1) of the AML/CFT Law.

CDD: means Customer Due Diligence measures and procedures, within the meaning of Section 61 of the AML/CFT Law.

CP-02-2020 means CySEC's Consultation Paper (CP-02-2020) titled '*Improving the Facilitation of Customer Due Diligence with Innovative Technologies*'.

CySEC AMLD: Directive of the Cyprus Securities and Exchange Commission for the Prevention and Suppression of Money Laundering and Terrorist Financing as in force from time to time.

CySEC means the Cyprus Securities and Exchange Commission.

Customer or Client means customer within the meaning of Section 2(1) of the AML/CFT Law.

EBA Guidelines: means the EBA Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849[1].

EBA Risk Factor Guidelines means the EBA Guidelines on 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

[1] Guidelines on the use of Remote Customer Onboarding Solutions.pdf (europa.eu), EBA/GL/2022/15 (available here)

and occasional transactions under Articles 17 and 18(4) of Directive (EU) 2015/849[2]. It is noted that the said Guidelines have been revised with the revised Guidelines coming into force in December 2024.

EBA means the European Banking Authority.

EEA means the European Economic Area.

eIDAS Regulation means Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

EIOPA means the European Insurance and Occupational Pensions Authority.

ESAs means the European Supervisory Authorities ESMA, EBA and EIOPA when referred to collectively.

ESAs Opinion means the ESAs Opinion on the use of Innovative Solutions by Credit and Financial Institutions in the Customer Due Diligence Process[3].

ESMA means the European Securities and Markets Authority.

EU means the European Union.

EU AMLD: 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.

FATF Guidance means the FATF Guidance on Digital ID[4].

FATF means the Financial Action Task Force.

IA means the Internal Auditor of an Obliged Entity (where applicable).

ICT means Information and Communication Technology.

---

[2] Final Report on Guidelines on revised ML TF Risk Factors.pdf (europa.eu), EBA/GL/2021/02 (available here).

[3] Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process, JC 2017 81 (available here)

[4] FATF Digital Identity (available here)

ID means a person's Identity.

Identification Document means an official document issued by the government of a Member State of the European Union or of a third country and which states the full name and the date of birth of the natural person and bears the photograph of that natural person.

IP means Internet Protocol.

KYC means Know-Your-Customer documentation in the context of CDD.

ML/TF means Money Laundering/Terrorist Financing, within the meaning of Section 2(1) of the AML/CFT Law respectively.

MOKAS means the Unit for Combating Money Laundering, within the meaning of Section 2(1) of the AML/CFT Law.

MRZ means machine-readable zone, within the meaning of Article 5 para.3 of Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement.

MS means a Member State of the European Union.

NCA means the National Competent Authority of a MS for AML/CFT purposes.

NFTF Customer CDD means CDD in cases of business relationships or transactions with an NFTF Customer.

NFTF Customer: means a Customer, who is not physically present, within the meaning of Annex III of the AML/CFT Law.

NFTF Customer Identification: means identification and verification of identity, within the meaning of Section 61(1)(a)-(c) of the AML/CFT Law of an NFTF Customer.

OCR: means Optical Character Recognition.

OE means Obliged Entity, within the meaning of Section 2(1) of the AML/CFT Law.

PRADO means the Public Register of Authentic Identity and Travel Documents Online of the European Council.

PS: means this Policy Statement.

Responsible Persons means the BoD, the AML/CFT Compliance Officer and the IA.

Remote Customer Onboarding Solutions or **RCOS** means an electronic method for the remote identification and verification of customers' identity.

Risk Assessment means the risk assessment that OEs are obliged to carry out prior to the introduction of an RCOS for the purposes of onboarding NFTF Customers, pursuant to Articles 58(a), 58(d), 58A, 61(2) and 66(2A) of the AML/CFT Law, in conjunction with Annex III of the AML/CFT Law and with Part IV of the CySEC AMLD.

VPN means Virtual Private Network.

1. INTRODUCTION

1.1. PURPOSE OF THIS POLICY STATEMENT

1.1.1. CySEC issued CP-02-2020, in order to facilitate the on-boarding of NFTF Customers by means of RCOS, i.e. by digital means and to provide relevant guidance to OEs as to how to introduce the use of RCOS in their NFTF Customer on-boarding operations. In addition to relying on the applicable regulatory framework, CP-02-2020 also relied on the guidance included in the ESAs Opinion, the FATF Guidance, the realities created by the Covid Pandemic and the experience gained through CySEC's Innovation Hub[5]. Based on the aforesaid, CP-02-2020 included certain initial policy suggestions, namely:

i. Amending the CySEC AMLD, in order to allow for a '*technology-neutral*' use of RCOS by OEs without favouring any specific RCOS or technology and repealing, the at the time applicable, sole eligibility of video-conferences for the onboarding of NFTF Customers;

ii. The requirement for OEs to carry out an extensive[6] risk assessment prior to incorporating the use of RCOS in their NFTF Customer onboarding procedures, without being subject to authorisation or other form of regulatory approval and notifying CySEC thereof;

iii. The limitation of the material scope of application of CP-02-2020 only to the onboarding of NFTF Customers being natural persons and only for purposes of CDD within the meaning of Section 61(1)(a)-(c) of the AML/CFT Law;

iv. The requirement for OEs to notify CySEC of the embedment of RCOS in their NFTF Customer onboarding procedures in advance and to have the Responsible Persons sign a relevant standardised attestation confirming that the introduction of RCOS is considered appropriate on a '*reasonable, consistent and demonstrable basis*';

[5] The said experience was helpful in relation to the practical guidance under Section 3.3.3 of CP-02-2020 as regards electronic NFTF Identification Procedure.

[6] Consideration of Section 58A and Annex III of the AML/CFT Law, the risk factors set out Part IV of the CySEC AMLD, the risk factors mentioned in the ESAs Opinion, the FATF Guidance (including the steps for technical implementation of the RCOS) and CySEC's Circular C399 on Financial Action Task Force (FATF) COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses.

v. The requirement that OEs set, on a risk-based approach, an explicit limit in relation to the level of assets to be deposited and the size of transactions involved, when an OE uses RCOS for onboarding NFTF Customers;

vi. The requirement that the electronic NFTF Identification procedure by means of dynamic selfie and/or video-call described in Section 3.3. of CP-02-2020 takes, at all times, place through the use of one and only device; and that, in the context of biometric solutions, a unique number be communicated only by means of SMS (mobile phone);

vii. The requirement that only PRADO-included documentation is eligible for the purposes of the practical implementation of the electronic NFTF Customer Identification by means of dynamic selfie and/or video-call described in Section 3.3. of CP-02-2020;

viii. Additional practical guidance regarding the electronic NFTF Customer Identification by means of dynamic selfie and/or video-call described in Section 3.3. of CP-02-2020.

1.1.2. Following the publication of CP-02-2020 stakeholders were requested to submit their views by 20 November 2020. While the evaluation of the comments and the finalisation of CySEC's approach was underway, the EBA issued on 10 December 2021, a Consultation Paper on Draft Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849[7]. The consultation ended in March 2022, while the EBA Guidelines were published in November 2022. The EBA Guidelines which apply from 2 October 2023 set common EU standards on the development and implementation of sound, risk-sensitive initial CDD processes in the remote customer onboarding context,[8] overlapping thus to a considerable extent with the content of CP-02-2020. In view of the aforesaid, CySEC work on digital onboarding was in the meantime put on hold while upon finalisation of the EBA Guidelines, the stakeholders' views and the CySEC approach was revisited.

[7] Consultation Paper on Draft Guidelines on used of remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849 (available here).

[8] P.3 of the EBA Guidelines.

1.1.3. The purpose of this PS is to present how the initial policy suggestions laid down in CP-02-2020 have been crystallised, following the publication of the EBA Guidelines and the evaluation of the feedback received. In essence, this PS clarifies how RCOS have to be selected and implemented by OEs for NFTF Customer onboarding purposes, while observing the requirement of Section 61(1)(a) of the AML/CFT Law for '*data and information from a reliable and independent source*'. Furthermore, this PS provides detailed guidance on the interplay between CP-02-2020 and the documents used for its production on the one hand and the subsequently issued EBA Guidelines on the other hand.

1.2. WHO THIS CONCERNS

1.2.1. Unlike CP-02-2020[9], which, as a result of the highly technical nature of RCOS, also invited developers of RCOS or outsourcing providers to express their views, this PS is addressed to OEs only, as it lays down the supervisory expectations from regulated entities. More specifically this PS applies to:

i. Cyprus Investment Firms, within the meaning of Law 87(I)/2017 as in force from time to time;

ii. Administrative Service Providers, within the meaning of Law 196(I)/2012 as in force from time to time;

iii. Internally managed Undertakings for Collective Investment in Transferable Securities, within the meaning of Law 78(I) of 2012 as in force from time to time;

iv. Management Companies of Undertakings for Collective Investment in Transferable Securities, within the meaning of Law 78(I) of 2012 as in force from time to time;

v. Authorised and registered Alternative Investment Fund Managers, within the meaning of Law 56(I)/2013 as in force from time to time;

vi. Internally managed Alternative Investment Funds falling under Part II of Law 124(I)/2018 as in force from time to time;

[9] P. 6 para.1.3.1.2 of CP-02-2020.

vii. Internally managed Alternative Investment Funds with Limited Number of Persons falling under Part VII of Law 124(I)/2018 as in force from time to time;

viii. CASPs were a category of OEs not in place at the moment the CP-02-2020 was issued. It merits clarification that the horizontal application of the policy decisions laid down herein to CASPs is not prejudiced by the fact that the EBA Guidelines, although setting EU standards, do not consider them as addressees thereof; the reason is that the addressees of the EBA guidelines are determined by the EBA's scope of action under the EBA's founding regulation with CASPs not being at the time part of this scope.[10] However, given that CASPs are considered to be OEs, the policy decisions laid down herein, even if relying on the guidance included in the EBA Guidelines, also apply to them (horizontal application across all CySEC supervised entities, which are OE);

ix. Any other entity supervised by CySEC and which is an OE under the AML/CFT Law.

1.2.2. By means of clarification, the following terms should be understood as follows:

i. The term '*credit and financial institutions*' employed in the EBA Guidelines and the term '*firms*' employed in the ESAs Opinion shall be understood as referring to the OEs;

ii. The term '*pre-implementation assessment*' employed in the EBA Guidelines shall be understood as referring to the Risk Assessment;

1.3. STRUCTURE OF THIS PS

1.3.1. Following the introduction in Section 1, this PS will present the final policy decisions as regards onboarding of NFTF Customers by means of RCOS. Given the interplay between CP-02-2020, the ESAs Opinion, which served as a main source for the production of CP-02-2020[11], and the subsequently issued EBA

[10] P.33 of the EBA Guidelines.

[11] The FATF Guidance lays down both technical safeguards as well as regulatory safeguards in relation to use of RCOS for NFTF Customer on-boarding purposes. Nevertheless, given that the EBA Guidelines are the common EU (regulatory) standard, the FATF Guidance should be used for the technical implementation of RCOS by OEs for on-boarding NFTF Customers.

Guidelines as well as the different nature of those documents, Section 3 of this PS provides a detailed presentation of this interplay. The consolidated presentation of the aforesaid sources also explains the rationale for the final policy decisions taken and why certain initial policy decisions have been amended, extended or replaced; in particular as a result of the publication of the EBA Guidelines, which set common EU standards on the development and implementation of sound, risk-sensitive initial CDD processes in the remote customer onboarding context[12].

1.3.2. Subsequently, Annex I to this PS includes the amendment to the CySEC AMLD, in order to allow for the use of RCOS by OEs on a '*technology-neutral*' basis without limitation to video-calls or any other RCOS or technology. Annex II to this PS includes CySEC's position in relation to the stakeholder views and comments expressed during the consultation period, while also substantiating certain abstract terms employed in the CP-02-2020. Annex III of this PS includes a Notification Form for the use of RCOS by OEs in the NFTF identification and verification process. Finally, Annex IV to this PS includes the revised Practical Guidance, initially laid down in Section 3.3 of CP-02-2022 including notes explaining the reasons for and the result of the revisions made. In essence, many of the requirements laid down in the said practical guidance have become generally applicable in relation to any RCOS, following the publication of the EBA Guidelines, thus not only in the specific context of the RCOS envisaged therein. At the same time certain requirements (use of a single device, sms only) have been relaxed in reliance to the EBA Guidelines.

2. WHAT WE EXPECT- POLICY DECISIONS

2.1. Following consideration of the stakeholder views expressed during the consultation period and of the changes brought to the initial policy suggestions laid down in CP-02-2020 as a result of the publication of the EBA Guidelines, this PS, outlines CySEC's final approach on digital onboarding, namely:

i. Reaffirms the technological neutrality of the RCOS to be employed by OEs for NFTF Customer on-boarding purposes. Thus, the suggestion in CP-02-2020 to amend the CySEC AMLD, so that videocalls are no longer the sole

[12] P.3 of the EBA Guidelines.

eligible RCOS for NFTF Customer onboarding purposes[13], is upheld. It is up to the OEs to select or combine one or more RCOS (as the case may be) for NFTF Customer onboarding purposes subject to observing:

a) Articles 58(a), 58(d), 58A,61(2) and 66(2A) of the AML/CFT, in conjunction with Annex III of the AML/CFT Law and with Part IV of the CySEC AMLD;
b) This PS, including the Q&As in Annex II and the revised practical guidance attached as Annex IV hereto respectively;
c) The EBA Guidelines;
d) The ESAs Opinion;
e) The FATF Guidance[14];
f) CySEC's Circular C399 on Financial Action Task Force (FATF) COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses;
g) CySEC's Circular 465 on the revised EBA Risk Factor Guidelines, which has been published following the issuance of CP-02-2020;
h) Any other relevant guidance or requirement addressed to OEs by CySEC from time to time.

Given the multitude of and the interplay between the regulatory documents applying, detailed guidance is provided under Section 3 herein as regards the interplay between the content of CP-02-2020, the ESAs Opinion and the EBA Guidelines as well as the regulatory novelties introduced pursuant to the latter.

However, it has to be stressed that Section 3 of this PS, is provided solely for facilitating the consideration of these documents by OEs and may not substitute a thorough review of the entire content of the aforesaid documents, which OEs are required to undertake;

ii. Reaffirms the requirement laid down in CP-02-2020 that OEs have to carry out the Risk Assessment, as further laid down herein, prior to using RCOS and notify the intention of such use towards CySEC in advance. However,

[13] See P.9 para. 1.5.1 of CP-02-2020 and the neutral wording of the new CySEC AMLD in Annex I.

[14] Given that the EBA Guidelines set the applicable regulatory standards, recurring to the FATF Guidance should rather take place for the purposes of technical implementation of RCOS by OEs.

such notification has an informative character and does not amount to licensing or other form of approval by CySEC of the RCOS to be used. The said approach is aligned with the ESAs Opinion[15] stating that: '*…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….'* Thus, OEs shall incorporate in their NFTF Customer CDD policies and procedures the on-boarding of NFTF Customers by means of RCOS and carry out the Risk Assessment prior to the operationalisation of the RCOS in question, both in accordance with the requirements in this PS, and subsequently notify CySEC thereof by means of the notification in Annex III to this PS;

iii. No longer requires a declaratory attestation to be signed by the Responsible Persons confirming the selection and operationalisation of RCOS for NFTF Identification, in accordance with the applicable framework and standards and the policy decisions laid down herein;

iv. Clarifies, in response to relevant questions, in detail the meaning of the term '*properly trained employee*'[16] for the purposes of the revised practical guidance under Annex IV hereto;

v. Reaffirms that the scope of application of the policy decisions laid down herein relates to the NFTF Customer CDD falling under section 61(1)(a)-(c) of the AML/CFT Law, to the exclusion of ongoing monitoring of the business relationship, as per the clear delineation in the EBA Guidelines: '*These guidelines set out the steps credit and financial institutions should take when adopting or reviewing solutions to comply with their obligations under Article 13(1) points (a), (b) and (c) of Directive (EU) 2015/849[17] to onboard new customers remote*ly'. Thus, the material scope of this PS is limited to NFTF Customer Identification. In alignment with the EBA Guidelines, this PS further applies to new business relationships, in situations where OEs adopt a new RCOS[18] and in situations where OEs review RCOS already in

[15] P.19 para.25 of the ESAs Opinion.

[16] P.25 section 3.3.1.2(i) of CP-02-2020.

[17] Corresponding to section 61(1)(a)-(c) of the AML/CFT Law.

[18] P.36 of the EBA Guidelines.

place[19].Nevertheless, the guidance laid down herein may also be useful in situations where institutions perform remote (NFTF) CDD on existing Customers[20]. The requirements laid down herein also apply to cases where reliance on third parties is being placed in accordance with section 67 of the AML/CFT Law. Finally, it is also clarified that, under this PS, the use of RCOS for on-boarding NFTF Customers is possible not only for natural persons but also for legal entities, including natural persons acting on their behalf. Thus, the term NFTF Customer is to be perceived as encompassing both natural persons as well as legal entities;

vi. No longer requires from an OE that the electronic NFTF Identification procedure, for which the revised guidance is provided in Annex IV hereto, takes, at all times, place through the use of one and only device, as there is sufficient guidance herein on addressing and managing delivery channel risks and geographical risks;

vii. No longer requires that, in the context of biometric solutions (where used) for the purposes of NFTF Customer Identification by means of RCOS, a unique number be communicated only by means of SMS (mobile phone)[21];

viii. Lays down, in reliance to the EBA Guidelines[22], that the use of RCOS that are not within the scope of the eIDAS Regulation is permitted, because Article 13(1) (a) of the EU AMLD[23] provides that relevant trust services and other solutions such as those that are regulated, recognized, approved or accepted at a national level might also be used to perform the identification and verification process. Thus, the use of such other solutions, e.g. non-qualified trust services or other solutions that are regulated, recognized,

[19] P.33 of the EBA Guidelines.

[20] See also P. 29&33 of the EBA Guidelines.

[21] See also P.20 para. 44 of the EBA Guidelines: '*In addition to the above, and where commensurate with the ML/TF risk associated with the business relationship, credit and financial institutions should use of one or more of the following controls or a similar measure to increase the reliability of the verification process. These controls or measures may include, but are not limited to, the following...b) send a randomly generated passcode to the customer to confirm the presence during the remote verification process. The passcode should be a single-use and time-limited code*'.

[22] P.30 of the EBA Guidelines.

[23] Corresponding to section 61(1)(a) of the AML/CFT Law.

approved, or accepted at a national level remains possible in line with Article 13(1) (a) of the EU AMLD/section 61(1)(a) of the AML/CFT Law, subject to specific safeguards.[24] More specifically, when using the said solutions[25], OEs should assess how far the RCOS in question complies with the requirements of this PS and apply measures necessary to mitigate any relevant risks that arise from the use of such solutions, in particular the:

a) Risks involved in the authentication and set out in their policies and procedures specific mitigation measures, especially with regard to impersonation fraud risks;
b) Risk that the NFTF Customer's identity is not the claimed identity;
c) Risk of lost, stolen, suspended, revoked, or expired identity evidence, including, as appropriate, tools to detect and prevent the use of identity frauds.[26];

For the avoidance of doubt, the expectations laid down herein, apply also to solutions that are utilized in accordance with the OE's own risk assessment and which facilitate the identification of customers and verification the customer's identity on the basis of documents, data or information obtained (electronically) from a reliable and independent source; hence not necessarily being solutions that are regulated, recognized, approved, or accepted at a national level.

ix. Clarifies, in alignment with the EBA Guidelines and the distinction between attended solutions and unattended solutions made therein[27] that the liveness detection[28] requirement as well other relevant guidance[29] is

[24] P.31f. of the EBA Guidelines.

