10 Shenton Way MAS Building Singapore 079117 Telephone 65 6225 5577 Facsimile 65 6229 9229

Circular No.: AMLD 01/2022

Date: 8 February 2022

To the Chief Executive Officers of All Financial Institutions

Dear Sir/Madam

NON-FACE-TO-FACE CUSTOMER DUE DILIGENCE MEASURES

A INTRODUCTION

Financial institutions (FIs) are increasing the use of non-face-to-face (NFTF) measures and technologies as part of their customer due diligence (CDD). We encourage the responsible adoption of new technologies to mitigate money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks. To better support FIs' understanding and assessment of available technology solutions, this Circular sets out industry good practices observed by MAS[1] and additional supervisory guidance on the NFTF CDD measures to help mitigate impersonation and fraud risks[2].

B NON-FACE-TO-FACE CUSTOMER DUE DILLIGENCE MEASURES

(i) Natural Persons[3]

2 FIs have been integrating the use of Myinfo in CDD checks, including the identification and verification of identity for Singapore Citizens and Permanent Residents at customer onboarding. While most FIs have also used Myinfo to identify and verify the identity (ID&V) of foreigners based in Singapore[4], they have supplemented this approach with additional checks (such as sighting of original documents) to verify passport details that are not currently available on Myinfo.

[1] Based on a series of thematic engagements with selected FIs such as banks, capital markets services intermediaries, payment institutions and direct life insurers.

[2] For avoidance of doubt, this Circular should be read in conjunction with the relevant MAS Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Notices and Guidelines in relation to CDD Measures for Non-Face-to-Face Business Relations, as well as MAS' Circular of 8 January 2018 (AMLD 01/2018) on the use of Myinfo and CDD measures for NFTF business relations.

[3] Includes connected parties, beneficial owners and natural persons appointed to act on behalf of the customer.

[4] Foreigners who have a valid permit (e.g. work permit or employment pass) can register for Singpass and avail themselves to the Myinfo service. From November 2021, the registered address for certain groups of foreigners based in Singapore (e.g. Long Term Visit Pass (LTVP), LTVP+, Student Pass, S Pass, Employment Pass, Dependent Pass) is available on Myinfo.

3 Besides the use of Myinfo, FIs have utilised video-conferencing as a means to onboard customers instead of physical meetings. This typically entails engaging the individuals and sighting their identification (ID) documents over the video call. To mitigate the risks of fraud and impersonation, FIs should put in place appropriate controls during the video-conferencing process to verify the identity of the customer and the authenticity of the ID documents sighted via video-conferencing. In this regard, some FIs have required the use of control questions to be answered by the customer, or performed liveness[5] checks to detect impersonation (such as the use of a pre-recorded video feed). As FIs transit to more digital means of onboarding customers, they should continue to raise staff vigilance and conduct training to enable detection of possible fraudulent or tampered ID documents. For example, some FIs have trained staff involved in the video-conferencing process to specifically look out for the requisite authentication markers on the ID documents displayed by the customer on screen.

4 Notwithstanding, the use of video-conferencing alone may not always be sufficiently adequate to detect and mitigate fraud and impersonation risks. FIs should perform additional checks via a different channel as appropriate, to complement the video-conferencing process, especially for accounts that pose higher ML/TF risks. On this front, some FIs have supplemented the video-conferencing approach with additional checks, such as verifying the customer's information against reliable and independent databases or performing a check sum digit test[6] to identify data validation errors in the customer's ID document.

(ii) Legal Persons and Legal Arrangements

5 In general, we noted that FIs tended to use publicly available sources or databases such as company registries and annual reports to ID&V customers who are legal persons. Video-conferencing may be used to ID&V connected parties, beneficial owners and natural persons appointed to act on behalf of the customer. However, CDD documents that cannot be verified against a registry or lack the requisite authenticity markers (such as a foreign certificate of incorporation) should not be verified purely via video-conferencing. FIs should institute additional measures to verify that the soft copies of documents are genuine, such as by obtaining an original certified true copy or requiring suitably qualified persons[7] to use digital signatures or watermarks to certify the authenticity of the soft copies of the documents.

