BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions (AML/CFT and TFS for FIs) (Supplementary Document No. 1) – Money Services Business Sector

Issued on: 30 June 2021

BNM/RH/PD 031-15

PART A: OVERVIEW

PART B: POLICY REQUIREMENTS

PART A: OVERVIEW

1. Introduction

1.1 As digitalised products have gained prominence in the recent years and is further accelerated by the new normal, there is a necessity to enhance digital solutions for corporate entities.

In view of this and following the successful introduction of electronic Know-Your-Customer (e-KYC) solutions for individual customers of remittance and money-changing businesses in 2017 and 2019 respectively, the scope of non face-to-face (non-FTF) onboarding verification process is further expanded to include corporate customers. This expanded scope aims to increase efficiency and inclusivity of electronic remittance and money-changing solutions through online channel and mobile channel, by leveraging on financial technology.

This policy document provides for the approved money services business (MSB) licensed under the Money Services Business Act 2011 (MSBA) to establish business relationships with their corporate customers by way of electronic means without face-to-face verifications, and sets out the minimum requirements and standards that an approved licensed MSB must observe in implementing non-FTF verification process to onboard corporate customers. This is to ensure effective and robust Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) control measures and systems are in place to safeguard the safety and integrity of money services.

2. Legal Provisions

2.1 This policy document is issued pursuant to:

(a) Sections 16, 18, 19, 66E and 83 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA); and

(b) Sections 34(1) and 74(1) of the MSBA.

3. Applicability

3.1 This policy document is applicable to reporting institutions licensed under the MSBA which carry on remittance and money-changing businesses using non-FTF onboarding verification process for corporate customers.

4. Effective Date

4.1 This policy document comes into effect on 30 June 2021.

5. Relationship with Existing Policies

5.1 Where applicable, this policy document must be read together with the followings –

(a) Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions (AML/CFT and TFS for FIs) policy document issued on 31 December 2019;

(b) Electronic Know-Your-Customer (e-KYC) policy document issued on 30 June 2020; and

(c) any other legal instruments, policy documents and guidelines issued by the Bank.

6. Interpretation

6.1 The terms and expressions in this policy document shall have the same meanings assigned to them in the AMLA, MSBA, and AML/CFT and TFS for FIs policy document issued on 31 December 2019, as the case may be, unless otherwise defined in this document.

6.2 For the purpose of this document–

"**S**" denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action.

"**G**" denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted.

"**the Bank**" means Bank Negara Malaysia.

"corporate customer" means a legal person as specified under paragraph 6.2 of AML/CFT and TFS for FIs policy document i.e. any entity other than a natural person that can establish a permanent customer relationship with a reporting institution or otherwise own property. This includes companies, bodies corporate, government-linked companies, foundations, partnerships, or associations and other similar entities.

"authorised person" means a natural person appointed in writing by a corporate customer to represent or act on its behalf. For avoidance of doubt, an authorised person, in this policy document refers to a person who is given the mandate by the corporate customer to operate and maintain an account with a reporting institution including to open, close and give any instruction for the conduct of remittance or money-changing transactions.

PART B: POLICY REQUIREMENTS

7. Implementation of Non Face-to-Face Business Relationship for Corporate Customers

S 7.1 Reporting institutions shall obtain approval from their Board of Directors (Board) prior to the implementation of non-FTF onboarding verification in establishing business relationships with its corporate customers, unless otherwise specified by the Bank.

S 7.2 Reporting institutions shall obtain prior written approval from the Director, Money Services Business Regulation Department, Bank Negara Malaysia to implement non-FTF for the provision of online or mobile remittance and money-changing business for their corporate customers.

S 7.3 The application for implementation of non-FTF for corporate customers shall include relevant information to demonstrate the reporting institution's ability to comply with the requirements in this policy document.

S 7.4 Reporting institutions must comply with any additional measures imposed on the implementation of non-FTF as deemed necessary by the Bank.

S 7.5 Reporting institutions are required to be vigilant in establishing and conducting business relationships via electronic means, which includes mobile channel and online channel.

S 7.6 In respect of paragraph 7.5, the Board shall set and ensure the effective implementation of appropriate policies and procedures to address any risks associated with the implementation of non-FTF business relationships with its corporate customers. These include risks on operational, information technology such as cyber threats as well as risks associated with money laundering and terrorism financing (ML/TF).

S 7.7 Reporting institutions must ensure and be able to demonstrate on a continuing basis that appropriate measures for identification and verification of the corporate customer's identity are as effective as that of face-to-face process and implement monitoring and reporting mechanisms to identify potential ML/TF activities.