[25] The term RCOS is used interchangeably with the terms '*solution*' or *'remote onboarding solution'*, which are the respective terms employed in the ESAs Opinion and the EBA Guidelines.

[26] P.23 para.54 of the EBA Guidelines.

[27] P.20 para.42 of the EBA Guidelines: '*…[un]attended remote customer onboarding solutions in which the customer [does not] interacts with an employee to perform the verification process*'.

[28] P.19 para. 41c) of the EBA Guidelines: *'…perform liveness detection verifications, which may include procedures where a specific action from the customer is required to verify that he/she is present in the communication session or which can be based on the analysis of the received data and does not require a specific action by the customer.*'

[29] P.19 para.41a) of the EBA Guidelines: '*Where credit and financial institutions use unattended remote onboarding solutions, in which the customer does not interact with an employee to perform the verification process, they should: a) ensure that any photograph(s) or video is taken under adequate lighting conditions*

mandatory only in respect of unattended solutions[30], so that only unattended solutions require liveness detection[31]. This without prejudice to OEs voluntarily incorporating liveness detection requirements when using attended solutions (RCOS) as well;

x. Clarifies that PRADO-included documentation is no longer exclusive[32] for the purposes of practical implementation of the revised electronic NFTF Customer Identification procedure by means of dynamic selfie and/or video-call (Annex IV hereto), in accordance with the approach laid down in the EBA Guidelines[33];

xi. Clarifies that the type of documentation accepted for NFTF Customers is no longer exclusively passports. The insertion of the term '*identification document*' to the amended CySEC AMLD, herein enclosed as ANNEX I introduces a broad definition, namely '*an official document issued by the government of a Member State of the European Union or of a third country and which states the full name and the date of birth of the natural person and bears the photograph of that natural person'*;

xii. Enables the confirmation of address when collecting copies of the original documents through RCOS, as per the amended Fourth Appendix of the aforesaid CYSEC AMLD. In addition to this, such RCOS can be used for addressing the geographical risk in the context of the Risk Assessment as further laid down in this PS.

---

and that the required properties are captured with necessary clarity to allow the proper verification of the customer's identity;' and p.28 of the EBA Guidelines: '…implementation of liveness detection may be costly but, by itself, it is not the unique key safeguard for the verification process.'

[30] P.28 of the EBA Guidelines: '*The preferred option is mandatory liveness detection in all unattended situations only*'.

[31] It is noted that the practices aiming at detecting spoofing attacks as those prescribed under the additional practical guidance of Annex IV, remain applicable irrespective of whether the solution is attended or not.

[32] P.27 section 3.3.3.2 of the CP-02-2020: '*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*.'

[33] P.18 para.33(a) of the EBA Guidelines: *'…by comparing them with official databases, such as PRADO…'*.

xiii. Revises the practical guidance in relation to the electronic NFTF Identification laid down in section 3.3 of CP-02-2020[34] as a result of the novelties brought by the EBA Guidelines and the ESAs Opinion. In essence, most of the aspects of the said practical guidance have to be anyway incorporated into the policies and procedures of OEs in respect of any RCOS[35].

3. SUPERVISORY EXPECTATIONS AND GUIDANCE- INTERPLAY BETWEEN THE ESAS OPINION, CP-02-2020 AND THE EBA GUIDELINES

3.1. GENERAL INFORMATION ON THE ESAS OPINION AND THE EBA GUIDELINES

3.1.1. Similarly, to the approach stated in the ESAs Opinion[36], the EU Commission's view was also that due diligence rules in the EU AMLD do not provide sufficient clarity about what is, and what is not, allowed in a remote and digital context[37]. Thus, it is important that OEs can demonstrate that they have identified, assessed and mitigated all relevant risks before introducing RCOS in their NFTF Customer CDD process.

3.1.2. As per the ESAs Opinion[38], OEs should inform CySEC of RCOS they intend to use - while such notifications would not result in an express approval of a particular solution. This is the reason for CySEC requesting prior notification before OEs use RCOS for NFTF Customer CDD purposes and not adopting the proposal by various stakeholders to certify or otherwise approve developers/providers of RCOS, which in any case does not currently fall under CySEC's statutory

[34] P.26 section 3.3.3 of CP-02-2020.

[35] See for example P.13 para.19 of the ESAs Opinion: '*Where customers are required to transmit their ID documentation, data or information via video conferences, mobile phone apps or other digital means…*'.

[36] P.4 para.10 of the ESAs Opinion.

[37] P. 3 and P.4 para.2 of the EBA Guidelines.

[38] P.19 para.25 of the ESAs Opinion.

mandate. In addition, as also laid down in the ESAs Opinion[39] and CP-02-2020[40], the EBA Guidelines[41] do not favour specific technological solutions either and do also observe the principle of technological neutrality[42]. However, while the standards laid down in the ESAs Opinion[43] applied only vis-à-vis NCAs, hence the incorporation of those standards in CP-02-2020[44] as supervisory expectations to be complied with by OEs, the EBA Guidelines[45] apply directly towards both NCAs and OEs[46], while having been issued as common EU standards.

3.1.3. Without prejudice to CySEC's Circular 465 declaring the applicability of the EBA Risk Factor Guidelines, it should be borne in mind that the content of the EBA Guidelines[47] has also to be assessed against the background of following Guidelines, since the EBA Guidelines complement these and cross-refer thereto:

i. EBA Guidelines on 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 ('***The ML/TF Risk Factors Guidelines'***) under Articles 17 and 18(4) of Directive (EU) 2015/849;

ii. EBA Guidelines on internal governance under Directive 2013/36/EU;

[39] P.6 para.15 of the ESAs Opinion: '*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…'.*

[40] See Annex 1 of CP-02-2020 containing the proposed amendment of the CySEC AMLD (para.3 of the suggested new CySEC AMLD), where no specific RCOS are being favoured.

[41] P.38 of the EBA Guidelines: '*Once the conditions set out in this Guideline are fulfilled, the technical details are at the discretion of the credit and financial institution*'.

[42] P.5 para.6 of the EBA Guidelines.

[43] P.1 para.2 of the ESAs Opinion.

[44] See also P.16 section 2.5.1 of CP-02-2020.

[45] P.9 para.1 of the EBA Guidelines.

[46] The addressees of the EBA Guidelines are financial institutions, within the meaning of the AMLD. For level playing field purposes among OEs and supervisory consistency purposes, the policy decisions laid down in this PS apply across all OEs.

[47] P.5 para.9 of the EBA Guidelines with relevant references.

iii. EBA Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849;

iv. EBA Guidelines on outsourcing arrangements; and

v. EBA Guidelines on ICT and security risk management.

3.2. THE EXTENSION OF THE MATERIAL SCOPE OF APPLICATION TO LEGAL ENTITIES AND THE ISSUE OF RELIANCE ON THIRD PARTIES

3.2.1. The material scope of the policy decisions suggested in CP-02-2020[48] which was limited to the remote onboarding of natural persons being NFTF Customers has now been extended to also encompass legal entities in reliance to the EBA Guidelines[49]. Furthermore, the material scope of the ESAs opinion also included certain obligations that went beyond initial NFTF Customer CDD and extended to ongoing monitoring tasks[50]. However, the EBA Guidelines[51], clearly limit their material scope to the initial onboarding of NFTF Customers[52], so that ongoing monitoring obligations of the business relationship are not encompassed by the policy decisions laid down herein. At this point, it is important to distinguish between ongoing monitoring of the relationship with the NFTF Customer, which is out of scope of this PS, and ongoing monitoring of the RCOS[53], which falls within scope[54]. Without prejudice to the aforesaid, OEs are obliged to monitor

[48] P. 4 section 1.1.3 of CP-02-2020.

[49] P.17 para.29 of the EBA Guidelines.

[50] P. 5 para.14 of the ESAs Opinion, P. 11 para.18b of the ESAs Opinion, P.12 para.18c of the ESAs Opinion and P.15 para. 19d of the ESAs Opinion.

[51] P.10 para.5 of the EBA Guidelines and particularly p.29 of the EBA Guidelines: '*This means that the scope is limited to initial customer due diligence processes under Article 13(1) (a), (b) and (c) of the AMLD*'.

[52] Art.13(1)(a)-(c) of the EU AMLD corresponding to section 61(1)(a)-(c) of the AML/CFT Law.

[53] P.14 para.18 of the EBA Guidelines.

[54] P.37 of the EBA Guidelines: '*The ongoing monitoring requirements addressed to credit and financial institutions relate to the quality, completeness, accuracy, and adequacy of the data for CDD purposes, which remains the responsibility of credit and financial institutions*'.

their business relationships on an ongoing basis, taking into account relevant applicable rules[55] and material published by standard setters, including CySEC, EBA and FATF and to take appropriate measures where this is deemed necessary.

3.2.2. In addition, the obligations incumbent on OEs for NFTF Customer CDD pursuant to the EBA Guidelines[56] also cover cases where performance of NFTF Customer CDD takes place by third parties in accordance with section 67 of the AML/CFT Law[57]; namely cases of reliance on third parties and outsourcing respectively, as it was also the case under the ESAs Opinion[58]. However, the EBA Guidelines[59], which unlike the ESAs Opinion are also addressed to OEs, require OEs to devise policies and procedures when onboarding NFTF Customers by means of RCOS and to include therein certain specifications; those specifications should be setting out which NFTF Customer onboarding functions and activities will be carried out or performed by the OE itself, by third parties or by another outsourced service provider. In cases of reliance on third parties, OEs should, in addition to the EBA Risk Factors Guidelines, in particular to guidelines 2.20 to 2.21 and 4.32 to 4.37 thereof, also apply the following criteria:

i. Take the steps necessary to be satisfied that the third party's own NFTF Customer CDD processes and procedures and the information and data they collect in this context, are sufficient and consistent with requirements laid down herein;

ii. Ensure the continuity of the business relationships established between the NFTF Customer and the OE to guard against events that might reveal shortcomings on the NFTF Customer on-boarding process carried out by the third party in question.[60]

[55] Including applicable sanctions and/or restrictive measures.

[56] P.10 para.5 of the EBA Guidelines.

[57] Corresponding to the reference to Chapter I, Section 4 of the AMLD in the EBA Guidelines.

[58] P.7 para.16 and P.8 para.17 of the ESAs Opinion.

[59] P.21 para.46 of the EBA Guidelines.

[60] P.21 para.47 of the EBA Guidelines.

3.2.3. Finally, the EBA Guidelines and subsequently the policy decisions laid down herein apply specifically to new business relationships[61], in situations where OEs adopt a new RCOS[62] and in situations where OEs review RCOS already in place[63]. Nevertheless, the guidance laid down herein may also be useful in situations where OEs perform remote CDD on existing Customers[64].

3.2.4. Generally, the EBA Guidelines should be read in conjunction with the EBA Risk Factor Guidelines[65], as these set out risk factors that also apply in the remote onboarding context.[66]

3.3. THE GRAVITY ASSIGNED TO THE EIDAS REGULATION PURSUANT TO THE EBA GUIDELINES AND THE POSSIBILITY TO USE ALTERNATIVE SOURCES

3.3.1. While the ESAs Opinion[67] and CP-02-2020[68] primarily rely (regarding eligible types of identity documents for managing impersonation fraud risk) on eIDAS Regulation-compliant solutions and on other solutions having high security, in particular biometric, features, the EBA Guidelines clarify that the use of solutions that are not within the scope of the eIDAS Regulation is also permitted.

3.3.2. More specifically, the EBA Guidelines[69] place significant importance on the comfort, without such comfort amounting to an exemption from governance provisions though, provided by RCOS using one of the following:

[61] P. 33 of the EBA Guidelines.

[62] P.36 of the EBA Guidelines.

[63] P.33 of the EBA Guidelines.

[64] P. 29&33 of the EBA Guidelines.

[65] P.33 of the EBA Guidelines.

[66] P.34 of the EBA Guidelines.

[67] P.14 para.19c of the ESAs Opinion and P.16 para.20a of the ESAs Opinion.

[68] P.25 para. 3.3.1.3 of CP-02-2020.

[69] E.g. P.13 para.15 of the EBA Guidelines, P.16 para.25 of the EBA Guidelines, P.21 para.45 of the EBA Guidelines.

i. Electronic identification schemes notified in accordance with Article 9 of the eIDAS Regulation and meeting the requirements of assurance levels '*substantial'* or '*high*' in accordance with Article 8 of that Regulation;

ii. Relevant qualified trust services that meet the requirements of the eIDAS Regulation, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation, the reason being that many of the requirements set out in the EBA Guidelines are deemed to be fulfilled where the RCOS in question uses any of the aforesaid. As per the EBA Guidelines[70], by resorting to digital interties under the eIDAS Regulation framework, some aspects of the policies and procedures on using RCOS to onboard NFTF Customers, may have been covered in the assessments conducted as part of rigorous conformity assessments and peer-to-peer reviews under Articles 8-12 of the eIDAS Regulation. This allows OEs, to the extent possible, to leverage the assessments already conducted, with the ultimate responsibility for the underlying verification process still lying with the OEs though.[71]

Thus, it merits clarification that reliance on solutions using eIDAS-compliant safeguards can be placed under this PS, but is not tantamount to an exemption from governance requirements. As regards which are those requirements, which can be met by eIDAS-compliant solutions, relevant reference is made throughout the text.

3.3.3. At the same time, the EBA Guidelines[72] clarify that the use of solutions that are not within the scope of the eIDAS Regulation is permitted, because Article 13(1) (a) of the EU AMLD[73] provides that relevant trust services and other solutions that are regulated, recognized, approved or accepted at a national level might also be used to perform the identification and verification process. The use of such other solutions, e.g. of non-qualified trust services or other solutions that are regulated, recognized, approved, or accepted at a national level remains possible in line with the Article 13(1) (a) of the EU AMLD/section 61(1)(a) of the

[70] P.26 of the EBA Guidelines.

[71] P.26 of the EBA Guidelines.

[72] P.30 of the EBA Guidelines.

[73] Corresponding to section 61(1)(a) of the AML/CFT Law.

AML/CFT Law, subject to specific safeguards being applied.[74] More specifically, when using the said solutions, OEs should assess in how far these comply with this PS and apply measures necessary to mitigate any relevant risks that arise from the use of such solutions, in particular the:

i. Risks involved in the authentication and set out in their policies and procedures specific mitigation measures, especially with regard to impersonation fraud risks;

ii. Risk that the NFTF Customer's identity is not the claimed identity;

iii. Risk of lost, stolen, suspended, revoked, or expired identity evidence, including, as appropriate, tools to detect and prevent the use of identity frauds.[75&76]

3.4. THE DISTINCTION BETWEEN '*ATTENDED*' AND '*UNATTENDED*' SOLUTIONS IN THE EBA GUIDELINES AND THEIR PRACTICAL RELEVANCE

3.4.1. Another novelty introduced by the EBA Guidelines[77] and adopted in this PS is the distinction of the RCOS to be used by OEs for onboarding NFTF Customers into attended and unattended ones. The practical consequence of this distinction is that, unlike the holistic approach taken under CP-02-2020[78], mandatory liveness detection is now required, in all (irrespective of the level of ML/TF risk) cases of unattended solutions only: *'The…use of liveness detection*[79]

[74] P.32 of the EBA Guidelines.

[75] P.23 para.54 of the EBA Guidelines.

[76] Further explanation on the rationale adopted can be found on p.42f. of the EBA Guidelines: '*In conclusion, when using nonqualified trust services and those identification processes regulated, recognised, approved, or accepted by the national relevant authority, it should be up to the credit and financial institutions to assess and make sure that they still meet the standards established in the EBA guidelines. To ensure a robust approach to remote customer onboarding, the Guidelines set out the safeguards institutions should apply in those cases. Finally, the EBA is aware that the European Commission's proposal to review the eIDAS Regulation and introduce a European Digital Identity Wallet would significantly help overcome the existing fragmentation in this area. However, until the review is finalised and enters into force, the EBA must base its assessment on the existing regulatory framework.*'

[77] P.28 of the EBA Guidelines.

[78] P.26f. para. 3.3.3 of CP-02-2020 on the onboarding procedure by means of dynamic selfie and/or video-call.

[79] P.28 of the EBA Guidelines. See also p.41f. of the EBA Guidelines: *'This guideline does not establish the liveness detection methods that might be used. As stated in guideline 43, it is up to the credit and financial*

only in unattended situations, i.e. where the [NFTF] customer does not interact with an employee of the credit and financial institution to perform the verification process. This means that all unattended situations, with fully automated remote verification, would require liveness detection (apart from situations where credit and financial institutions resort to Digital Identity Issuers). Unattended situations are highly dependent on the technology with little or no direct human intervention. Requiring liveness detection will increase the reliability of the verification process. This approach is proportionate, acknowledges the advances in technology and makes sure that liveness detection is deployed when most needed.'

3.5. REQUIREMENTS TO BE COMPLIED WITH PRIOR TO THE INTRODUCTION OF THE RCOS IN THE ON-BOARDING PROCESS OF NFTF CUSTOMERS AND ON AN ONGOING BASIS

3.5.1. GENERAL OVERVIEW

3.5.1.1. CP-02-2020[80] required OEs to incorporate the on-boarding of NFTF Customers by means of RCOS in their NFTF CDD procedures and carry out the Risk Assessment prior to the introduction of such method(s). The EBA Guidelines, which set common EU standards on the development and implementation of sound, risk-sensitive initial CDD processes in the NFTF Customer onboarding context[81], reaffirm and further elaborate on those obligations of OEs. More specifically, the EBA Guidelines require OEs to carry out a pre-implementation assessment[82] prior to the introduction of the RCOS, which is the term employed in the EBA Guidelines to describe the Risk Assessment; and to produce NFTF CDD policies and procedures or carry out relevant amendments to existing ones (as the case may be).

---

institution to decide whether liveness detection should be performed actively or passively. ISO 30.107 defines several standards for liveness detection techniques that might be consulted by the credit and financial institution.'

[80] P.22 para.3.2.2. and P.12 para. 2.3.1 of the CP-02-2020.

[81] P.3 of the EBA Guidelines.

[82] As to avoiding duplication of tasks in a group context, it is stated on P.43 of the EBA Guidelines: '*The remote customer onboarding processes carried out by intra-group entities should follow the same approach as the other methods of onboarding new customers, therefore, the same principles should be applied. This means that, for example, nothing prevents the use of the pre-implementation assessment carried out by an entity of the group that uses the remote customer onboarding solution by another entity of the group'.*

3.5.1.2. Furthermore, given that the Risk Assessment may also have to take place in the future, e.g. upon re-assessment of existing or introduction of additional RCOS, the requirements in relation to the Risk Assessment must be incorporated in the OE's NFTF CDD policies and procedures.[83] In addition to these high-level formulated requirements, the EBA Guidelines, when read jointly with the ESAs Opinion, further substantiate the structure and content of the Risk Assessment and of the said policies and procedures. For this reason, the following sections will present how the supervisory expectations initially laid down in CP-02-2020 are further substantiated following the issuance of the EBA Guidelines and their interaction with the ESAs Opinion. Thus, the topics substantiated herein relate both to the content of the Risk Assessment, including further guidance thereupon, as well as to the OE's policies and procedures regarding NFTF CDD.