6 A few FIs have also started to explore the use of electronic signing (e-signing) techniques to facilitate the establishment and continuation of NFTF business relations, instead of obtaining wet ink signatures. For example, FIs are exploring the acceptance of documents that have been e-signed by directors and authorised signatories of corporate customers using GovTech's new "Sign with

[5] Example of liveness checks manually performed by the FI's staff include requesting the customer to tilt his head in a unique sequence of different directions as prescribed by the FI's staff.
[6] This typically involves an algorithm test to verify the data integrity of the digits set out in the machine readable zone (MRZ) of passports.
[7] Examples of a suitably qualified person include a notary public, a lawyer or certified public or professional accountant.

Singpass"[8] feature, while some are using or considering the use of various vendor solutions for enabling e-signatures. The MAS Notices on the prevention of ML and countering the financing of terrorism provide for the use and retention of electronic copies of documents, subject to them being admissible as evidence in the Singapore courts. FIs should assess the robustness of processes in place to safeguard the authenticity of electronic documents and their admissibility in court[9].

C USE OF NEW TECHNOLOGY SOLUTIONS

7 The use of new technology solutions[10] (e.g. biometrics technologies, liveness detection technologies, document authenticity verification tools, etc.) has the potential to improve effectiveness and efficiency of the NFTF CDD processes as well as enhance the customer experience. FIs should regularly review such technology solutions to ensure their continued effectiveness in identifying and verifying customers remotely.

8 In general, the adoption of new technology solutions to fulfil CDD requirements appear to be more widely adopted for natural persons than legal persons and arrangements. This section elaborates on some of these new technology solutions adopted by a small but growing number of FIs to address the heightened risks of (i) impersonation and (ii) fraudulent or tampered documents in a NFTF setting.

(i) Risk of Impersonation

9 Most of the solutions deployed by FIs surveyed included elements of biometrics technology, such as facial recognition, where digital algorithms are used to match the face in the ID document against that in the live video or selfie photo. Liveness detection technology that uses algorithms to analyse data collected from biometric sensors is also employed to verify if the FI is interfacing with an actual customer or a fake representation[11].

10 These new technology solutions are either purchased from third-party solution providers or developed in-house. Several FIs are exploring "Identiface with Singpass"[12], which taps on facial biometrics data available with the Singapore Government to verify the identity of the customer, without the need for FIs to collect them separately.

---

[8] https://api.singpass.gov.sg/library/sign/business/introduction

[9] For instance, in Singapore's context, the admissibility of electronic records as evidence is governed by the Evidence Act (Cap 97). Section 116A of the Evidence Act contains certain presumptions which a party seeking to use electronic records as evidence in court may rely on.

[10] For avoidance of doubt, a technology is considered new if it is new to, or has yet to be widely adopted by, FIs in Singapore for AML/CFT purposes. Some examples are provided in section C of this Circular.

[11] The use of liveness detection technology enables the FI to more effectively detect spoofing attempts, as compared to a manual liveness check performed by the FI's staff. The latter may not be as effective in addressing impersonation risks, such as the case where deepfake video frames are being injected directly into the camera feed to appear like the customer is responding to instructions by the FI's staff to tilt his head etc.

[12] https://api.singpass.gov.sg/library/identiface/business/introduction

(ii) Risk of Fraudulent or Tampered Documents

11 A number of FIs reported the use of in-house or third-party ID document authenticity verification tools to detect fraudulent or tampered ID documents. This includes capturing unique security features embedded in the customer's ID document and verifying them against databases through the use of Application Programming Interfaces (APIs). Data validation[13] and data consistency[14] checks are also performed in addition to checks against police records, to ascertain if the ID document has been stolen, lost or compromised.