S 7.8 In relation to paragraph 7.7, reporting institutions shall take all necessary measures to identify and verify a corporate customer's identity which include, at a minimum:

(a) undertake all measures as required by AML/CFT and TFS for FIs policy document in relation to corporate customers. This includes understanding the nature of the corporate customer's business, its ownership and control structure, verifying the corporate customer's identity against independent and credible sources, including information on its CEO and directors as well as taking reasonable measures to verify the identity of the ultimate beneficial owners as specified under paragraph 14C.10.7 of AML/CFT and TFS for FIs policy document;

(b) verify the existence of business activity of the corporate customer through a mandatory verification method supported by at least an additional verification method specified in paragraph 7.9; and

(c) verify the authorised person to represent the corporate customer by means of a letter of authority or directors' resolution when dealing with such person. This is to ensure that the person is authorised to conduct transactions on behalf of the corporate customer. In identifying and verifying an authorised person's identity, reporting institutions may undertake measures including but are not limited to the following-

(i) verifying the authorised person against a government issued ID by utilising biometric technology;

(ii) ensuring that the government issued ID used to support e-KYC verification is authentic by utilising appropriate fraud detection mechanisms; and/or

(iii) ensuring the authorised person is a live subject and not an impersonator (e.g.through use of photos, videos, facial masks) by utilising liveness detection[1].

S 7.9 In relation to paragraph 7.8 (b), reporting institutions shall undertake a mandatory verification method and at least one additional verification method that is relevant to the nature or business model of the corporate customers, as follows:

Mandatory verification

(a) make unannounced video calls to the CEO, directors, or authorised person assigned to the corporate customer. During the video call, reporting institutions may request the person to show proof of business existence such as signboard or inventories (if any); and

Additional verification methods

(b) identify the location of corporate customer to ensure that the location matches the registered or business address of the corporate customer. Reporting institutions may also verify location of the CEO, directors, or authorised person during the video call;

(c) verify the corporate customer's information against a database maintained by credible independent sources such as relevant regulatory authorities, government agencies or associations of the regulated sectors. Reporting institutions may also request for corporate customer's active bank account or audited financial statement as proof of on-going business activity; or

(d) any other credible verification methods as approved by the Bank.

[1] For the purpose of this document, liveness detection refers to the ability of a system to determine if the person is a live person, a person impersonating as another or a reproduction. This includes determining the person's face has not been digitally modified, and analysing facial movements such as lip movement, eye movement or blink detection.

S 7.10 Reporting institutions, based on their own risk assessment, shall clearly define parameters for higher risk corporate customers that are not allowed to transact with the reporting institutions through non-FTF onboarding process.

S 7.11 Reporting institutions must ensure the systems and technologies developed and used for the purpose of establishing business relationships using non-FTF channels (including verification of identification documents) have capabilities to support an effective AML/CFT compliance programme.

S 7.12 In addition to paragraphs 7.8 and 7.9, reporting institutions shall comply with the following requirements for remittance and money-changing transactions undertaken based on non-FTF:

(a) all payments or transfer of funds for remittance and money-changing transactions made to the reporting institutions shall only be made from a bank account with any licensed bank or licensed Islamic bank under the Financial Services Act 2013 and Islamic Financial Services Act 2013 respectively, or any prescribed institution under the Development Financial Institutions Act 2002, registered under the name of its corporate customer. Corporate customer details (i.e. name or business identity number) obtained in relation to the bank account must be consistent with the details provided by its corporate customer during the non-FTF onboarding process;

(b) put in place robust and appropriate information technology security control measures which include, but are not limited to, linking each authorised person's account to only one mobile device, with unique login credentials for the purpose of authenticating the transaction. The Bank may at any time impose additional specific controls as it deems appropriate; and

(c) no more than two authorised persons shall be registered under each corporate customer's transaction account at any one time.

S 7.13 For remittance transactions undertaken based on non-FTF, in addition to paragraph 7.12, reporting institutions shall comply with the following requirements:

(a) observe the daily outward transaction limits set out under paragraph 3 (a) and (b) of Money Services Business (Remittance Business) Regulations 2012, and paragraph 2 of Money Services Business (Remittance Business) (Amendment) Regulations 2015; and

(b) sight and obtain relevant documentary proof on business transactions such as invoices, loan documentation etc., prior to undertaking the transactions.

8. Enforcement

S 8.1 Where the Bank deems that the requirements in this document have not been complied with, the Bank may:-

(a) take appropriate enforcement action against the reporting institution, including the directors, officers and employees, with any provision marked as “S” in this document;

(b) direct the reporting institution to undertake corrective action to address any identified shortcomings; and/or

(c) suspend or revoke an approval given under paragraph 7.2.