3.5.1.3. It is clarified that the purpose of this Section is to facilitate the implementation of the content of the EBA Guidelines, the ESAs Opinion and the revised practical guidance (initial version included in section 3.3. of CP-02-2020), by analysing the interplay of those documents and to outline the additional documents to be considered by OEs, when using RCOS. However, the content of this Section should be used merely for facilitating a thorough review of the relevant material by OEs and shall neither be considered as exhaustive nor may replace a thorough study of the relevant material by OEs.

3.5.2. THE FACTORS TO BE CONSIDERED IN THE RISK ASSESSMENT AND GUIDANCE IN RELATION THERETO

3.5.2.1. In accordance with the ESAs Opinion[84] and the initial policy approaches laid down in CP-02-2020[85], OEs should consider in the Risk Assessment[86] a number of factors when assessing the extent to which the intended use of RCOS is adequate in the light of the ML/TF risk[87] associated with individual business relationships. Those factors to be considered were both regulatory but also

[83] P.13 para.14 of the EBA Guidelines.

[84] P.6 para.15 of the ESAs Opinion.

[85] P.16 para. 2.5.1 of CP-02-2020.

[86] Which has to take place per RCOS to be applied, as per P.23 para.3.2.3 of CP-02-2020.

[87] Same approach under the EBA Guidelines P.12 para.9.

technological in nature, in particular the idiosyncratic risks related to the introduction of the RCOSs.[88]. In the meantime, the EBA Guidelines were issued and the feedback of stakeholders has been taken into consideration. Thus, based on the ESAs Opinion[89], the CP-02-2020[90], the EBA Guidelines[91] and this PS after considering stakeholders' contributions, the Risk Assessment must be risk-based approach and should consider:

i. Articles 58(a), 58(d), 58(A)[92], 61(2) and 66(2A), in conjunction with Annex III of the AML/CFT Law and with Part IV of the CySEC AMLD;

ii. The technical (implementation) standards laid down in the FATF Guidance[93] aiming at establishing the required assurance level[94];

iii. A testing of the solution prior to the introduction of the RCOS in question, for which further guidance is provided under section 3.5.3.3 below herein;

iv. The reliability of NFTF Customer CDD measures for which further guidance is provided under section 3.5.3.4 below herein;

v. Delivery channel risks, in the context of using an RCOS for onboarding NFTF Customers, for which further guidance is provided under section 3.5.3.1 below herein;

vi. Geographical risks, in the context of using an RCOS for onboarding NFTF Customers, for which further guidance is provided under section 3.5.3.2 below herein;

[88] P.9 para. 1.5.2 of CP-02-2020.

[89] P.6 para.15 of the ESAs Opinion.

[90] P.16 para.2.5.1 of CP-02-2020 and P.22 para.3.2.1 of CP-02-2020.

[91] P.33 of the EBA Guidelines.

[92] Section 58A AML/CFT Law corresponds to Article 8 of the EU AMLD.

[93] P.12 para. 2.3.1 of CP-02-2020.

[94] P.13 para. 2.3.4 of CP-02-2020.

vii. The content of CySEC's Circular C399 on Financial Action Task Force (FATF) COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses;

viii. CySEC's Circular 465 (on the adoption of the EBA Risk Factor Guidelines);

ix. The level of assets to be deposited and the size of transactions involved per RCOS (including per combination of RCOS, where applicable) and per NFTF Customer risk category as an additional CDD measure that will have to be undertaken on a case-by-case basis per type of risk identified[95];

x. The revised practical guidance (initial version included in section 3.3. of CP-02-2020) attached as Annex IV hereto;

xi. OEs should also ensure by means of relevant assessments compliance with the GDPR as well as with any other relevant legislation, as GDPR applies also in the context of onboarding of NFTF Customers;

3.5.3. GUIDANCE IN RELATION TO CERTAIN FACTORS INCLUDED IN THE RISK ASSESSMENT AND ON THE POLICIES AND PROCEDURES

3.5.3.1. GUIDANCE ON ASSESSING THE DELIVERY CHANNEL RISKS

3.5.3.1.1. The delivery channel risk in the context of RCOS for NFTF Customer CDD purposes, relates to the assessment by OEs of ML/TF risks associated with non-face-to-face business relationships; and the extent to which the use of RCOS can address, or might further exacerbate, those risks.[96] To this end, OEs should assess the existence of impersonation risk[97] and demonstrate that they have assessed the availability and effectiveness of safeguards that could mitigate this risk. Such safeguards may include:

[95] P.22 para. 3.2.3 of the CP-02-2020.

[96] P.16 para.20 of the ESAs Opinion.

[97] P.16 para.20a of the ESAs Opinion: '*…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)…*'

i. The verification of a customer's identity on the basis of a notified eID scheme, as defined in the eIDAS Regulation, where the scheme's assurance level is classified as high[98];

ii. The use of solutions that are not within the scope of the eIDAS Regulation[99] subject to observance of relevant safeguards;

iii. A combination of other checks that ensure the information obtained during the transmission can be linked to a particular NFTF Customer, for example:
   a) The verification of an NFTF Customer's identity based on multiple factors and data sources. For example, the NFTF Customer's personal information can be 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;
   b) Built-in features that allow OEs to detect their NFTF Customers' native language based on their written communications with them;
   c) A requirement that all NFTF Customer CDD documentation contains a qualified electronic signature created in line with standards set in the eIDAS Regulation;
   d) Verifying an NFTF Customer's identity on the basis of more traditional processes such as sending a letter to the customer's verified home address[100&101].

iv. Tests in the context of the Risk Assessment '*to assess fraud risks including impersonation fraud risks and other information and communications technology **('ICT')** and security risks, in accordance with the provision 43 of the EBA Guidelines on ICT and security risk management'*.[102] This

[98] P.16 para.20a of the ESAs Opinion.

[99] P.32 of the EBA Guidelines.

[100] See to this end the hybrid safeguards provided under P.20f. ra.44 of the EBA Guidelines.

[101] P.16 para.20a of the ESAs Opinion.

[102] P.13 para. 14d of the EBA Guidelines.

criterion is considered to be met by default where the solution uses one of the following:

a) Electronic identification schemes notified in accordance with Article 9 of the eIDAS Regulation and meeting the requirements of assurance levels '*substantial*' or '*high*' in accordance with Article 8 of that Regulation;

b) Relevant qualified trust services that meet the requirements of the eIDAS Regulation, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation[103].

v. In addition to safeguards against impersonation fraud risks, the consideration of the delivery channel risks also includes assessing the existence of coercion risk. For this reason, OEs should implement strong controls to identify cases of coercion. Such controls may include a built-in technical feature in the RCOS; or that an NFTF Customer is required to have a live chat with an administrator who is well trained to spot any abnormalities in the customer's behaviour. This may assist in identifying situations where the NFTF Customer is behaving suspiciously (e.g. psychological profiling).[104] The EBA Guidelines[105] provide further guidance in this respect: '*Where possible, credit and financial institutions should use remote customer onboarding solutions that include randomness in the sequence of actions to be performed by the customer for verification purposes to guard against risks such as the use of synthetic identities or coercion. Where possible, credit and financial institutions should also provide random assignments to the employee responsible for the remote verification process to avoid collusion between the customer and the responsible employee*'. This EBA Guidelines[106] criterion is considered to be met by default where the RCOS uses one of the following:

a) Electronic identification schemes notified in accordance with Article 9 of the eIDAS Regulation and meeting the requirements of assurance levels '*substantial*' or '*high*' in accordance with Article 8 of that Regulation;

[103] P.13 para.15 of the EBA Guidelines.

[104] P.16f. para.20b of the ESAs Opinion.

[105] P.20 para.43 of the EBA Guidelines.

[106] P.21 para.45 of the EBA Guidelines.

b) Relevant qualified trust services that meet the requirements of Regulation (EU) No 910/2014, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation.

3.5.3.2. GUIDANCE ON ASSESSING THE GEOGRAPHICAL RISK

3.5.3.2.1. The geographical risk in the context of NFTF business relationships means that a NFTF Customer tries to access financial services in another MS for ML/TF purposes[107], i.e. it is a risk emanating from the nature of the NFTF relationship[108]. OEs should assess geographical risks presented by a business relationship, including through:

i. Controls OEs may have in place that capture their NFTF Customers' 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.[109] In alignment therewith, the EBA Guidelines[110] also require that OEs establish and maintain mechanisms ensuring that the information they capture automatically, in order to identify a natural person being a NFTF Customer or a natural person acting on behalf of a legal person, is reliable. Furthermore, OEs must apply controls to address associated risks, including risks associated with automatic capture of data, such as the obfuscation of the location of the customer's device, spoofed Internet Protocol (IP) addresses or services such as Virtual Private Networks (VPNs); and

ii. Practices to assess the reasons why NFTF Customers from other jurisdictions are using their services[111].

[107] P.17 para.22 of the ESAs Opinion.

[108] P.20 para.2.6.5 of the CP-02-2020.

[109] P.17 para.22 of the ESAs Opinion.

[110] P.17 para.28 of the EBA Guidelines.

[111] P.17 para.22 of the ESAs Opinion.

3.5.3.3. GUIDANCE ON TESTING THE RCOS PRIOR TO ITS INTRODUCTION

3.5.3.3.1. OEs shall carry out an assessment of the RCOS with the relevant control functions' involvement prior to introducing the RCOS in question in their NFTF Customer onboarding operations.

3.5.3.3.2. The aforesaid assessment should include a full testing of the RCOS in question. The results of this testing should be available upon CySEC's request and should attest to the compatibility of the RCOS in question with the OE's NFTF CDD policies and procedures and with the applicable regulatory framework[112&113]. As to the testing itself, the EBA Guidelines[114] provide further guidance requiring '*an end-to-end testing of the functioning of the solution targeting customer(s), product(s) and service(s) identified in the remote customer onboarding policies and procedures*'. Certain aspects of the testing are considered to be met by default where the RCOS to be introduced uses one of the following:

i. Electronic identification schemes notified in accordance with Article 9 of the eIDAS Regulation and meeting the requirements of assurance levels '*substantial*' or '*high*' in accordance with Article 8 of that Regulation;

ii. Relevant qualified trust services that meet the requirements of the eIDAS Regulation, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation[115];

[112] Same approach taken under the EBA Guidelines: P.13 para. 14e of the EBA Guidelines.

[113] P.8 para.17a of the ESAs Opinion.

[114] P.13 para. 14e of the EBA Guidelines.

[115] P.13 para.15 of the EBA Guidelines.

3.5.3.3.3. In case where the testing results are inconclusive, the ESAs Opinion[116] requires a co-existence of legacy solutions and RCOS[117] for as long as is necessary, in order to have full confidence in the RCOS[118].

3.5.3.3.4. As a necessary prerequisite of the Risk Assessment and in order to ensure a complete and thorough understanding of the RCOS, OEs should in particular consider whether they have sufficient in-house expertise, over and above any external expert advice, in order to guarantee the implementation and use of the RCOS. Additionally, OEs should consider whether they have contingency plans in place. The said contingency plans should ensure the continuation of operation should the RCOS suffer irreparable system failure or should the business relationship between the OE and the external provider of the RCOS be terminated (where it is not developed in-house). Bearing the aforesaid in mind, the following shall be assessed in the Risk Assessment:

i. Whether or not the OE has appropriate technical skills to oversee the development and proper implementation of the RCOS, particularly where it is developed or used by a third party (where reliance is placed on such third party in line with section 67 of the AML/CFT Law) or an external provider[119]. This requirement is further substantiated by the EBA Guidelines[120&121] which require a description of the induction and regular training programs. The aim thereof is to ensure staff awareness and up-to-date knowledge of the functioning of the RCOS in question, of the associated risks, of the NFTF CDD onboarding policies and procedures

[116] P.8 para.17a of the ESAs Opinion.

[117] Examples of '*hybrid*' onboarding involving use of conventional methods can be found on P.20f. para.44 of the EBA Guidelines: *'…a) the first payment is drawn on an account in the sole or joint name of the customer with an EEA-regulated credit or financial institution or in a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849; b) send a randomly generated passcode to the customer to confirm the presence during the remote verification process. The passcode should be a single-use and time-limited code; c) capture biometric data to compare them with data collected through other independent and reliable sources; d) telephone contacts with the customer; e) direct mailing (both electronic and postal) to the customer*'.

[118] As regards such '*hybrid safeguards*' see p.20f. para.44 of the EBA Guidelines

[119] P.7 para.16 of the ESAs Opinion.

[120] P.12 para.9e of the EBA Guidelines.

[121] P.12 para.9c of the EBA Guidelines.

aimed at mitigating such risks as well as a determination of which steps are fully autonomized and which steps require human intervention;

ii. Whether or not the senior management and the AML/CFT Compliance Officer of the OE have appropriate understanding of the RCOS[122];

iii. That the RCOS can be integrated into the OE's wider internal control system, thereby allowing the OE to adequately manage the ML/TF risks that may arise from the use of the RCOS.[123]

3.5.3.4. GUIDANCE ON THE RELIABILITY OF NFTF CDD MEASURES

3.5.3.4.1. The reliability of NFTF CDD measures is to be understood in relation to the validity and authenticity of data, documentation and information obtained through RCOS in the context of the NFTF CDD process.[124] In this context, the EBA Guidelines[125] require an assessment of the adequacy of the RCOS regarding the completeness and accuracy of the data and documents to be collected, as well as of the reliability and independence of the sources of information the RCOS uses. This EBA Guidelines criterion is considered to be met by default where the RCOS uses one of the following:

i. Electronic identification schemes notified in accordance with Article 9 of the eIDAS Regulation and meeting the requirements of assurance levels *'substantial*' or '*high*' in accordance with Article 8 of that Regulation;
ii. Relevant qualified trust services that meet the requirements of Regulation (EU) No 910/2014, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation;[126]

3.5.3.4.2. Without prejudice to the generality of the foregoing, where NFTF Customers are required to transmit to the OE their identification document(s), data or information via video conferences, mobile phone apps or other digital means[127],

[122] P.7 para.16 of the ESAs Opinion.

[123] P.14 para.17 of the EBA Guidelines.

[124] P.13 para.19 of the ESAs Opinion.

[125] P.13 para. 14a of the EBA guidelines.

[126] P.13f. para.15 of the EBA Guidelines.

[127] This being the reason why the requirements under the practical guidance in section 3.3 of CP-02-2020 have become generally applicable.

then OEs should consider applying the following controls which should be taken into consideration and be assessed in the context of the risk assessment:

i. Avoidance or mitigation of risk of tampering by means of any or all of the following:
   a) A feature whereby an NFTF 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.[128] The EBA Guidelines[129], provide flexibility in this respect, since they introduce the distinction between attended solutions, i.e. solutions where the NFTF Customer interacts with staff of the OE during the verification process, and unattended ones, where no OE staff is participating. Thus, it is allowed to also use unattended solutions, subject to observance of the liveness detection requirement. In case of attended solutions, OEs should:
   '*a) ensure that the quality of the image and audio is sufficient to allow the proper verification of the customer's identity and that reliable technological systems are used;*
   b)foresee the participation of an employee that has sufficient knowledge of the applicable AML/CFT regulation and security aspects of remote verification and who is sufficiently trained to anticipate and prevent the intentional or deliberate use of deception techniques related to remote verification, and to detect and react in case of their occurrence; and
   c) develop an interview guide defining the subsequent steps of the remote verification process as well as the actions required from the employee. The interview guide should include guidance on observing and identifying psychological factors or other features that might characterise suspicious behaviour during remote verification.'[130]

   OEs should consider the criteria of point a-c above to be met where the solution uses one of the following:

[128] P.13 para.19a of the ESAs Opinion.

[129] P.20 para.42 of the EBA Guidelines.

[130] P.20 para.42 of the EBA Guidelines.

1) Electronic identification schemes notified in accordance with Article 9 of the eIDAS Regulation and meeting the requirements of assurance levels 'substantial' or 'high' in accordance with Article 8 of that Regulation;
2) Relevant qualified trust services that meet the requirements of the eIDAS Regulation, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation[131].

b) 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 to the extent permissible under GDPR).[132] The EBA Guidelines[133] provide further guidance in this respect: *'Where the RCOS involves the use of biometric data[134] to verify the NFTF Customer's identity, OEs should make sure that the biometric data is sufficiently unique to be unequivocally linked to a single natural person'.* Furthermore, strong and reliable algorithms should be used to verify the match between the biometric data provided on the submitted identity document and the NFTF Customer being onboarded. OEs should consider the aforesaid criteria laid down in the EBA Guidelines to be met by default where the solution uses one of the following:
   1) Electronic identification schemes notified in accordance with Article 9 of the eIDAS Regulation and meeting the requirements of assurance levels '*substantial*' or '*high*' in accordance with Article 8 of that Regulation;
   2) Relevant qualified trust services that meet the requirements of the eIDAS Regulation, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation.[135] The EBA Guidelines[136] also clarify that technical details of the use of

[131] P.21 para.45 of the EBA Guidelines.

[132] P.14 para.19a of the ESAs Opinion.

[133] P.19 para.39 of the EBA Guidelines.

[134] P.41 of the EBA Guidelines: '*The definition of 'biometric data' is aligned with GDPR regulation which also includes the reference to 'facial images*".

[135] P.21 para.45 of the EBA Guidelines.

[136] P.30 of the EBA Guidelines.

biometric data is outside of the scope of these guidelines and that these do not prevent the use of different forms of biometrics once they are sufficiently unique to be unequivocally linked to a single natural person.

c) A requirement for the screen to be adequately illuminated when taking a person's photograph or recording a video during the identity verification process.[137] Without prejudice to the application of this requirement in all cases where NFTF Customers are required to digitally transmit their identification document(s), data or information, the EBA Guidelines[138] provide further guidance in relation to lighting conditions in the context of **unattended** RCOS:
'*Where credit and financial institutions use unattended remote onboarding solutions, in which the customer does not interact with an employee to perform the verification process, they should:*
a) ensure that any photograph(s) or video is taken under adequate lighting conditions and that the required properties are captured with necessary clarity to allow the proper verification of the customer's identity;
b) ensure that any photograph(s) or video is taken at the time the customer is performing the verification process;
c) perform liveness detection verifications, which may include procedures where a specific action from the customer is required to verify that he/she is present in the communication session or which can be based on the analysis of the received data and does not require a specific action by the customer;
d) use strong and reliable algorithms to verify if the photograph(s) or video taken matches the picture(s) retrieved from the official document(s) belonging to the customer'. OEs should consider the aforesaid criteria to be met by default where the solution uses one of the following:

1) Electronic identification schemes notified in accordance with Article 9 of the eIDAS Regulation and meeting the requirements of assurance levels '*substantial*' or '*high*' in accordance with Article 8 of that Regulation;

[137] P.14 para.19a of the ESAs Opinion.

[138] P19f. para.41 of the EBA Guidelines.