12 To ensure that these new technology solutions are fit-for-purpose, FIs should conduct an internal assessment of the effectiveness of the solutions in mitigating impersonation and fraud risks prior to implementing them. FIs should not solely rely on external quality assurance standards of the technology service providers to arrive at their conclusion, but should perform their own assessments. The FI's assessment of technology solutions should be approved by Board and Senior Management. On an ongoing basis, FIs should also monitor the robustness of their technology solutions to ensure that the solutions continue to remain effective in mitigating impersonation and fraud risks. Guidance on the assessments of new technology solutions is provided in the **Annex**.

D ENHANCING INTERNAL CONTROLS

13 The use of new technology solutions has the potential to improve onboarding efficiency and mitigate risks associated with NFTF onboarding. Notwithstanding, technology solutions are not immune to failures and can still be exploited by criminals. For example, there may be instances where the Optical Character Recognition technology may not be able to correctly recognise text on low-quality images or documents with physical labels added onto them. When verification by the new technology solution fails, corrective action is required. As such, it is important for FIs to establish appropriate metrics to monitor the performance of the technology solutions employed and take timely intervention measures where there are issues observed.

14 To address the residual risks with the use of new technology solutions, FIs have put in place additional controls, such as requiring the customer to make an initial deposit into the account with the FI from funds held by the customer in a bank account in Singapore[15] or performing a call-back to the customer using a telephone number that can be independently verified.

15 MAS expects the Board and senior management of FIs to maintain effective oversight of the management of ML/TF risks and AML/CFT controls. In particular, FIs should put in place effective

[13] This includes verifying whether algorithmically-validatable elements e.g. document numbers in the MRZ of the ID document are accurate.

[14] This includes verifying whether data represented in multiple places on the ID document e.g. MRZ lines and Optical Character Recognition-extracted text on the ID document are consistent.

[15] Some FIs have extended this to funds held by the customer in an account with a foreign bank subject to, and supervised for compliance with AML/CFT requirements consistent with the standards set by the Financial Action Task Force (FATF). Where this is the case, FIs should perform adequate risk assessment to assess the ML/TF risks associated with the jurisdiction, to ensure that it is within the FI's risk appetite to do so.

mitigating controls to address the heightened impersonation and fraud risks where customers are onboarded remotely. It is also imperative that FIs properly establish clear accountability for the effectiveness of NFTF CDD processes and technology solutions to manage these risks.

16 A number of FIs have raised queries on the adoption of NFTF CDD measures that may be of relevance to the wider industry. Our responses to these frequently asked questions are in the **Annex** to this Circular.

Yours faithfully

(Sent via MASNET)

VALERIE TAY
EXECUTIVE DIRECTOR
ANTI-MONEY LAUNDERING DEPARTMENT

Annex: FAQs on the Adoption of NFTF CDD Measures

A. Use of Video-Conferencing (VC) to establish NFTF business relations
A1. Where VC is used to establish NFTF business relations, would the FI need to conduct additional checks or would the sole use of VC suffice? As outlined in MAS' Circular No. AMLD 01/2018 dated 8 January 2018, FIs may hold real-time VC that is comparable to face-to-face communication, in establishing NFTF business relations. In using this approach, FIs should put in place appropriate controls during the VC process, to verify the identity of the customer and the authenticity of the ID documents sighted via VC. Some examples of such controls that are put in place during the VC process are set out in paragraph 3 of this Circular. To mitigate the risks of impersonation and fraud, FIs should also perform additional checks, as appropriate, to complement the VC process. The Guidelines to MAS' Notices on prevention of ML and countering the financing of terrorism provide some examples of these additional checks. Other examples are also set out in paragraph 4 of this Circular. FIs are encouraged to adopt new technology solutions (e.g. biometrics technologies, liveness checks, document authenticity verification tools, etc.) that complement the use of VC, to more effectively ID&V customers remotely.
A2. Would the use of VC to sight the original CDD documents suffice, or would the FI still be required to obtain a Certified True Copy (CTC) of the documents from the customer? Where the FI has sighted an original ID document via VC and is satisfied that the ID document sighted is consistent with the soft copy furnished by the customer, the FI would not need to obtain a CTC of the ID document. Please note that the supervisory expectations on the use of VC (as set out in A1 above) would continue to apply. For the avoidance of doubt, CDD documents that cannot be verified against a registry or lack the requisite authenticity markers (e.g. a foreign certificate of incorporation that cannot be verified against a company registry) should not be verified via VC alone. FIs should conduct additional checks to verify that the soft copy is genuine, such as obtaining an original CTC[16], or requiring suitably qualified persons to use digital signatures or watermarks to certify the authenticity of the soft copy.