2) Relevant qualified trust services that meet the requirements of the eIDAS Regulation, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation[139].

d) 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.[140] The EBA Guidelines[141] further require that, where available, during the verification process OEs should verify the security features embedded in the official document such as holograms, as a proof of their authenticity. In addition: *'Where possible, credit and financial institutions should use remote customer onboarding solutions that include randomness in the sequence of actions to be performed by the customer for verification purposes to guard against risks such as the use of synthetic identities or coercion*...'.[142] This criterion is considered to be met by default where the solution uses one of the following:

1) Electronic identification schemes notified in accordance with Article 9 of the eIDAS Regulation and meeting the requirements of assurance levels '*substantial*' or '*high*' in accordance with Article 8 of that Regulation;
2) Relevant qualified trust services that meet the requirements of Regulation (EU) No 910/2014, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation[143].

ii. Avoidance or mitigation of the risk of just similarity but not identity between the person participating in the transmission and the person depicted in the identification document either by means of built-in features of the RCOS in question or by means of specialised staff training[144].

[139] P.21 para.45 of the EBA Guidelines.

[140] P.14 para.19a of the ESAs Opinion.

[141] P.18 para.36 of the EBA Guidelines.

[142] P.20 para.43 of the EBA Guidelines.

[143] P.21 para.45 of the EBA Guidelines.

[144] P.14 para.19b of the ESAs Opinion.

iii. Avoidance or mitigation of the risk of unauthorised alterations[145] by means of any or all of the following:

a) Built-in features which enable OEs to detect fraudulent documents on the basis of the relevant document's 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);

b) 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 OE's internal identity document database. In situations where the device that the NFTF Customers use to prove their identity allows the collection of relevant data (for example because the data is contained in the chip of a national identity card, and it is technically feasible for the OE to access this data), the OE should consider using this information to verify its consistency with the information obtained through other sources, such as the submitted data or other documents submitted by the NFTF Customer[146];

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

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

2) A qualified electronic signature created in line with standards the eIDAS Regulation (especially relevant where a customer is a legal person);

3) A feature that links the RCOS with trade registers or other reliable data sources such as the database of a company registration office; or

4) A feature that adjoins the RCOS with the government-established CDD data repository (if any) or the notified e-ID scheme as defined in the eIDAS Regulation, if the scheme's assurance level is classified as substantial[147].

[145] P.14f. para.19c of the ESAs Opinion: *'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)'*.

[146] P.18 para.35 of the EBA Guidelines.

[147] P.14f. para.19c of the ESAs Opinion.

It is noted that given the ongoing character of the reliability of the RCOS, the guidance and requirements of this section have also to be reflected in the OE's policies and procedures in order to make sure that the required standards are kept on an ongoing basis.

3.5.3.5. OTHER SPECIFIC ISSUES TO BE ADDRESED IN THE RISK ASSESSMENT

3.5.3.5.1. When OEs make use of or intend to make use of RCOSs for NFTF Customer CDD purposes they should take into account the potential impact that this may have on the OEs' overall risk profiles[148]. To this end, the EBA Guidelines[149] require OEs to also assess the impact of the use of the RCOS on the OE's business-wide risks, including ML/TF, operational[150], reputational and legal risk as well as to identify possible mitigating measures and remedial actions for each risk identified in the said assessment. Under the ESAs Opinion[151] OEs should also identify and assess idiosyncratic risks associated with the RCOS and its provider/developer (where the solution is not developed in-house), e.g. no track record risk of the provider/developer, financial risk of the provider/developer etc.

3.5.3.5.2. OEs should, based on their analysis of the RCOS's characteristics and the assessment of ML/TF risks linked to their NFTF Customers and business relationships, be able to demonstrate that the RCOS is sufficiently reliable and commensurate with the level of ML/TF risks presented[152], having regard to section 61(2) of the AML/CFT Law.

3.5.3.5.3. Finally, the RCOS implemented by an OE should, as a minimum, allow for the following, as part of their verification process:

i. That there is a match between the visible information of the natural person and the documentation provided, whereas OEs should use strong and reliable algorithms to verify the match between the biometric data

[148] P.7 para.16 of the ESAs Opinion.

[149] P.13 para.14b and 14c of the EBA Guidelines.

[150] Also required under P.10 para.17j of the ESAs Opinion.

[151] P.10 para.17j of the ESAs Opinion.

[152] P.11 para.18 of the ESAs Opinion.

provided on the submitted identity document and the NFTF Customer being onboarded[153];

ii. That where the NFTF Customer is a legal entity, it is publicly registered (where applicable);

iii. That where the NFTF Customer is a legal entity, the natural person that represents it is entitled to act on its behalf [154].

3.5.3.5.4. The criteria under i-iii of the preceding paragraph are considered to be met by default where the RCOS uses one of the follow:

i. Electronic identification schemes notified in accordance with Article 9 of the eIDAS Regulation and meeting the requirements of assurance levels '*substantial*' or '*high*' in accordance with Article 8 of that Regulation;

ii. Relevant qualified trust services that meet the requirements of the eIDAS Regulation, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation[155];

3.5.3.5.5. In case of an RCOS provided by an external party located in a third country, whose rules prevent effective information sharing with the OE and/or CySEC, such solution shall be considered to have an unacceptable risk profile and shall not be adopted by the OE[156].

3.5.3.6. REQUIREMENTS ON THE NFTF CDD POLICIES AND PROCEDURES

3.5.3.6.1. GENERAL REQUIREMENTS ON THE POLICIES AND PROCEDURES RELATING TO THE ADOPTION OF THE RCOS

3.5.3.6.1.1. To adequately oversee and gain reasonable assurances that the RCOS to be employed by OEs is and will be operating appropriately and to prepare for situations should the solution break down or fail, OEs should have a full and thorough understanding of its features[157]. Proof of such understanding will have to be reflected in relevant policies and procedures[158] on an ongoing basis

[153] P.19 para.39 of the EBA Guidelines.

[154] P.19 para.38 of the EBA Guidelines.

[155] P.21 para.45 of the EBA Guidelines.

[156] P.11 para.17k of the ESAs Opinion.

[157] P.7 para.16 of the ESAs Opinion.

[158] P.12 para.9 of the EBA Guidelines.

following testing as well. The EBA Guidelines[159] specify that OEs must devise a general description of the RCOS put in place to collect, verify, and record information throughout the NFTF Customer CDD process, which should include an explanation of the features and functioning of the RCOS in question. Furthermore, OEs should specify the situations where the RCOS can be used. This shall be done by taking into account the risk factors identified and assessed in accordance with section 58A of the AML/CFT Law in conjunction with Annex III to the AML/CFT Law and with Part IV of the CySEC AMLD and the Risk Assessment, including a description of the category of NFTF Customers, products and services that are eligible for remote on-boarding[160];

3.5.3.6.1.2. The senior management and the AML/CFT Compliance Officer of the OE must have appropriate understanding of the RCOS.[161] The EBA Guidelines[162] require the involvement of the AML/CFT Compliance Officer and of the BoD in the preparation of the policies and procedures relating to the use of the RCOS by the OE: '*In addition to the provisions set out in the Section 4.2.4 of the EBA Compliance Officer Guidelines, the AML/CFT Compliance Officer should, as part of their general duty to prepare policies and procedures to comply with the CDD requirements, make sure that remote customer onboarding policies and procedures are implemented effectively, reviewed regularly and amended where necessary. The management body of the credit and financial institution should approve remote customer onboarding policies and procedures and oversee their correct implementation*; and

3.5.3.6.1.3. In addition to the aforesaid, the OEs must have proper contingency plans in place[163].

[159] P.12 para. 9a of the EBA Guidelines.

[160] P.12 para.9b of the EBA Guidelines.

[161] P. 13 para. 11 of the EBA Guidelines.

[162] P.13 paras 11 and 12 of the EBA Guidelines.

[163] P.7 para.16 of the ESAs Opinion.

3.5.3.6.2. SPECIFIC REQUIREMENTS ON THE POLICIES AND PROCEDURES RELATING TO THE ADOPTION OF THE RCOS

3.5.3.6.2.1. The EBA Guidelines[164] require that the policies and procedures of OEs regarding onboarding of NFTF Customers by means of RCOS also include:

i. The steps OEs will take to be satisfied of the ongoing quality, completeness, accuracy and adequacy of data collected during the NFTF Customer onboarding process. Those steps should be commensurate to the ML/TF risks to which the OE is exposed to, whereas it is not to prescribe which documents and data that should be collected during the process[165]. OEs should also ensure within this context that:
   a) The information obtained through the RCOS is up to-date and adequate to meet the applicable legal and regulatory standards for initial customer due diligence;
   b) Any images, video, sound and data are captured in a readable format and with sufficient quality so that the customer is unambiguously recognisable; and
   c) The identification process does not continue if technical shortcomings or unexpected connection interruptions are detected. 166

   OEs should consider the criteria under points a)-c) of the previous sentence directly above to be met by default where the RCOS in question uses one of the following:
   a) Electronic identification schemes notified in accordance with Article 9 of the eIDAS Regulation and meeting the requirements of assurance levels '*substantial*' or '*high*' in accordance with Article 8 of that Regulation;
   b) relevant qualified trust services that meet the requirements of the eIDAS Regulation, in particular Chapter III, Section 3 and Article 24 (1), subparagraph 2, point (b) of that Regulation[167].

   In those cases, the Guidelines should be read in conjunction with the eIDAS Regulation[168].

[164] P.14 para. 18a of the EBA Guidelines.

[165] P.31 of the EBA Guidelines.

[166] P.16 para.24 of the EBA Guidelines.

[167] P.16 para.25 of the EBA Guidelines.

[168] P.31 of the EBA Guidelines.

ii. The scope and frequency of such regular reviews[169].

iii. The circumstances that will trigger ad hoc reviews, which should include at least:
   a) Changes to the ML/TF risk exposure of the OE;
   b) Deficiencies on the functioning of the RCOS detected in the course of monitoring, audit or supervisory activities;
   c) A perceived increase in fraud attempts; and
   d) Changes to the legal or regulatory framework170.

   The requirements under i)-iii) above herein also apply where fully automated RCOS are used which are highly dependent on automated algorithms, without or with little human intervention[171].

iv. The information OEs need to obtain, as there is no relevant prescription in the EBA Guidelines, in order to identify NFTF Customers in accordance with section 61(a) and (c) of the AML/CFT Law.[172] More specifically, OEs need to lay down in their policies and procedures the information needed to identify the NFTF, the types of documents, data, or information the institution will use to verify the customer's identity and the manner in which this information will be verified[173].

v. In case of RCOS that have not been developed in-house or where reliance on a third party using these is being placed, OEs should ensure a clear allocation of roles with the external provider and retain a '*saying*' by means of relevant contractual and operational arrangements, regarding changes to the RCOS or the NFTF Customer CDD measures and processes.

---

[169] P.14 para.18b of the EBA Guidelines and P.37 of the EBA Guidelines: '*The Guidelines provide that credit and financial institutions should define in their policy with which frequency and according to which process they intend to carry out ongoing reviews. The ongoing monitoring requirements addressed to credit and financial institutions relate to the quality, completeness, accuracy, and adequacy of the data for CDD purposes, which remains the responsibility of credit and financial institutions*'.

[170] Page 14 para.18c of the EBA Guidelines.

[171] P.15 para.21 of the EBA Guidelines.

[172] P.16 para.27 of the EBA Guidelines.

[173] P.16 para.23 of the EBA Guidelines.

3.5.3.6.3. CONTENT OF POLICIES AND PROCEDURES IN RELATION TO INFORMATION FROM NFTF CUSTOMERS (NATURAL PERSONS AND LEGAL PERSONS)

3.5.3.6.3.1. As regards NFTF Customers being natural persons, the EBA Guidelines[174] require OEs to define in their policies and procedures what information is:

i. Manually entered by the said Customer;
ii. Automatically captured from the documentation provided by such Customer. Where this is the case, the EBA Guidelines[175] further require that where OEs use features to automatically read information from documents, such as Optical Character Recognition (OCR) algorithms or Machine Readable Zone (MRZ) verifications, they should take the steps necessary to ensure that that these tools capture information in an accurate and consistent manner; and
iii. Gathered using other internal or external sources.

3.5.3.6.3.2. As regards NFTF Customers being legal entities, the EBA Guidelines[176] require OEs to define in their policies and procedures which category of legal entities they will on-board remotely, taking into account the level of ML/TF risk associated with each such category, and the level of human intervention required to validate the identification information. Additionally, OEs should ensure that the NFTF Customer on-boarding solution has features to collect:

i. All relevant data and documentation to identify and verify the legal entity[177] in question;
ii. All relevant data and documentation to verify that the natural person acting on behalf of the legal person is legally entitled to act as such; and
iii. The information regarding the beneficial owners in accordance with provision 4.12 of the EBA Risk Factor Guidelines[178].

[174] P.16f. para.27 of the EBA Guidelines.

[175] P.18 para.34 of the EBA Guidelines.

[176] P.17 paras 29 of the EBA Guidelines.

[177] The EBA Guidelines use the term '*legal person*', but this seems to contradict the previous reference to '*legal entities*', which is a broader including but not limited to legal persons.

[178] P.17 para.30 of the EBA Guidelines.

Regarding the natural person acting on behalf of a legal entity, OEs should apply the identification process described in the preceding paragraph in relation to natural persons[179].

3.5.3.6.3.3. In any case where the evidence provided is of insufficient quality resulting in ambiguity or uncertainty so that the performance of remote checks is affected, the EBA Guidelines[180] require that '*the individual remote customer onboarding process should be interrupted and restarted or redirected to a face-to-face verification*'.

3.5.3.6.3.4. **Excurse: Financial inclusion**

The EBA Guidelines[181] allow for a more lenient treatment of documents received from NFTF Customers for the purposes of financial inclusion: OEs should set out in their policies and procedures how they will adjust their documentation requests for the purposes of financial inclusion. Where weaker or non-traditional forms of documentation are accepted as a result, OEs should carry out in addition to measures as set out in paragraph 4.10 of the EBA Risk Factors Guidelines, controls or increased human intervention to satisfy themselves that they understand the ML/TF risk associated with the business relationship.[182] However in view of CySEC explicitly prescribing the characteristics of the acceptable Identification Documents, OEs subject to CySEC supervision may not diverge therefrom and shall not accept documents that do not meet as a minimum the characteristics set our in the definition of the '*Identification Document*' under the amended CySEC AMLD.

[179] P.17 para.31 of the EBA Guidelines.

[180] P.19 para.40 of the EBA Guidelines.

[181] P.18f. para.37 of the EBA Guidelines.

[182] See also P.40f of the EBA Guidelines: '*Where credit and financial institutions accept alternative documentation for the purposes of financial inclusion, it is expected that it is done in a way which balances the need for financial inclusion with the need to mitigate ML/TF risk. Explicitly excluding such customers from remote onboarding, as per respondent suggestions, would be contrary to the goal of financial inclusion'.*

3.5.3.6.4. CONTENT OF POLICIES AND PROCEDURES IN RELATION TO RECTIFICATION OF WEAKNESSES

3.5.3.6.4.1. Where errors or weaknesses are identified[183] or risks have materialised[184], OEs should in ascending order of intensity:

i. Review affected relationships and assess, following remedial action, the future of the transaction in question as well as of the business relationship as a whole and consider possible suspicious transaction reporting (STR).[185] The EBA Guidelines[186] provide further guidance in case where weaknesses are identified or a risk has materialised. More specifically: '*These measures [remedial measures in case where a risk has materialised or a weakness has been identified] should include at least:*

a) a review of all affected business relationships, to assess whether sufficient initial CDD has been applied by the credit and financial institutions in order to comply with article 13 (1), (a), (b) and (c) of the AMLD[187]. Credit and financial institutions should prioritise those business relationships that carry the highest ML/TF risk;

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

a. subject to additional due diligence measures;

b. subject to limitations, such as limits on the volume of transaction, where permitted under national law, until such time as a review has taken place;

c. terminated;

d. reported to the [Financial Intelligence Unit] FIU; and

e. reclassified into a different risk category'.

[183] P.9 para.17c of the ESAs Opinion.

[184] P.15 para.19 of the EBA Guidelines.

[185] P.9 para.17c of the ESAs Opinion.

[186] P.15 para.19 of the EBA Guidelines.

[187] Corresponding to Section 61(1)(a)-(c) of the AML/CFT Law.

As per the EBA Guidelines[188], the said remedial measures must be embedded in the OE's policies and procedures regarding the onboarding of NFTF Customers by means of RCOS. This requirement also applies where fully automated remote customer onboarding solutions are used which are highly dependent on automated algorithms, without or with little human intervention[189].

ii. Re-evaluate, in case of serious weaknesses/actual issues, confidence in the RCOS with regard to OE's NFTF Customer/business relationship risks, any improvements to the RCOS, including even the (dis)continuation of the use of the RCOS itself[190].

3.5.3.6.5. POLICIES AND PROCEDURES IN RELATION TO DATA-RETENTION AND RECORD-KEEPING REQUIREMENTS

3.5.3.6.5.1. Furthermore, controls should be in place for the purpose of compliance with data-retention and record-keeping requirements, irrespectively of the RCOS (to be) used, by means of relevant monitoring and testing respectively[191]. The EBA Guidelines[192] further substantiate the said requirement, namely that '*The documents and information collected during the remote identification process, which are required to be retained in accordance with Article 40(1) point (a) of Directive (EU) 2015/849[193], should be time-stamped[194] and stored securely by the credit and financial institution. The content of stored records, including images, videos, sound and data should be available in a readable format and allow for ex-post verifications*'.

[188] P.15 para.19 of the EBA Guidelines.

[189] P.15 para.21 of the EBA Guidelines.

[190] P.9 para.17d of the ESAs Opinion.

[191] P.9 para. 19e of the ESAs Opinion.

[192] P.16 para.26 of the EBA Guidelines.

[193] Corresponding to Article 68(1)(a) of the AML/CFT Law.

[194] P.38 of the EBA Guidelines: '*The GDPR applies, therefore the guidelines do not specify retention periods. In the same vein, references to 'ex-post verifications' do not prevent the encryption of data, in line with Article 32 of the GPDR Regulation. The EBA agrees to specify that the obligation to store and time stamp the identification proofs lies with the credit and financial institution*.'

3.5.3.6.6. POLICIES AND PROCEDURES IN RELATION TO ICT AND SECURITY RISKS

3.5.3.6.6.1. In addition, high standards of data and IT security have to be observed by OEs, in particular in cases of outsourcing of data storage. This generic requirement under the ESAs Opinion[195] is further substantiated in the EBA Guidelines[196]:
'Credit and financial institutions should identify and manage their ICT and security risks related to the use of the remote customer onboarding process, including where credit and financial institutions rely on third parties or where the service is outsourced, including to group entities.
In addition to complying with requirements set out in the EBA Guidelines on ICT and security risk management where applicable, credit and financial institutions should use secure communication channels to interact with the customer during the remote customer onboarding process. The remote customer onboarding solution should use secure protocols and cryptographic algorithms according to the industry best practices to safeguard the confidentiality, authenticity, and integrity of the exchanged data, where applicable.
Credit and financial institutions should provide a secure access point for starting the remote customer onboarding process based on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 or for website authentication as referred to in Article 3(39) of that Regulation. The customer should also be informed about the applicable security measures that should be taken to ensure a secure use of the system.
Where a multi-purpose device is used to perform the remote customer onboarding process, a secure environment should be used for the execution of the software code on the customer's side, where applicable. Additional security measures should be implemented to ensure the security and reliance of the software code and the collected data, according to the security risk assessment as laid down in EBA Guidelines on ICT and security risk management'.