[16] Identification documents of customers, authorised signatories and beneficial owners should be certified by parties independent of the customer. For "connected parties" as defined in the Notices on Prevention of Money Laundering and Countering the Financing of Terrorism, where only identification is required, and verification is risk-based, the CTC could be done by internal parties of the customer, such as company secretary, in-house lawyer, or director (although a director cannot CTC his own ID document).

B. CTC documents

B1. Can soft copies of CTC documents be accepted, or would the FI need to obtain the original hard copy CTC documents?

Scanned copies of CTC documents may be accepted, provided the FI puts in place measures to detect possible fraudulent or tampered documents. This could include, but are not limited to, (i) sighting the original document via VC with the appropriate controls in place (see A1 and A2 above), in addition to obtaining a scanned copy of the CTC document, or (ii) performing an independent call-back to the certifier, to verify the authenticity of the certification provided.

In the longer term, FIs are encouraged to adopt new technology solutions and digital signatures or watermarks to verify the authenticity of soft copy documents.

C. Assessment of New Technology Solutions

C1. How should the assessment of the new technology solution be conducted, and what should be included in the scope of such assessments?

(i) Prior to implementing the technology solution, the FI should conduct an internal assessment[17] of the effectiveness of the technology solution in mitigating impersonation and fraud risks. The FI's assessment should be approved by Board and Senior Management.

Some non-exhaustive areas that FIs may cover in this assessment include:

- Understand functionalities of the technology solution;
- Evaluate effectiveness in risk mitigation – including testing functionalities and assessing reliability of underlying databases used;
- Evaluate residual risks and put in place appropriate risk mitigation measures.

(ii) At the first-year mark after implementation, a once-off independent assessment by a suitably qualified professional[18] should be performed to certify the effectiveness of the new technology solution in managing impersonation and fraud risks. This has been conveyed in MAS' Circular No. AMLD 01/2018 dated 8 January 2018.

Some non-exhaustive areas that FIs may cover in this assessment include:

- Review the policies and procedures, including guidance and training provided to staff, on the use of the new technology solution to perform NFTF CDD;

[17] This can be conducted in-house by the FI's control function (e.g. Internal Audit or Compliance). Where the FI does not have the relevant capabilities or expertise to do so, the assessment should be done by an independent third party (e.g. External Auditor or qualified consultant).

[18] Any suitably qualified professional may perform the independent assessment of new technology solutions for NFTF verification. This can include the FI's Internal Audit (IA) function, where the IA has the necessary expertise to do so. FIs may also engage an External Auditor or independent qualified consultant to conduct the assessment and certification of the effectiveness of the new solution in managing impersonation and fraud risks.

- Test the effectiveness of the new technology solution in detecting red flags e.g. potential fraudulent or tampered document;
- Assess the adequacy and effectiveness of controls that have been put in place to mitigate impersonation and fraud risks;
- Ensure the proper oversight and governance of the adoption of the new technology solution;
- Propose recommendations for enhancements and remediate any gaps on a timely basis.

FIs should continue to monitor the robustness of their technology solutions on an ongoing basis to ensure that the solutions remain effective in mitigating impersonation and fraud risks.

C2. Would it suffice for the FI to rely on an external quality assurance standard to ascertain the robustness of the technology solution?

FIs cannot solely rely on external quality assurance standards of the technology service providers to arrive at its conclusion but should perform its own assessment (as set out in C1 above). For avoidance of doubt, FIs are not expected to assess the algorithms underpinning the new technology solution, but rather to understand the functionalities offered by the solution, to assess its suitability for the FI's NFTF CDD process.

FIs should also ensure that the implementation of the technology solution is in line with the MAS Technology Risk Management guidelines.