3.5.3.6.7. POLICIES AND PROCEDURES IN RELATION TO THE INTEGRITY AND CAPABILITY OF THE OE'S STAFF

3.5.3.6.7.1. Ensuring the integrity of the OE's staff, including the staff of an external RCOS provider where this applies, by means of relevant controls and its abilities to use

[195] P.9f. para.17f of the ESAs Opinion.

[196] P.22f. paras. 50-53 of the EBA Guidelines.

the RCOS in question by provision of regular and specialised operational and compliance training is an additional requirement.[197] The EBA Guidelines[198] require the documentation of the induction and regular training programs to ensure staff awareness and up-to-date knowledge of the functioning of the RCOS, of the associated risks and of the remote customer onboarding policies and procedures aimed at mitigating such risks. The EBA Guidelines[199] provide further guidance as regards integrity: '*…Where possible, credit and financial institutions should also provide random assignments to the employee responsible for the remote verification process to avoid collusion between the customer and the responsible employee*'.

3.5.3.6.7.2. Finally, further guidance on the induction and training of OEs' staff with regard to RCOS, is being provided in Annex IV to this PS, as many of the requirements laid down in the initial practical guidance[200] with regard to dynamic selfie and/or video-call have now become generally applicable to the introduction of any RCOS.

3.5.3.6.8. POLICIES AND PROCEDURES IN RELATION TO THE ADEQUACY AND QUALITY OF NFTF CUSTOMER CDD MEASURES

3.5.3.6.8.1. OEs should ensure in their policies and procedures that:

i. There are controls in place ensuring that a business relationship with an NFTF Customer commences only once all initial NFTF CDD measures commensurate with the ML/TF risk have been applied under the OE's exclusive responsibility, irrespective of whether the solution in question is internally developed or externally purchased. [201] The EBA Guidelines cross-refer to section 4.38 of the EBA Risk Factors Guidelines that OEs: '*should, for the purposes of these guidelines, have completed the relevant actions before the end of the remote customer onboarding process.*[202] For the

[197] P.10 para.17i of the ESAs Opinion in conjunction with P.20 para.43 of the EBA Guidelines.

[198] P.12 para.9e of the EBA Guidelines.

[199] P.20 para.43 of the EBA Guidelines.

[200] Section 3.3 of CP-02-2020.

[201] P.11 para.18a of the ESAs Opinion and EBA Guidelines, P.12 para.9d and p.34 thereof.

[202] P.17 para. 32 of the EBA Guidelines.

avoidance of doubt, NFTF Customer CDD measures also include OEs assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship under section 61(1) point (c) of the AML/CFT Law, which falls within the scope of initial CDD[203]. Where RCOS are used to assess the ML/TF risks associated with a business relationship, it has to be ensured by OEs that all available data and information are considered as reliable and are used in this process. To this end, OEs 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 NFTF Customer's account profile and web login activity, government or third-party-issued watch-lists, online news and publications, social media, and public databases[204];

ii. There are quality controls in place as regards NFTF Customer CDD procedures, data and information used or collected, irrespective of whether the solution in question is internally developed or externally purchased or whether a case of outsourcing is in place. The ESAs Opinion[205] provides examples of such quality controls, which may include quality assurance testing, ongoing compliance monitoring, reviews by the IA function and regular discussion and reviews at senior management level as well as escalation management. The EBA Guidelines[206] provide for additional examples of quality controls in respect of the RCOS in question, including but not limited to automated critical alerts and notifications, regular automated quality reports, sample testing and manual reviews. The quality control requirement under the EBA Guidelines also applies where fully automated remote customer onboarding solutions are used which are highly dependent on automated algorithms, without or with little human intervention[207];

[203] P.39 of the EBA Guidelines: '*The risk factors guidelines clarify that initial customer due diligence includes a specific step to identify the purpose and intended nature of the business relationship, in line with Article 13 of the AMLD. The guidelines were amended to make this clear*'.

[204] P.15 para.19e of the ESAs Opinion.

[205] P.11f. para.18b of the ESAs Opinion.

[206] P.15 para.20 of the EBA Guidelines.

[207] P.15 para.21 of the EBA Guidelines.

iii. In case of externally purchased, i.e. not in-house developed, solutions or of outsourcing, relevant on-site visits should also take place as a means of quality control.[208] The EBA Guidelines[209] further substantiate the quality controls requirement in case of outsourcing, considering on-site visits just a part of a broader quality enhancement procedure:

'Where credit and financial institutions outsource all or parts of the remote customer on-boarding process to an outsourced service provider, as referred to in Article 29 of Directive (EU) 2015/849[210], credit and financial institutions should apply in addition to guidelines 2.20 to 2.21 and 4.32 to 4.37 of the EBA Risk Factors Guidelines and in addition to the EBA Guidelines on Outsourcing where applicable, before and during the business relationship with the outsourced service provider the following measures, the extent of which should be adjusted on a risk-sensitive basis:

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

b) carry out assessments to ensure that the outsourced service provider is sufficiently equipped and able to perform the remote customer on-boarding process. Assessments may include, but are not limited to, the assessment of staff training, technology fitness and data governance at the outsourced service provider;

c) ensure that the outsourced service provider informs the credit and financial institutions of any proposed changes of the remote customer on-boarding process or any modification made to the solution provided by the outsourced service provider.

[208] P.11f. para.18b of the ESAs Opinion.

[209] P.22 paras 48-49 of the EBA Guidelines.

[210] Corresponding to section 67(5) of the AML/CFT Law.

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

a) only necessary customer's data is collected and stored in line with a clearly defined retention period;
b) access to the data is strictly limited and registered;
c) appropriate security measures are implemented to ensure that the stored data is protected.'

3.5.3.6.9. EXCURSE: REPRODUCTIONS AND '*HYBRID SAFEGUARDS*'

3.5.3.6.9.1. **Excurse Reproductions**

As regards the specific issue of OEs accepting reproductions[211] of an original document without examining the original document, the EBA Guidelines[212] require OEs to take steps to ascertain that the reproduction is reliable and establish at least the following:

i. Whether the reproduction includes security features embedded in the original document and whether the specifications of the original document that are being reproduced are valid and acceptable, in particular, type, size of characters and structure of the document, by comparing them with official databases, **such as** PRADO[213];

ii. Whether personal data has been altered or otherwise tampered with or, where applicable, whether the picture of the customer embedded in the document was not replaced;

iii. Whether the integrity of the algorithm used to generate the unique identification number of the original document, in case the official identification document has been issued with machine-readable zone (MRZ);

[211] The term '*reproductions*' has replaced the terms '*paper copies, photos or scans of paper-based documents…*', since some respondents requested during the consultation on the EBA Guidelines to add the case when credit and financial institutions accept videos of physical identity document or indicated that using copies, photos or scans of identity documents during remote onboarding process is not in line with most national requirements, prevailing practise and increases the risk of fraud and ID theft (P.39 of the EBA Guidelines).

[212] P.18 para.33 of the EBA Guidelines.

[213] PRADO thus not being exclusively eligible, unlike the position taken in CP-02-2020.

iv. Whether the provided reproduction of the identification document is of sufficient quality and definition so as to ensure that relevant information is unambiguous; and

v. That the provided reproduction of the identification document has not been displayed on a screen based on a photograph or scan of the original identification document.

3.5.3.6.9.2. **Excurse '*hybrid safeguards*'**

In addition to the guidance, which aims at enhancing the reliability of the RCOS to be used by focusing on innovative technology-related aspects, the EBA Guidelines[214] provide additional guidance to enhance the reliability of an RCOS by laying down '*hybrid*' safeguards, consisting of both innovative but also conventional safeguards: '*where commensurate with the ML/TF risk associated with the business relationship, credit and financial institutions should use of one or more of the following controls or a similar measure to increase the reliability of the verification process. These controls or measures may include, but are not limited to, the following: a) the first payment is drawn on an account in the sole or joint name of the customer with an EEA-regulated credit or financial institution or in a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849; b) send a randomly generated passcode to the customer to confirm the presence during the remote verification process. The passcode should be a single-use and time-limited code; c) capture biometric data to compare them with data collected through other independent and reliable sources; d) telephone contacts with the customer; e) direct mailing (both electronic and postal) to the customer'*.

3.6. NEXT STEPS

3.6.1. OEs wishing to make use of RCOS should abide by the applicable rules, as substantiated by means of guidance provided herein. The amended CySEC AMLD comes into application on the date of its publication in the Official Gazette of the Republic, except for the new rules on the use of RCOS that come into application on 1 December 2024 to ensure a smooth transition thereto.

[214] P.20f. para.44 of the EBA Guidelines.

ANNEX I

CySEC AMENDING AML DIRECTIVE

ΟΔΗΓΙΑ ΤΟΥ 2024 ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΚΕΦΑΛΑΙΑΓΟΡΑΣ ΓΙΑ ΤΗΝ ΠΑΡΕΜΠΟΔΙΣΗ ΚΑΙ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΗΣ ΝΟΜΙΜΟΠΟΙΗΣΗΣ ΕΣΟΔΩΝ ΑΠΟ ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ (ΤΡΟΠΟΠΟΙΗΤΙΚΗ)

(Τροποποιητική της Οδηγίας για την
Παρεμπόδιση και Καταπολέμηση της Νομιμοποίησης Εσόδων

από Παράνομες Δραστηριότητες)

N. 188(I)/2007
N. 58(I)/2010
N. 80(I)/2012
N. 192(I)/2012
N. 101(I)/2013
N. 184(I)/2014
N. 18(I)/2016
N. 13(I)/2018
N. 158(I)/2018
N. 81(I)/2019
N. 58(I)/2016
ΔΙΟΡΘ. Ε.Ε. Παρ. I(I), Αρ. 4564
13(I)/2018
158(I)/2018
81(I)/2019
13(I)/2021
ΔΙΟΡΘ. Ε.Ε. Παρ.I(I), Αρ. 4816
22(I)/2021
N. 98(I)/2023.

N. 58(I)/2016.

Η Επιτροπή Κεφαλαιαγοράς Κύπρου, ασκώντας τις εξουσίες που της παρέχονται δυνάμει του εδαφίου (4) του άρθρου 59 του περί της Παρεμπόδισης και Καταπολέμησης της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες Νόμου 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 2024 για την Παρεμπόδιση και Καταπολέμηση της Νομιμοποίησης Εσοδών από Παράνομες Δραστηριότητες (Τροποποιητική) και θα διαβάζεται μαζί με την Οδηγία για την Παρεμπόδιση και Καταπολέμηση της Νομιμοποίησης Εσοδών από Παράνομες Δραστηριότητες και την Οδηγία του 2020 για την Παρεμπόδιση και Καταπολέμηση της Νομιμοποίησης Εσοδών από Παράνομες Δραστηριότητες (που στο εξής θα αναφέρονται ως η «βασική Οδηγία») και η βασική Οδηγία και η παρούσα Οδηγία θα αναφέρονται μαζί ως οι Οδηγίες για την Παρεμπόδιση και Καταπολέμηση της Νομιμοποίησης Εσοδών από Παράνομες Δραστηριότητες του 2019 έως 2024.

Τροποποίηση της παραγράφου 2 της βασικής Οδηγίας.

2. Η παράγραφος 2 της βασικής Οδηγίας τροποποιείται με την προσθήκη, στην κατάλληλη αλφαβητική σειρά, του ακόλουθου νέου όρου και του ορισμού του:

««έγγραφο ταυτοποίησης» σημαίνει επίσημο έγγραφο που εκδίδεται από κυβέρνηση κράτους μέλους της Ευρωπαϊκής Ένωσης ή τρίτης χώρας και στο οποίο αναγράφεται το πλήρες όνομα και η ημερομηνία γέννησης του φυσικού προσώπου και φέρει τη φωτογραφία αυτού.».

Τροποποίηση της παραγράφου 11 της βασικής Οδηγίας.

3. Η παράγραφος 11 της βασικής Οδηγίας τροποποιείται με την αντικατάσταση αυτής με την ακόλουθη νέα παράγραφο 11:

«Μηνιαία Προληπτική Κατάσταση

11. Ο λειτουργός συμμόρφωσης ετοιμάζει και υποβάλλει στην Επιτροπή, κατά τα οριζόμενα στην παράγραφο 9(1)(ιζ), σε μηνιαία βάση, τη Μηνιαία Προληπτική Κατάσταση, στην οποία περιλαμβάνονται στοιχεία για τις συνολικές καταθέσεις που δέχεται η Υπόχρεη Οντότητα σε μετρητά, για τις Εσωτερικές Εκθέσεις Αναφοράς Υποψιών και για τις Εκθέσεις του λειτουργού συμμόρφωσης προς τη ΜΟΚΑΣ, κατά τα οριζόμενα στις παραγράφους 9(1)(ε) και 9(1)(ζ), αντίστοιχα. Η Μηνιαία Προληπτική Κατάσταση υποβάλλεται συμπληρωμένη στην Επιτροπή εντός δεκαπέντε (15) ημερών από το τέλος κάθε μήνα. Η συμπλήρωση αυτής αποτελεί ευκαιρία για την Υπόχρεη Οντότητα κατ' αρχή να αξιολογήσει και ακολούθως να ενισχύσει τα συστήματα ελέγχου και παρακολούθησης των εργασιών του με σκοπό την έγκαιρη επισήμανση συναλλαγών σε μετρητά που ενδεχομένως να είναι ασυνήθη ή/και που δυνατόν να συνεπάγονται αυξημένο κίνδυνο ξεπλύματος παράνομου χρήματος ή χρηματοδότησης της τρομοκρατίας.».

Τροποποίηση της παραγράφου 33 της βασικής Οδηγίας.

4. Η παράγραφος 33 της βασικής Οδηγίας τροποποιείται με τη διαγραφή του στοιχείου i, του σημείου α), της υποπαραγράφου (2) και την αναρίθμηση των υφιστάμενων στοιχείων ii., iii., iv. και v. του σημείου α), της υποπαραγράφου (2), σε στοιχεία i., ii., iii. και iv., αντίστοιχα.

Τροποποίηση του Πρώτου Παραρτήματος της βασικής Οδηγίας.

5. Το Πρώτο Παράρτημα της βασικής Οδηγίας τροποποιείται με την αντικατάσταση του εντύπου με τίτλο «Εσωτερική Έκθεση Αναφοράς Υποψιών», με το ακόλουθο νέο έντυπο με τίτλο «Εσωτερική Έκθεση Αναφοράς Υποψιών»:

ΕΣΩΤΕΡΙΚΗ ΕΚΘΕΣΗ ΑΝΑΦΟΡΑΣ ΥΠΟΨΙΩΝ ΓΙΑ ΞΕΠΛΥΜΑ
ΠΑΡΑΝΟΜΟΥ ΧΡΗΜΑΤΟΣ ΚΑΙ ΧΡΗΜΑΤΟΔΟΤΗΣΗΣ ΤΗΣ ΤΡΟΜΟΚΡΑΤΙΑΣ

ΣΤΟΙΧΕΙΑ ΠΛΗΡΟΦΟΡΙΟΔΟΤΗ

Όνομα: ..... Τηλέφωνο:. .....
Τμήμα:..... Τηλεομοιότυπο:.....
Τίτλος/θέση: .....

ΣΤΟΙΧΕΙΑ ΠΕΛΑΤΗ

Όνομα: ....
Διεύθυνση: ....
..... Ημερομηνία Γέννησης:.....
Τηλέφωνο:..... Επάγγελμα/
Τηλεομοιότυπο:..... Στοιχεία Εργοδότη:.....
.....

Αρ. Εγγράφου Ταυτοποίησης:..... Εθνικότητα: .....
Άλλα στοιχεία ταυτότητας:.....

ΠΛΗΡΟΦΟΡΙΕΣ/ΥΠΟΨΙΕΣ

Σύντομη περιγραφή γεγονότων/συναλλαγής:..... .....
....
Λόγοι υποψίας:..... .....
....
Υπογραφή πληροφοριοδότη Ημερομηνία

..... ……

ΓΙΑ ΧΡΗΣΗ ΑΠΟ ΤΟΝ ΛΕΙΤΟΥΡΓΟ ΣΥΜΜΟΡΦΩΣΗΣ

Ημερ. Λήψης: .....Ώρα λήψης:.....Αναφ.....
Ενημέρωση ΜΟΚΑΣ: Ναι/Όχι.....Ημερ ενημέρωσης:.....Αναφ .....

Τροποποίηση του Τρίτου Παραρτήματος της βασικής Οδηγίας.

6. Το Τρίτο Παράρτημα της βασικής Οδηγίας τροποποιείται με τη διαγραφή της παραγράφου 24 στο Μέρος Α. αυτού και την αντικατάσταση της με την ακόλουθη νέα παράγραφο 24:

«24. Εγείρονται ανεξήγητες αντιφάσεις κατά τη διάρκεια της εξακρίβωσης της ταυτότητας του πελάτη (π.χ. προηγούμενη ή υφιστάμενη χώρα διαμονής, χώρας έκδοσης του εγγράφου ταυτοποίησης, χώρες που επισκέφθηκε σύμφωνα με το διαβατήριο, έγγραφα που έχουν εκδοθεί για επιβεβαίωση του ονόματος, της διεύθυνσης και της ημερομηνίας γεννήσεως κτλ.).».

Τροποποίηση του Τέταρτου Παραρτήματος της βασικής Οδηγίας.

7. Το Τέταρτο Παράρτημα της βασικής Οδηγίας τροποποιείται:

(α) με την αντικατάσταση της υποπαραγράφου ii. της παραγράφου 2 αυτού, με την ακόλουθη νέα υποπαράγραφο ii.:

«ii. Λήψη απευθείας βεβαίωσης της σύναψης επιχειρηματικής σχέσης μέσω άμεσης προσωπικής επαφής, του πραγματικού ονόματος, διεύθυνσης και αριθμού εγγράφου ταυτοποίησης του πελάτη, από πιστωτικό ίδρυμα ή χρηματοπιστωτικό ίδρυμα με το οποίο συνεργάζεται ο πελάτης, που λειτουργεί σε χώρα του Ευρωπαϊκού Οικονομικού Χώρου ή σε τρίτη χώρα, η οποία προσδιορίζεται από την Υπόχρεη Οντότητα ως χαμηλότερου κινδύνου λαμβάνοντας υπόψη τις Κοινές Κατευθυντήριες Γραμμές και το Παράρτημα ΙΙ του Νόμου (ή πιστού αντίγραφου της βεβαίωσης).»·

(β) με την αντικατάσταση της υποπαραγράφου iv. της παραγράφου 2 αυτού, με την ακόλουθη νέα υποπαράγραφο iv.:

«iv. Χρήση μίας ηλεκτρονικής μεθόδου ή συνδυασμού περισσότερων αυτών για την εξ' αποστάσεως εξακρίβωση και επαλήθευση της ταυτότητας πελατών, στη βάση της εκτίμησης, αξιολόγησης και διαχείρισης κινδύνου νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας.

Η υπόχρεη οντότητα οφείλει να ενημερώσει την Επιτροπή για την ηλεκτρονική μέθοδο για την εξ' αποστάσεως εξακρίβωση και επαλήθευση της ταυτότητας πελατών που θα χρησιμοποιήσει, πριν τη χρήση αυτής.».

Τροποποίηση του Πέμπτου Παραρτήματος της βασικής Οδηγίας

8. Το Πέμπτο Παράρτημα της βασικής Οδηγίας τροποποιείται:

(α) με την αντικατάσταση του σημείου i., της υποπαραγράφου (α), της παραγράφου 1 αυτού, με το ακόλουθο νέο σημείο i.:

«i. πραγματικό όνομα ή/και ονόματα που χρησιμοποιούνται, βάσει του εγγράφου ταυτοποίησης,» ·

(β) με την αντικατάσταση του σημείου ii., της υποπαραγράφου (γ), της παραγράφου 1 αυτού, με το ακόλουθο νέο σημείο ii.:

«ii. προσκόμιση ενός πρόσφατου (μέχρι 6 μήνες) λογαριασμού τηλεφώνου, ηλεκτρικού ρεύματος, δημοτικών φόρων, ή κατάστασης τραπεζικού λογαριασμού, ή άλλου παρόμοιου, με τα προαναφερθέντα, εγγράφου.»·

(γ) με την αντικατάσταση των υποπαραγράφων (β) και (γ) της παραγράφου 2 αυτού, με τις ακόλουθες νέες υποπαραγράφους (β) και (γ):

«(β) Για τους πελάτες που διαμένουν εκτός Δημοκρατίας, ζητείται έγγραφο ταυτοποίησης, και κρατούνται αντίγραφα των σελίδων που περιέχουν τις σχετικές πληροφορίες, τα οποία πιστοποιούνται ως πιστά αντίγραφα (true copies). Περαιτέρω, συστήνεται όπως, εκεί που εγείρεται οποιαδήποτε αμφιβολία για την ταυτότητα ενός προσώπου επιδιώκεται η εξακρίβωσή της από την Πρεσβεία ή το Προξενείο της χώρας έκδοσής τους στη Δημοκρατία ή από αξιόπιστα χρηματοπιστωτικά ιδρύματα που βρίσκονται στη χώρα καταγωγής του πελάτη.

(γ) Οι πιο πάνω πληροφορίες είναι επίσης αναγκαίες, πέραν του σκοπού της παρεμπόδισης ξεπλύματος παράνομου χρήματος και χρηματοδότησης της τρομοκρατίας, και για σκοπούς εφαρμογής των οικονομικών κυρώσεων που επιβάλλονται εναντίον διαφόρων προσώπων από τα Ηνωμένα Έθνη και την Ευρωπαϊκή Ένωση. Συνεπώς, στα αντίγραφα των στοιχείων που λαμβάνονται, από την Υπόχρεη Οντότητα, φαίνονται πάντοτε ο αριθμός, η ημερομηνία και η χώρα έκδοσης του εγγράφου ταυτοποίησης καθώς και η ημερομηνία γέννησης του πελάτη, ούτως ώστε η Υπόχρεη Οντότητα να είναι σε θέση να εξακριβώνει κατά

πόσον ο πελάτης βρίσκεται σε κατάλογο προσώπων που υπόκεινται σε κυρώσεις που έχουν εκδοθεί από τα Ηνωμένα Έθνη ή την Ευρωπαϊκή Ένωση βάσει σχετικού ψηφίσματος του Συμβουλίου Ασφάλειας των Ηνωμένων Εθνών και Κανονισμού ή Κοινής Θέσης του Συμβουλίου της Ευρωπαϊκής Ένωσης αντίστοιχα.».

Έναρξη ισχύος της παρούσας Οδηγίας.

9. (1) Με την επιφύλαξη της υποπαραγράφου (2), η παρούσα Οδηγία τίθεται σε ισχύ από την ημερομηνία δημοσίευσής της στην Επίσημη Εφημερίδα της Δημοκρατίας.

(2) Οι διατάξεις της παραγράφου 7(β) τίθενται σε ισχύ την 1η Δεκεμβρίου 2024.

ANNEX II
SUMMARY OF THE RESPONSES RECEIVED TO THE QUESTIONS IN CP-02-2020

Question 1

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

SUMMARY OF FEEDBACK RECEIVED

All respondents agreed in respect of Question 1 with the incorporation of RCOS for the purposes of conducting CDD as to the NFTF Identification process.
One of the respondents proposed to extend the application of RCOS also to cases of onboarding NFTF Customers being legal entities, including their management and ownership (the initial policy approach was limited to NFTF Customers being natural persons). Respondents further proposed that RCOS should also apply to the verification of an NFTF Customer's address, in addition to the verification of such Customer's identity. The reason for proposing this was that an enhanced level of address authentication (over and above address authentication through the check of a common utility bill) could secure higher and advanced levels of overall verification.

Furthermore, one of the respondents suggested that the use of Regtech Technology should extend to all AML compliance matters and not be limited to the CDD process. Another respondent would support CySEC's proposal provided that an RCOS would incorporate independent verification means and avoid reliance on self-verification means (the so-called '***trusted anchors***' according to the respondent).

CySEC'S RESPONSE:

The scope of application of RCOS for NFTF identification purposes has been expanded to also encompass the remote identification and verification of legal entities, including their ownership and management. Further information on the implementation of digital onboarding of legal entities can be found under Section 3 of this PS.

As regards the suggested extension of the material scope of application of this PS to also encompass RCOS for an NFTF Customer's address verification, the current regulatory focus on a European basis is, as the content of the EBA Guidelines also clearly demonstrates, limited to a natural person's or a legal entity's identification and identity verification. The use of RCOS to verify a NFTF Customer's proof of address, without collecting accepted

documents as proof of address can be examined in a future point in time**.** However, we have removed the requirement under the Fifth Appendix of the CySEC AMLD, to collect only original documents as proof of address, to facilitate the confirmation of address and/or document authenticity through RCOS, as per the amended Fourth Appendix of the aforesaid CYSEC AMLD. In addition to this, such RCOS can be used for addressing the geographical risk in the context of the Risk Assessment as further laid down in this PS.

Question 2

Do you agree that the use of such RCOS 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?

SUMMARY OF FEEDBACK RECEIVED

The vast majority of the respondents agreed in respect of Question 2 that the use of RCOS should be subject to the Risk Assessment, based on which it has to be ascertained that the ML/TF risks are being addressed on a reasonable, consistent and demonstrable basis. Within the said context, two of the respondents additionally suggested the following:

i. The Risk Assessment should also consider the *FATF report (September 2020): Virtual Assets – Red Flag Indicators of Money Laundering and Terrorist Financing*, which complements the FATF Guidance for a Risk Based Approach to Virtual Assets Service Providers (June 2019).[215]

ii. The results of the Risk Assessment should be integrated into the risk scoring framework that OEs apply during the onboarding process of an NFTF Customer. This would, as per the respondents, allow sufficient flexibility to address a diverse range of circumstances and provide a framework whereby OEs would be in a position to produce demonstrable evidence of the assessment process.

iii. Two respondents expressed opposite views in respect of the requirement for a Risk Assessment, namely:

   a. Instead of requiring OEs to carry out the Risk Assessment, CySEC should indicate minimum requirements which should be in place prior to OEs engaging with a provider offering an RCOS. OEs would in such a case assess as part of their AML/CFT processes how each method would fit the overall risk profile of each NFTF Customer. Thus, the Risk Assessment might not be necessary, so

[215] Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (fatf-gafi.org)

the suggestion, as long as the OE would have processes clearly defining the reasoning behind the requirements to be applied per risk category.

b. CySEC should subject the providers of an RCOS to regulation and supervision.

iv. Lastly, one respondent suggested that in cases where an NFTF Customer is of low risk, the use of any automated onboarding method is sufficient, whereas, in cases where an NFTF Customer is of high risk the use of a video-based technology must instead be preferred.

CySEC'S RESPONSE

By means of a preliminary clarification, CASPs are additionally subject to specific AML/CFT rules, which are laid down in the AML/CFT Law, the CySEC Directive on the Register of Crypto-asset Service Providers and in CySEC's PS-01-2021 on the registration and operations of CASPs. Those specific rules relate to the idiosyncrasies arising out of the nature of crypto-assets (e.g. pseudonymity, anonymity enhanced tokens etc.) and apply over and above to the AML/CFT rules that apply horizontally to all OEs. However, the scope of this PS relates to the AML/CFT rules that are horizontally applicable to all OEs.

As regards the proposal for integration of the Risk Assessment into the risk scoring framework that OEs apply during the onboarding process of NFTF Customers, it must be borne in mind that the Risk Assessment prior to the introduction of an RCOS and determining a specific NFTF Customer's risk scoring (as of low/medium/high risk) are two distinct procedures. Besides, it is also required that OEs incorporate the onboarding of NFTF Customers by means of RCOS in their NFTF Customer CDD policies and procedures, so that the said exercise cannot be merged with any other AML/CFT compliance-related exercise. A specific NFTF Customer's risk scoring, is one of several factors to be considered when determining the additional measures to be taken by the OEs.

As to the (non) obligation for a Risk Assessment, OEs are required to carry out the Risk Assessment before OEs incorporate an RCOS in their NFTF Identification process as a dedicated mandatory exercise; provided OEs want to make use of RCOS for NFTF Customer onboarding purposes, so that is up to the OEs to choose. The said exercise has to take place in accordance with the AML/CFT Law's '*risk-based*' approach, as further substantiated herein, and is aligned with common EU standards. This approach, apart from being mandatory, allows OEs to be in the best position to evaluate their own business-and NFTF Customer-related risk(s) and opt for the most suitable means for mitigating those risks.

As regards the suggestion for CySEC to indicate minimum requirements prior to an OE engaging with an RCOS provider instead of being required to devise a Risk Assessment, the EBA Guidelines[216], being a common EU-wide standard, make it clear that '*The ultimate responsibility under AMLD lies with the credit and financial institution and could not be transferred to a third party. This aspect goes beyond the scope of these Guidelines and would be too prescriptive with insufficient legal bases. Although EBA understands that in some countries, remote onboarding solutions must be authorised, it is not the case everywhere. The Guidelines should be relevant for all addressees. There is no official list of relevant standards and technical specifications and these Guidelines do not intend to give prescriptive indications as to how credit and financial institutions are expected to draw up their policies and procedures'.* Within the same context of ideas, the ESAs Opinion[217] also clarifies that: '…*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*…' Besides, the providers of RCOS are not offering or intending to offer any financial service falling under CySEC's supervision, but providing a RegTech tool assisting OEs in the compliant provision of their regulated services and activities, so that it is out of regulatory context to subject them to authorisation and supervision.

As regards the suggestion that in cases where an NFTF Customer is of low risk the use of an automated onboarding method is sufficient, whereas, in cases where an NFTF Customer is of high risk the use of a video based technology must instead be preferred, this is an issue that has to be assessed by each OE itself in light of the overall Risk-Assessment prior to the introduction of the RCOS. CySEC will be reviewing the implementation of the digital onboarding rules in the context of exercising its supervisory responsibilities.

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 RCOS), into consideration and the content of CySEC's Circular C399

SUMMARY OF FEEDBACK RECEIVED

[216] Page 34 of the EBA Guidelines.

[217] P.19 para.25 of the ESAs Opinion.

All respondents agreed in respect of Question 3 with this proposal in principle but had different views on the exact form of the Risk Assessment.
One differentiated view suggested that the risk factors listed in the ESAs Opinion should be stated as guidelines rather than as requirements, in order to preserve a risk-based approach instead of a '*tick the box'* exercise, so the differentiated view.
Another respondent stated that the proper assessment of the applicability of an RCOS requires technical expertise which is not easy to be found within the organisation of an OE, so that, CySEC should consider, as an alternative, to provide OEs with the following:

i. a standard template checklist of the tests that OEs are required to carry out when assessing proposed RCOS; or

ii. a list of providers, evaluated and approved by CySEC.

Another respondent suggested that CySEC should substantiate what constitutes a '*reliable and independent*' digital ID system, along with the establishment of assurance frameworks and technical standards, through expertise of qualified professionals in this field. This way, so the suggestion, the features and parameters embedded in each digital ID system will not be upon the discretion of each OE. Similarly, another respondent expressed the view that, as per the FATF Guidance (paragraphs 141-149)[218], if the RCOS has been assessed as having a reliable level of assurance by an NCA, then a Risk Assessment by the OE should not be required. The same respondent also mentioned that OEs should be allowed to rely for parts of the Risk Assessment on information obtained from the RCOS provider; provided that such an assessment is either verified or conducted by the RCOS provider and/or by an independent third party. This would, as per the said respondent, be quite useful especially for the assessment of complex areas that require expertise such as biometrics technology and algorithmic models.
At last, a respondent suggested that the Risk Assessment needs to be tested by OEs on a statistical data basis. They argued that a Risk Assessment tested on a statistical data basis, would provide OEs with reliable results, especially for the mitigation of the risk factor of impersonation fraud, which is of particular concern and consideration during the process of an NFTF Customer identification.

[218] Guidance on Digital ID (fatf-gafi.org)

CySEC'S RESPONSE:

As regards the suggestion for CySEC to devise template checklists of tests and approval of RCOS providers, we would like to refer to our answer to Question 2 point 4. The same with regard to the suggestion for CySEC establishing assurance frameworks and technical standards.

The FATF Guidance and the recommendation provide for the case where governments have assessed the level of assurance of RCOS and have authorised specific tools. However CySEC has adopted the approach of the EBA Guidelines[219], which clearly lay down that: '*The guidelines are expected to provide significant benefit to the institutions as they will be able to have a common standard to follow and to make sure that the AML risk is minimized by following the recommended steps…When considering whether to adopt a new remote customer onboarding solution, credit and financial institutions should carry out a pre-implementation assessment of the remote customer onboarding solution…The ultimate responsibility under AMLD lies with the credit and financial institution and could not be transferred to a third party. This aspect goes beyond the scope of these Guidelines and would be too prescriptive with insufficient legal bases. Although EBA understands that in some countries, remote onboarding solutions must be authorised, it is not the case everywhere. The Guidelines should be relevant for all addressees. There is no official list of relevant standards and technical specifications and these Guidelines do not intend to give prescriptive indications as to how credit and financial institutions are expected to draw up their policies and procedures'.* In addition to the aforesaid, CySEC has no statutory mandate as regards the authorisation and/or approval of individual solutions. To this end CySEC does not intend to ex-ante assess and authorise individual solutions but to supervise OEs and enforce the legislation were deemed necessary. Nevertheless, the FATF Guidance contains useful technical information, in order for OEs to assess the level of assurance of the RCOS in question.

As regards the argument that the introduction of an RCOS requires technical expertise going beyond an OE's relevant expertise, it merits clarification that the use of an RCOS is not compulsory and/or should not be considered as a '*must*'; conversely, OEs must consider whether they are indeed in a position to recourse to an RCOS as an additional/alternative tool for the facilitation of their NFTF Identification process. If OEs consider the use of an RCOS for NFTF Identification purposes as a burdensome procedure given the cost, time, resources and effort required, the use of or co-existence with conventional methods always remains possible. Nevertheless, it merits reiteration that the FATF Guidance contains useful

[219] P.3, P.13 para.13 and P.34 of the EBA Guidelines.

technical information, in order for OEs to assess the level of assurance of the RCOS in question.

As to the possibility of placing of reliance, the PS lays down cases, where reliance on eIDAS compliant solutions can be placed. However, such reliance is not tantamount to an exemption from governance requirements, as explained in this PS in reliance to the EBA Guidelines.

As to the issue of the risk factors to be considered for the purposes of the Risk Assessment, the purpose is to consider all risks that are applicable in the present case, namely the onboarding of NFTF Customers. Thus, it is not a matter of discretion to consider the said risk factors, but a matter of sound AML/CFT risk management by taking into consideration all relevant risks[220].

Finally, OEs may incorporate the testing of the Risk Assessment on a statistical data basis in their relevant policies, as they are required to include therein tests to assess fraud risks including impersonation fraud risks[221]; provided the OE considers, under its ultimate responsibility, this test appropriate in view of the ML/TF risk faced.

Question 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 OE to be able to use an RCOS, provided that such limits will be set by the OEs in the content of their Risk Assessment per risk category and be further reviewed on a case-by-case basis?

SUMMARY OF FEEDBACK RECEIVED

The vast majority of the respondents agreed with CySEC's intention in respect of Question 4, to refrain from setting up explicit limits concerning the level of assets to be deposited and the size of transactions to be carried out in respect of NFTF Customers onboarded pursuant to the use of an RCOS.

Certain respondents agreeing with the threshold idea in general, suggested the following three alternative methods instead:

[220] See also P.25 of the EBA Guidelines: '*Option 2 is preferred, as it ensures that the credit and financial institutions oversee the remote customer onboarding solution(s) during its lifecycle, while all areas of potential risks, including shortcomings in governance, are covered*.'

[221] P.13 para.14(d) of the EBA Guidelines.

i. **First alternative method**: Applying different levels of verifications based on the NFTF Customer's projected level of transactions/business/assets to be deposited:
   1st level: ID/Passport+selfie requirements, verification of email and mobile phone via a code;
   2nd level: proof of address, utility bills etc;
   3rd level: enhanced documentation (financial statements etc).

ii. **Second alternative method:** CySEC to consider, alternatively or cumulatively, following two (sub)methods to monitor both the systemic and the OEs' specific risk resulting from the use of RCOS for NFTF Identification purposes:
   a. The monthly AML returns to be amended to include a section whereby the OEs will disclose on a monthly basis the absolute number of investments that have been approved pursuant to the use of RCOS;
   b. The quarterly statistics returns to be amended to include a section where the number of investments that have been approved pursuant to the use of RCOS are quantified as per the following:
      a) The number of investors;
      b) The total investment amounts; and
      c) The geographical distributions.

iii. **Third Alternative Method:** An OE should be able to use RCOS across all NFTF Customers (irrespective of the Customer's size of assets and level of transactions). Consideration of the risk mitigation measures must take place before the choice of an RCOS, as appropriate and necessary on each case depending on the RCOS to be used. The results of the Risk Assessment on such method including the level of assurance it provides as well as the controls and safeguards it involves must be also considered by the OEs.

Additionally, one of the respondents who agreed with CySEC's overall approach on setting thresholds, suggested that CySEC could provide more detailed guidelines (including examples) to assist OEs in imposing their own limits in relation to the level of assets to be deposited and the size of transactions involved.

The respondents who disagreed with the CySEC's approach expressed the view that CySEC should set a specific limit on the level of assets to be deposited and the size of transactions, thus, ensuring that a universal treatment will be applied to NFTF Customers posing the same levels of risks.

CySEC'S RESPONSE:

CySEC setting horizontal explicit limits would contravene the provisions of Section 58A and 66(2A) of the AML/CFT Law as well as paragraph 12 of CySEC AMLD, under which OEs must apply appropriate measures and procedures on a risk-based approach, so as to focus their efforts in those areas where the risk of AML/CFT appears to be higher. In addition to the aforesaid setting a horizontal limit might give the wrong impression that any transaction up to that limit could be automatically considered as low risk, whereas the amounts involved is only one of the several factors that need to be taken into consideration.

Considering the above context, the EBA Guidelines as a common EU standard in the context of AML/CFT and the stakeholder views expressed, consenting, concurring but also dissenting ones, the asset limit up to which an RCOS may be used will not be set by CySEC, but OEs are required to apply (additional) varying due diligence measures, including thresholds, which the OE will internally determine depending on the ML/TF risks associated therewith. This is also the approach taken by the EBA Guidelines[222], namely that: '*credit and financial institutions should set out in their procedures and processes remedial measures where a risk has materialised, or where errors have been identified that have an impact on the efficiency and effectiveness of the general remote customer onboarding solution. These measures should include at least… an assessment of whether an affected business relationships should be… subject to limitations, such as limits on the volume of transaction, where permitted under national law, until such time as a review has taken place*;' CySEC will review those policies, procedures, measures and thresholds in the context of its supervisory work.

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 RCOS 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 RCOS?

SUMMARY OF FEEDBACK RECEIVED

Most of the respondents agreed with CySEC's proposition in respect of Question 5, however guidance was requested on the meaning and definition of the terms 'reasonable, consistent

[222] P.15 para. 19(b) of the EBA Guidelines.

and demonstrable' basis, since, lack of defining such terms would leave room to a subjective interpretation and hence potential inconsistencies in their application by OEs.

One of the respondents who disagreed with CySEC's approach, suggested that the attestation should not be the decisive factor as to whether an OE can use an RCOS; rather, CySEC's consent, so the said suggestion, should be granted upon the detailed examination of the Risk Assessment submitted by an OE to CySEC. According to their view a non-exhaustive list of such criteria could include, the following:

i. whether or not an OE has appropriate technical capabilities to implement and oversee the development of the RCOS;

ii. whether the RCOS is proportionate to the ML/TF risks that the OE is exposed to;

iii. whether or not the senior management, the Regulatory Compliance/AML Compliance Officer and Internal Audit function of the OE have appropriate understanding of the RCOS;

iv. whether an OE has an appropriate contingency plan in place to ensure continuity of services in case of malfunction or interruption of the RCOS; and

v. whether the OE has put in place a training plan for its employees in order to keep them up-to-date with the on-going developments of the technology and the use of RCOS, as well as the ML/TF risks involved due to the risk of technological abuse.

In addition to the above, other respondents who also disagreed with the CySEC's approach alleged that the proposed attestation does not change or enhance the legal obligations and responsibilities of the OEs, but instead, it creates additional procedural requirements and burdens. They considered it inappropriate to submit such an attestation, as an RCOS is not a product but a procedure forming part of their overall regulatory obligation in ensuring compliance with the provisions and requirements of the AML/CFT regulatory framework. Moreover, they stated that the use of any RCOS is part of the enhanced due diligence process already followed by OEs, meriting therefore sole approval by their BoD.

CySEC'S RESPONSE

As regards the suggestion of having the Risk Assessment approved by CySEC, CySEC would like to reiterate that: *'The ultimate responsibility under AMLD lies with the credit and financial institution and could not be transferred to a third party. This aspect goes beyond*

the scope of these Guidelines and would be too prescriptive with insufficient legal bases. Although EBA understands that in some countries, remote onboarding solutions must be authorised, it is not the case everywhere. The Guidelines should be relevant for all addressees. There is no official list of relevant standards and technical specifications and these Guidelines do not intend to give prescriptive indications as to how credit and financial institutions are expected to draw up their policies and procedures'. [223] Within the same context of ideas, the ESAs Opinion also clarifies that: *'…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…'.*[224] In addition, as to the non-exhaustive list of criteria proposed by a respondent for assessment by CySEC, such criteria have already been considered throughout this PS.

CySEC taking into account the legal basis underpinning the issuance of the CySEC AMLD, has amended its approach on requiring a standardized attestation. OEs are now required to submit a notification of informative character, which in any case does not amount to licensing or other form of approval by CySEC of the RCOS to be used.

Question 6:

Do you agree with the additional considerations and Practical Guidance?

SUMMARY OF FEEDBACK RECEIVED

All the respondents except four, agreed with the additional considerations and the Practical Guidance issued by CySEC. The respondents who agreed with CySEC's approach have provided the following further views on the above-mentioned considerations and Practical Guidance:

i. That today's technology allows for a direct video stream to be fraudulently manipulated in real time by Artificial Intelligence ('***AI***'), while the video is lively being conducted. In other words, respondents claim that AI may even replace the face of a person while he/she is lively (i.e. in real time) speaking on the camera, the so-called '*spoofing*'. Accordingly, any system that would be used for the purposes of NFTF Identification would need to bear an inherent robust authentication software that prevents other streams during the CDD process.

[223] Page 34 of the EBA Guidelines.

[224] P.19 para.25 of the ESAs Opinion.

ii. CySEC should develop a common understanding of what constitutes '*properly trained employee*'.

iii. Paragraph 3.3.3.4(ii) of the CP-02-2020 should explicitly mention that the employee performing the video-based verification should be trained to determine that the verification process is not vitiated by phishing, social engineering attack[225] or carried out with the NFTF Customer being under duress.

iv. Recurring to PRADO should be done with caution, since PRADO provides information as to how an original document looks like and what kind of information is indicative of such a document, but not as to whether the identification document in question is indeed a real one.

One of the respondents who expressed disagreement with CySEC's guidance in respect of paragraph 3.3.3.1 (vi)[226] of the CP-02-2020, raised the issue that there are cases where the NFTF Identification process by means of RCOS may be undergone by an NFTF Customer through using different devices. Especially, it has been asserted that, in the case of the online brokers business, a potential NFTF Customer has the option to complete the application and submit the required identification documents at a later stage. Consequently, strict application of the '*single device*' guidance would mean that all incomplete applications would be automatically deleted and that the NFTF Customer would need each time to start the application process from the beginning.

The second respondent who disagreed with CySEC's approach mentioned in respect of paragraphs 3.3.1.3[227] and 3.3.3.2[228] of the CP-02-2020 that CySEC should also allow the use of other documents issued by governmental agencies as proof of identity, such as national identities for foreign NFTF Customers and driving licenses. Furthermore, it has been

[225]Social engineering is a risk that has been rapidly grown in the past months, especially because of COVID-19.

[226]Ensure that the electronic NFTF Identification procedure takes, at all times, place through the use of one and only device.

[227]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.

[228]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.

suggested that paragraphs 1 and 2 of the Fifth Appendix of the CySEC AMLD should be amended to allow for the use of alternative identification documents, as this will offer more flexibility to OEs, without increasing the risk of the business relationship. In addition, this would ensure a level playing field between brokers established in other MS, where national identities and driving licenses are acceptable documents for identity verification. As an example it was mentioned that other EU Member States and third countries allow the use of a driving license. Also, apart from the photo, the other safety features, including signature and MRZ should not be mandatory and should be opted-in by the OEs based on the inherent risk of the NFTF Customer, as this requirement would otherwise be very restrictive.

Moreover, concerning paragraph 3.3.3.3 (i) (a) of the CP-02-2020 and the requirement to take photos from different angles, a third respondent disagreed and mentioned that there are other technologies that can identify, if the image in question is that of a live person, as for instance, to include a short video to demonstrate liveness.

A fourth respondent who disagreed with CySEC's approach mentioned that explicit reference to the utilization of video-conference should be avoided as this suggests, that video-conference is the only preferred option and only adherence thereto would ensure compliance.

Lastly, one of the respondents requested clarifications concerning paragraphs 3.3.3.1 (ii) and 3.3.3.1(vi) of the CP-02-2020. Particularly, for paragraph 3.3.3.1(ii) of the CP-02-2020, clarification has been requested as to which are the circumstances to which the sentence, '*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*', refers to. Concerning paragraph 3.3.3.1 (vi) of the CP-02-2020, clarification was requested as to what the term '*one and only device*' means, to what kind of device this refers to and what is the purpose of the check. The same respondent stated in respect of paragraph 3.3.3.3 (iii) of the CP-02-2020[229] that, depending on the provider, it may be possible for an NFTF Customer to also receive a unique link which he/she can input in the web browser for the purposes of performing the biometric selfie/video, not only a unique number. Thus, the relevant requirement should encompass all possible electronic means not only mobile phones.

[229]Require the natural person in question to register the unique code number the person receives by email or SMS in its mobile phone.

CySEC'S RESPONSE

By means of preliminary clarification, the use of a video conference is considered to be a mainstream and generally accepted method but neither the exclusive nor the preferred one from CySEC's point of view, as CySEC's approach is technologically neutral and future-proof, so that this PS neither encourages nor otherwise prioritises the use of a specific RCOS over any other. The practical guidance provided in relation herewith acknowledges an existing market reality but does not prescribe the use of any specific RCOS.
As to the need for OEs to devise safeguards against innovative forms of impersonation fraud risk, relevant guidance is provided in the EBA Guidelines[230] and this PS[231].

As to the meaning of the term '***properly trained employee***', it needs indeed to be further specified. For the purposes of digital onboarding of NFTF Customers by means of an RCOS, a '*properly trained employee*' is to be understood as an employee of the OE or a person offering services to an OE under the provisions of sections 67(1)[232] or 67(5)[233] (as the case may be) of the AML/CFT Law, who has:

i. Received a professional training on the RCOS to be used by the OE, as well as to how fraudulent practices such as '*deep faking*', '*impersonation*', '*phishing'*, '*spoofing*' etc. that are not akin to a specific technology can apply in the context of the RCOS in question; and
ii. Participated in the production or the application of/produced (as the case may be) the OE's rules and procedures as regards the introduction and operation of the RCOS in question, including but not limited to the section on the risks arising from the use of such RCOS; for example, weaknesses of the specific underlying technology of the RCOS, which can be used for fraudulent purposes; and
iii. Is sufficiently trained to anticipate and prevent the intentional or deliberate use of deception techniques related to remote verification, and to detect and react in case of their occurrence; and

[230] P.17 para.28 of the EBA Guidelines: '*They* [OEs] *should apply controls to address associated risks, including risks associated with automatic capture of data such as the obfuscation of the location of the customer's device spoofed Internet Protocol (IP) addresses or services such as Virtual Private Networks (VPNs)'*.

[231] See section 3.5.3.2 of this PS on the assessment of geographical risk.

[232]Article 67(1) of the AML/CFT Law – Performance by Third Parties.

[233] Article 67(5) of the AML/CFT Law provides for an outsourcing or agency relationship, where, based on a contractual agreement, the outsourcing provider or agent is to be regarded as part of the OE.

iv. Been designated by the OE as a person responsible for participating in and/or supervising the process of onboarding the NFTF Customer by means of the RCOS in question.

As regards the issue of specific training to be received by the staff of an OE, in order to address the risks of phishing, social engineering and coercion, this is already addressed in this PS in reliance to the EBA Guidelines[234] and the ESAs Opinion[235].

As to the reliance to be placed on PRADO, it has to be borne in mind that PRADO is an official database but not the only one, whereas use thereof shall be made in cases where specific safeguards apply and in any case not as a sole safeguard[236].

As regards the issue of an OE ensuring that the electronic NFTF Identification procedure by means of RCOS takes, at all times, place through the use of one and only device, this view was, following the feedback received by stakeholders, measured against the objectives pursued by CP-02-2020. Bearing in mind that:

i. The objective of both CP-02-2020 and of this PS is to facilitate the onboarding of NFTF Customers by means of RCOS, under observance of the risk-based approach; and
ii. That any risks arising from the use of different devices will have to be addressed and assessed in the relevant Risk Assessment,
iii. CySEC believes that, the use of different devices for performing the verification of identification documents, shall not be excluded as an option and has amended its initial approach on this.

[234] P.20 para.42b) and 43 of the EBA Guidelines: *'…foresee the participation of an employee that has sufficient knowledge of the applicable AML/CFT regulation and security aspects of remote verification and who is sufficiently trained to anticipate and prevent the intentional or deliberate use of deception techniques related to remote verification, and to detect and react in case of their occurrence… . Where possible, credit and financial institutions should use remote customer onboarding solutions that include randomness in the sequence of actions to be performed by the customer for verification purposes to guard against risks such as the use of synthetic identities or coercion.*'

[235] P.17 para. 20b of the ESAs Opinion: '*firms should have strong controls in place to identify possible coercion…*'.

[236] P.18 para. 33a) of the EBA Guidelines: '*If the reproduction includes security features embedded in the original document and if the specifications of the original document that are being reproduced are valid and acceptable, in particular, type, size of characters and structure of the document, by comparing them with official databases, such as PRADO'*.

As regards the issue of communicating a unique number for the biometric solutions, this may be now done not only by means of SMS (mobile phone)[237] but also thorough other personalised channels.

As to the liveness issue, it is clarified that following publication of the EBA Guidelines that liveness detection is mandatory in all cases of unattended solutions.[238] This is without prejudice to OEs incorporating similar practices in cases of attended solutions as well. As to liveness detection practices themselves, no limitation is placed on the practices that can be used, provided these satisfy the supervisory expectations laid down herein[239].

Lastly, as to the suggestion that CySEC should also allow the use of other documents issued by governmental agencies as proof of identity, such as national identities for foreign NFTF Customers and driving licenses, it should be noted that CySEC has amended its approach, by introducing a new term under the amended CySEC AMLD, namely that of '*identification document*'. The new term has been broadly defined and it captures any '*official document issued by the government of a Member State of the European Union or of a third country and which states the full name and the date of birth of the natural person and bears the photograph of that natural person*'.

Question 7:

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

[237] P. 20 Para. 44 of the EBA Guidelines: *'In addition to the above, and where commensurate with the ML/TF risk associated with the business relationship, credit and financial institutions should use of one or more of the following controls or a similar measure to increase the reliability of the verification process. These controls or measures may include, but are not limited to, the following...b) send a randomly generated passcode to the customer to confirm the presence during the remote verification process. The passcode should be a single-use and time-limited code*'.

[238] P.28 of the EBA Guidelines: '*The preferred option is mandatory liveness detection in all unattended situations only (Option 2). These situations are highly dependent on the technology with little or no direct human intervention. In this context, EBA considered that the reliability of the verification process increases significantly when the process resorts to liveness detection*.'.

[239] P.19 para.41(c) of the EBA Guidelines: '[OEs]should…*perform liveness detection verifications, which may include procedures where a specific action from the customer is required to verify that he/she is present in the communication session or which can be based on the analysis of the received data and does not require a specific action by the customer*…'.

SUMMARY OF FEEDBACK RECEIVED

The following points have been suggested by stakeholders in respect of Question 7:

i. Customer to read loudly a set of four numbers that randomly appear on his/her screen during the liveness verification.

ii. CySEC should consider the creation of a standardized methodology/template to be used in order to assist OEs in performing a Risk Assessment in relation to the use of RCOS, and that such a methodology/template be circulated to all OEs.

iii. OEs will be required to receive CySEC's approval following the review of their submitted attestations, before initiating onboarding NFTF Customers using the means of RCOS.

iv. CySEC to request yearly reports, from the OEs' Internal Auditors on the compliance of each entity with the applicable provisions, to be submitted to CySEC.

v. With the aim of ensuring a robust document verification process, not only a photo of the document should be submitted, but also a short clip of when the document was captured. This would allow to successfully detect these security features and would also provide more confidence that the document has not been tampered with.

vi. RCOS can also be applied in the field of proof of address as well.

vii. Restate the FATF Guidance and ESAs Opinion on RCOS in the form of practical and comprehensive Guidance by CySEC to avoid the ambiguity caused by the current state of affairs.[240]

viii. Additional safeguards be incorporated requiring OEs to have the RCOS included within the scope of the Quality Assurance reviews undertaken. Quality Assurance reviews will ensure that an OE follows the additional safeguards and Practical Guidance, as well as its internal policies and procedures regarding the use of an IM. The RCOS should also be included within the scope of Internal Audits.

[240]It was submitted that, the current state of affairs in which an OE, in carrying out the Risk Assessment required by section 58A of the AML/CFT Law and Part IV of the CySEC AMLD, requires OEs to consider multiple sources of guidance, might lead to ambiguity as to what the Risk Assessment should entail and what the assessment's outcome should be.

ix. CySEC to provide more clarity regarding the results of the Risk Assessment. What happens if for example in one of the four areas the results are Low and in the remaining three areas Substantial or High? Can an OE still use the solution on a risk-based approach?

CySEC'S RESPONSE

By means of preliminary clarification, the scope of this PS is limited to initial CDD for NFTF Customers, in accordance with section 61(1)(a)-(c) of the AML/CFT Law, hence limited to the identification of an NFTF Customer and the verification of his/her/its identity. Notwithstanding the aforesaid, constructive proposals, such as the need to also verify a person's (real) address, has been considered, resulting in CySEC removing the obligation to collect only original documents for the purpose of verifying a client's address, enabling thus the verification to be performed through additionally applying an RCOS, where the OEs do not collect the original documents (e.g. where they accept a photo of the document taken in real time). In addition to the aforesaid, such RCOS can be used for addressing the geographical risks in the context of the Risk Assessment, as further laid down in this PS. As to the suggestion for CySEC to gather, compile and summarise the various relevant documents issued by standard-setting bodies, CySEC has provided compiled information as regards the content of various regulatory sources, consulted thereupon, assessed the feedback received and finally issued this PS. Nevertheless, it is reminded that it is the OEs' obligation to have built and retained sufficient in-house expertise prior to using RCOS for onboarding NFTF Customers[241]. Such expertise may not be built based on summarised material but requires navigating, studying and mastering the relevant material, which is an obligation of the OE.

As regards various practices suggested, such as the NFTF Customer being a natural person or a natural person acting on behalf of or associated with an NFTF Customer being a legal entity, to loudly read a set of four numbers that appear randomly on his/her screen during the liveness verification process; or suggestions aiming at ensuring a robust document verification, these are indeed constructive proposals. Such proposed practices could be considered together with or weighted against (as the case may be) other sound practices by OEs, when devising the NFTF CDD policies and procedures, depending on their specific circumstances and the findings of their Risk Assessment.

[241] See also P.7 para.16 of the ESAs Opinion: '*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…*'

As regards proposals requiring CySEC to devise relevant methodologies or even templates or proceed to approve specific RCOS, we would like to reiterate our response in point 4 of Question 2. Furthermore, it needs to be reiterated, that OEs have to carry out the Risk Assessment, as explain in Section 3 of this PS, prior to using RCOS and notify the intention of such use towards CySEC in advance. However, such notification has an informative character and does not amount to licensing or other form of approval by CySEC of the RCOS to be used. The said notification is not constitutive or declaratory but rather purely informative (i.e. it is not at any point the decisive factor of whether an OE may use one or more RCOS and as well as the use of RCOS by OEs is not mandatory either).

As to the suggestion that OEs submit yearly internal audit reports to CySEC in respect of the RCOS used for NFTF Identification purposes or that CySEC should require that RCOS be included in the Quality Assurance reviews to be undertaken, this is already a requirement under paragraphs 6, 9(1)(d) and 10(4)(b) of the CySEC AMLD and quality assurance is expected to be covered in the annual reports of the Internal Auditors and of the Compliance Officers.

As regards the issue of gravity to be assigned to the factors to be included in the Risk Assessment, it is reiterated that the introduction of RCOS for NFTF Customers is an optional regime for OEs, with the final decision as to the adoption of an RCOS for NTFT Identification purposes resting with the OEs themselves. An exhaustive response on how to treat a poor topical or sectoral (as the case may be) scoring, cannot be provided and the ability of an OE to properly assess the impact of each and every topical issue is a prerequisite for an OE to use RCOS on a risk basis. OEs that do not have the capacity to properly and prudently undertake a risk assessment on the subject matter, are strongly discouraged from relying on RCOS to onboard customers.

Question 8:

Do you have any other comments?

SUMMARY OF FEEDBACK RECEIVED

The following views were expressed in respect of Question 8:

i. Consideration and enforcement of the eIDAS Regulation.

ii. Care should be taken that the risk-based approach which forms the foundation of the AML/CFT regulatory framework is not undermined by the introduction of processes that could lead to a '*tick the box*' compliance, which may complicate the supervisory function of CySEC.

iii. CySEC may consider the framework, conditions and measures that other jurisdictions have put in place for the use of RCOS by OEs. It is important that Cyprus does not impose higher conditions and requirements for the use of RCOS than in other jurisdictions.

iv. CySEC may consider issuing a regulatory framework (e.g. a Directive) that will define what is accepted in matters of KYC documentation through these RCOS.

v. CySEC may consider implementing an electronic registry which will electronically verify the address of natural persons.

vi. CySEC may consider implementing a repository of KYC information where individual documents and information is kept. Each individual submits his/her KYC documentation and holds his/her own credentials. OEs will have access to this repository and when a potential NFTF Customer wishes to be onboarded by them, he/she will be logging in this repository through his/her own credentials, giving access to his/her documentation to OEs.

vii. Consideration by CySEC to establish a database where lost/stolen/compromised official identity documents will be published/available, thus assisting OEs to rapidly identify compromised documents/credentials. Additionally, it is essential for OEs to have access to reliable and transparent data on corporate entities so that the ultimate beneficial owner(s) and director(s) can be identified and verified.

viii. OEs intending to make use of RCOS must also assess the risks arising from a possible failure of the relevant provider due to bankruptcy or lack of funding or irreparable system failure or any other possibility of the RCOS becoming obsolete, including potential loss of data in such a scenario.

ix. Selfie images do not improve reliability as such images may have been easily undergone tampering or spoofing.

x. CySEC should consider assessing and endorsing third party RCOS. RCOS endorsed and approved by CySEC should not require a Risk Assessment by OEs.

xi. Lastly, one of the respondents requested clarification as to how the suitability of the employee using an RCOS can be ascertained and established.

CySEC'S RESPONSE

Starting from the requested clarification as to how the suitability of the employee using an RCOS can be ascertained and established, we would like to refer to the concept of the '*properly trained employee*' as explained in the answer to Question 6 above herein.

As regards the consideration of eIDAS-compliant solutions, such consideration takes place extensively in this PS, in the EBA Guidelines and, to a lesser extent, in the ESAs Opinion, which stakeholders are urged to consult.

As to the concern that the '*risk-based approach*' might turn into a '*tick the box exercise*', it is reminded that this PS relies on common EU standards and it is evident throughout this PS and the documents that it refers to that a risk based approach must be well rounded and substantiated. Therefore a '*tick the box*' approach would not qualify as a '*risk-based approach*'

As to considering various national regulatory practices, such insights and exchanges of views take place in the context of the work undertaken by collective regulatory (standard-setting) bodies in which CySEC participates. Nevertheless, it has to be emphatically clarified that the regulatory approach(es) and requirements laid down in the CP-02-2020 and this PS are primarily determined by the business models and the ML/TF risks faced by OEs under CySEC's supervision and the need to ensure compliance with applicable EU rules and standards. It should also be reiterated that CySEC's supervisory mandate relates to entities providing financial services and not to providers of technological solutions, even if for RegTech purposes, which do not constitute a regulated activity.

As to the issue of eligible KYC documentation in relation to the use of RCOS, this was out of the scope of the consultation RCOS[242].

[242] See also P.14 para.18 of the EBA Guidelines: '*Credit and financial institutions should …complement their policies and procedures described in paragraph 9 with a description of at least: a) the steps they will take to be satisfied of the ongoing quality, completeness, accuracy and adequacy of data collected during the remote customer onboarding process, which should be commensurate to the ML/TF risks to which the credit and financial institution is exposed to'*.

As to the suggestion that OEs intending to make use of RCOS must also assess the risks arising from a possible failure of the relevant provider due to bankruptcy or lack of funding, this is addressed in the ESAs Opinion[243] and in this PS[244].

As regards the suggestions in relation to electronic registries, databases and repositories, the difference between regulatory action on the one hand and legislative action on the other hand needs to be always borne in mind. Such decisions involve constitutional and general data protection related considerations and assessments, which go beyond CySEC's (financial services-related) supervisory mandate and have hence to take place at legislative and not at regulatory level.

As to the suggestion to combine selfie photos with other measures, such issues are already addressed in Fourth Appendix, paragraph 2 '*Non Face to Face Customers'* of the CySEC AMLD and in the EBA Guidelines, which provide for a combination of innovative and legacy safeguard, also mentioned as '*hybrid safeguards'* in this PS. For instance, Para. 44 of the EBA Guidelines states the following: '*In addition to the above* [i.e. the techniques to match customer identity during the verification process as per paras 41-43 of the EBA Guidelines]*, and where commensurate with the ML/TF risk associated with the business relationship, credit and financial institutions should use of one or more of the following controls or a similar measure to increase the reliability of the verification process. These controls or measures may include, but are not limited to, the following: a) the first payment is drawn on an account in the sole or joint name of the customer with an EEA-regulated credit or financial institution or in a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849; b) send a randomly generated passcode to the customer to confirm the presence during the remote verification process. The passcode should be a single-use and time-limited code; c) capture biometric data to compare them with data collected through other independent and reliable sources; d) telephone contacts with the customer; e) direct mailing (both electronic and postal) to the customer.*'. Such measures should in any case be also compatible with code of conduct.

[243] P.10 para. 17j: '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'.

[244] See para. 3.5.3.5 of this PS.

ANNEX III
NOTIFICATION FORM

NOTIFICATION BY OBLIGED ENTITIES IN RELATION TO THE INTRODUCTION OF REMOTE CUSTOMER ONBOARDING SOLUTIONS AS PER PARAGRAPH 2(iv) OF ANNEX FOUR OF CySEC DIRECTIVE FOR THE PREVENTION AND SUPPRESSION OF MONEY LAUNDERING AND TERRORIST FINANCING

A.(1) NOTIFICATION

In accordance with Paragraph 2(iv) of Annex Four of CySEC Directive for the Prevention and Suppression of Money Laundering and Terrorism Financing we notify 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	☐
Crowdfunding Services Provider	☐

Crypto Asset Services Provider	☐
Other [please specify]	☐

2. **[insert the name of the Obliged Entity]** intends to use **Remote Customer Onboarding Solutions** referred to in Table 2.1:

Table 2.1

Complete this table by indicating the Remote Customer Onboarding Solutions introduced.

	Remote Customer Onboarding Solutions
1.	
2.	
3.	

A.(2) Persons signing this notification:

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]**	

This Notification Form must signed by all persons referred to in column 1 of Table 3 directly above and must be submitted via email at aml@cysec.gov.cy**.**

ANNEX IV
REVISED ADDITIONAL CONSIDERATIONS AND PRACTICAL GUIDANCE

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

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 practices we have encountered in the context of the activities of the CySEC Innovation Hub, we would like to provide herewith some additional practical guidance on their implementation.

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 OE; and,
ii. An automated process initiated by the individual taking a dynamic real-time selfie.

1.3. Within the context of the aforesaid methods, the acceptable documents for the identification of natural persons are those that meet the definition of the CySEC AMLD. Based on the EBA Guidelines, OEs may use biometric data for the purposes of NFTF Customer onboarding purposes, but not exclusively. It is provided that biometric data may be used to the extent permissible under GDPR[245].

1.4. OEs shall ensure that the electronic NFTF identification process remains reliable, including by making use, of multiple and alternative sources of information. Under the EBA Guidelines[246], this is a generally applicable requirement for the purpose of the risk assessment, so that it has to be considered in the context of any RCOS.

[245] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[246] P.40 of the EBA Guidelines: '*The proposal to include the checking of data against reliable external sources is already included.*' and more emphatically p.13 para.14 of the EBA Guidelines: '*Credit and financial institutions should set out the scope, steps and record keeping requirements of the pre-implementation assessment in their policies and procedures, which should include at least: a) an assessment of the adequacy of the solution regarding the completeness and accuracy of the data and documents to be collected, as well as of the reliability and independence of the sources of information it uses;*'

1.5. OEs should also be in a position to shield themselves against spoofing[247] and deep-fake synthetic media[248]. Under the EBA Guidelines[249] controls against spoofing is a generally applicable requirement for the purpose of the risk assessment, so that it has to be considered in the context of any RCOS. As regards controls against the synthetic media[250] issue, this is also considered to be a generally applicable requirement under the ESAs Opinion[251], so that it has to be considered in the context of any RCOS.

1.6. OEs 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.

It Is noted that the issue of impersonation fraud is already addressed in the ESAs Opinion[252] as a generally applicable risk factor that has to be considered for the purposes of the risk assessment under the delivery channel risk, so that it has to be considered in the context of any RCOS.

[247] Malicious parties impersonating another device or user.

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

[249] P.17 para.28 of the EBA Guidelines: *'Credit and financial institutions should put in place and maintain appropriate mechanisms to ensure that the information they capture automatically in line with paragraph 27 is reliable. They should apply controls to address associated risks, including risks associated with automatic capture of data such as the obfuscation of the location of the customer's device spoofed Internet Protocol (IP) addresses or services such as Virtual Private Networks (VPNs).'*

[250] P.14 para.19b of the ESAs Opinion.

[251] P.13 para.19 of the ESAs Opinion: *'…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.'*

[252] P.16 para.20a of the ESAs Opinion: '*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'.*

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

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 OE's Board[253]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, the management of the relevant risks and compliance with the guidance laid down in this PS, the EBA Guidelines and the ESAs Opinion;[254]

ii. A procedure for activating additional measures and safeguards, in cases where the OE is not satisfied with regard the validity of an identification document or with the conclusion about a natural person's identity;[255]

[253] P.13 para.12 of the EBA Guidelines explicitly introduces governance arrangements, so that the approval of the BoD is required prior to the introduction of any RCOS as a generally applicable requirement: '*The management body of the credit and financial institution should approve remote customer onboarding policies and procedures and oversee their correct implementation*'

[254] P. 12 para.9 of the EBA Guidelines set out requirements for detailed policies and procedures, whereas P.12 para.10 thereof explicitly requires that the said policies and procedures ensure overall compliance in the context of any RCOS, hence as a generally applicable requirements: '*The policies and procedures, when implemented, should enable credit and financial institutions to ensure compliance with the provisions in Section 4.2 to 4.7 of these Guidelines.*'

[255] This is a generally applicable requirement in the context of any RCOS under both P.8 para.17a of the ESAs Opinion: '*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*.' as well as under P.15 para.19b of the EBA Guidelines: '*Credit and financial institutions should set out in their procedures and processes remedial measures where a risk has materialised, or where errors have been identified that have an impact on the efficiency and effectiveness of the general remote customer onboarding solution. These measures should include at least:… an assessment of whether an affected business relationships should be: a. subject to additional due diligence measures*;' and P.19 para.39 of the EBA Guidelines: '*Where the remote customer onboarding solution involves the use of biometric data to verify the customer's identity, credit and financial institutions should make sure that the biometric data is sufficiently unique to be unequivocally linked to a single natural person. Credit and financial institutions should use strong and reliable algorithms to verify the match between the biometric data provided on the submitted identity document and the customer being onboarded. In situations where the solution does not provide the required level of confidence, additional controls should be applied'.*

ii. A procedure for recording and monitoring any divergences/discrepancies between the electronic NFTF identification procedure as it has been approved by the BoD and its actual implementation; and

iii. 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[256].

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

3.1. As to the practical implementation of the electronic NFTF identification procedure as such, OEs must irrespective of the specific method applied:

i. Apply safe communication techniques between the OE and the person in question, in order to ensure the integrity and confidentiality of the information transmitted;[257]

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;[258]

[256] Without prejudice to OEs determining their own specific criteria, relevant criteria are also provided under P.16 para.24c of the EBA Guidelines in the context of any RCOS: '*Credit and financial institutions should ensure that:… the identification process does not continue if technical shortcomings or unexpected connection interruptions are detected*.' The same under P.19 para.40 of the EBA Guidelines: '*In situations where the evidence provided is of insufficient quality resulting in ambiguity or uncertainty so that the performance of remote checks is affected, the individual remote customer onboarding process should be interrupted and restarted or redirected to a face-to face verification*.'

[257] Under P.22f. para.51 of the EBA Guidelines this a generally applicable requirement in the context of any RCOS: '*where applicable, credit and financial institutions should use secure communication channels to interact with the customer during the remote customer onboarding process. The remote customer onboarding solution should use secure protocols and cryptographic algorithms according to the industry best practices to safeguard the confidentiality, authenticity, and integrity of the exchanged data, where applicable'.*

[258] While the requirement for a '*real time identification*' continues to apply, the '*no-interruption control*' is addressed as a generally applicable requirement, in the context of P.16 para.24c of the EBA Guidelines: '*the identification process does not continue if technical shortcomings or unexpected connection interruptions are detected.*' As to the real-time data transmission issue, P.19 para.41b of the EBA Guidelines limits this requirement in the context of unattended solutions only: '*Where credit and financial institutions use unattended remote onboarding solutions, in which the customer does not interact with an employee to perform the verification process, they should… ensure that any photograph(s) or video is taken at the time the customer is performing the verification process;*'

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 OEs in question) are not subject to spoofing or deep-fake media attacks. It is noted that under the EBA Guidelines[259] controls against spoofing is a generally applicable requirement for the purpose of the risk assessment, so that it has to be considered in the context of any RCOS. As to the issue of impersonation fraud, this is already addressed in the ESAs Opinion[260] as a generally applicable risk factor that has to be considered for the purposes of the risk assessment under the delivery channel risk, so that it has to be considered in the context of any RCOS.

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, OEs 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

[259] P.17 para.28 of the EBA Guidelines: '*Credit and financial institutions should put in place and maintain appropriate mechanisms to ensure that the information they capture automatically in line with paragraph 27 is reliable. They should apply controls to address associated risks, including risks associated with automatic capture of data such as the obfuscation of the location of the customer's device spoofed Internet Protocol (IP) addresses or services such as Virtual Private Networks (VPNs).*'

[260] P.16 para.20a of the ESAs Opinion: '*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'.*

during the electronic NFTF identification procedure and it should be kept available for supervisory Audit[261].

3.2. OEs shall in the course of the electronic NFTF identification procedure and irrespective 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, 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. Require the natural person in question to register a unique code number the person receives through personalised channels (e.g. by means of SMS in its mobile phone). It is noted that under the EBA Guidelines[262], this is addressed as a generally applicable requirement in the context of introducing any RCOS, including thus the one in question, and has to be reflected in any case in the OE's policies and procedures.

[261] This requirement is considered to be a substantiation of the generally applicable requirement under P.9 para.17e of the ESAs Opinion: *'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.'* as well as under P.16 para.26 and P.38 of the EBA Guidelines: *'The documents and information collected during the remote identification process, which are required to be retained in accordance with Article 40(1) point (a) of Directive (EU) 2015/849, should be time-stamped and stored securely by the credit and financial institution. The content of stored records, including images, videos, sound and data should be available in a readable format and allow for ex-post verifications…The GDPR applies, therefore the guidelines do not specify retention periods. In the same vein, references to 'ex-post verifications' do not prevent the encryption of data, in line with Article 32 of the GPDR Regulation. The EBA agrees to specify that the obligation to store and time stamp the identification proofs lies with the credit and financial institution.'.*

[262] Per P.20 para.44(b) of the EBA Guidelines '*credit and financial institutions should use of one or more of the following controls or a similar measure to increase the reliability of the verification process. These controls or measures may include, but are not limited to…send a randomly generated passcode to the customer to confirm the presence during the remote verification process. The passcode should be a single-use and time-limited code*'.

3.3. In case where OEs 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 their finger in front of the safety features of their identification document or move their hand in front of their face;

ii. Have in place controls in order to identify any suspicious behaviour of the natural person in question, which may imply that this person is under the influence of narcotic or other substances or compulsion[263] or eventually under a mental or physical disorder.

4. THE OE's STAFF PARTICIPATING IN ELECTRONIC NFTF IDENTIFICATION PROCEDURE

4.1. OEs shall ensure that the electronic NFTF identification procedure is carried out by properly trained employees, which has been vested with necessary resources and specialized technical means for the seamless and safe implementation of the procedure in question.

4.2. The training of the relevant employees 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, as well as of the identification of unusual or suspicious transactions and the transmission of relevant reports, in accordance with the OE's internal procedures. The required training, which has to be provided over and above of the general AML/CFT training required under the applicable framework,

[263] Controls against coercions are considered to be a generally applicable requirement in every case where, pursuant to the use of an RCOS, NFTF Customers are required to transmit ID documentation, data or information under both P.16f.para.20b of the ESAs Opinion: '*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)*' as well as under P.20 para.43 of the EBA Guidelines: '*Where possible, credit and financial institutions should use remote customer onboarding solutions that include randomness in the sequence of actions to be performed by the customer for verification purposes to guard against risks such as the use of synthetic identities or coercion*'.

shall take place before the assumption of the relevant duties by the staff in question and must repeated at regular time intervals[264].

4.3. For the purposes of digital onboarding of NFTF Customers by means of an RCOS, a '*properly trained employee*' is to be understood as an employee of the OE or a person offering services to an OE under the provisions of sections 67(1) or 67(5) (as the case may be) of the AML/CFT Law, who has:

i. Received a professional training on the RCOS to be used by the OE, as well as to how fraudulent practices such as '*deep faking*', '*impersonation*', '*phishing*', '*spoofing*' etc. that are not akin to a specific technology can apply in the context of the RCOS in question; and

ii. Participates in the production or application of/produced (as the case may be) the OE's rules and procedures as regards the introduction and operation of the RCOS in question, including but not limited to the section on the risks arising from the use of such RCOS; for example, weaknesses of the specific underlying technology of the RCOS, which can be used for fraudulent purposes; and

iii. Is sufficiently trained to anticipate and prevent the intentional or deliberate use of deception techniques related to remote verification, and to detect and react in case of their occurrence; and

iv. Been designated by the OE as a person responsible for participating in and/or supervising the process of onboarding the NFTF Customer by means of the RCOS in question.

[264] This is a generally applicable requirement that has to be considered in the context of any RCOS, including thus the one in question, as per P.10 para.17i of the ESAs Opinion: '*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*' and P.12 para.9e of the EBA Guidelines: *'…a description of the induction and regular training programs to ensure staff awareness and up-to-date knowledge of the functioning of the remote customer onboarding solution, the associated risks, and of the remote customer onboarding policies and procedures aimed at mitigating such risks.*'. and P.20 para.42(b) of the EBA Guidelines: '*…foresee the participation of an employee that has sufficient knowledge of the applicable AML/CFT regulation and security aspects of remote verification and who is sufficiently trained to anticipate and prevent the intentional or deliberate use of deception techniques related to remote verification, and to detect and react in case of their occurrence…*'.

4.4. In addition, OEs shall ensure through appropriate procedures that the employees carrying out the NFTF identification and verification of the identity of natural persons by means of any technological solution chosen, do not co-operate with persons involved in illegal activities[265]. Such procedures must include the control on the suitability of the employees in question prior to their employment and such employees' regular assessment thereafter. Furthermore, the random assignment to the employees 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 employees' communication with other natural persons during or after the performance of the electronic NFTF identification procedure.

[265] Controls against collusion practices is a generally applicable requirement under both P.10 para.17h of the ESAs Opinion: '*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*.' and P.20 para.43 of the EBA Guidelines: '*Where possible, credit and financial institutions should use remote customer onboarding solutions that include randomness in the sequence of actions to be performed by the customer for verification purposes to guard against risks such as the use of synthetic identities or coercion. Where possible, credit and financial institutions should also provide random assignments to the employee responsible for the remote verification process to avoid collusion between the customer and the responsible employee*.'