BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Guidance on Verification of Individual Customers for Customer Due Diligence

Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions, Designated Non-Financial Businesses and Professions and Non-Bank Financial Institutions (AML/CFT and TFS for FIs, DNFBPs and NBFIs)

Date: 1 September 2020

TABLE OF CONTENTS

Part A: Overview

1.0 Foreword

1.1 This Guidance is intended to provide clarification and recommended practices in relation to identification and verification of the customer due diligence (CDD) requirements under the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions, Designated Non-Financial Businesses and Professions and Non-Bank Financial Institutions (AML/CFT and TFS for FIs, DNFBPs and NBFIs) Policy Documents (hereinafter referred to as Policy Documents).

1.2 The Guidance is not intended to replace any requirements in the abovementioned Policy Documents. Reporting institutions should not regard the information in the Guidance as exhaustive nor should it be used as evidence of compliance.

1.3 Any updates to the Guidance will be notified to the reporting institutions from time to time. Should there be any need to obtain further clarification or explanation on the Guidance, enquiries may be mailed to the following addresses:

(i)	For FIs	: amlpolicy@bnm.gov.my
(ii)	For DNFBPs & NBFIs	: fied@bnm.gov.my

2.0 Objectives

2.1 An effective CDD is the cornerstone of a robust AML/CFT and TFS program. The CDD process involves identifying and verifying the identity of customers as well as understanding the purpose and nature of business relationship.

2.2 The objective of this process is fundamentally to:

(a) prevent reporting institutions from creating anonymous and fictitious accounts[1]; and

(b) assess the extent of money laundering and terrorism financing (ML/TF) risks posed by customers and businesses, for the development of appropriate controls and mitigation that commensurate with identified risks.

[1] Section 16 of the AMLA prohibits RIs to open or operate anonymous account or account which is in a fictitious, false or incorrect name.

2.3 Identification in the context of CDD refers to the process where reporting institutions obtain information about customers in accordance with the Policy Documents.

2.4 Verification refers to the process of confirming the customers' information collected at the identification stage against documents, data or information from reliable sources, independent of the customers.

2.5 Reporting institutions are expected to determine the extent of verification, depending on the identified ML/TF risks. For example, where there are higher ML/TF risks, the extent to which information must be verified should expand, while where ML/TF risks are lower, verification process may be more simplified.

2.6 This document aims to clarify the definition of customer's identity, factors to guide risk-based verification, types of reliable and independent sources of documents, information and data, as well as suggested risk-based applications for verification particularly with regard to individual customers, and where applicable, to beneficial owners.

Part B: Guidance

3.0 CDD: Customer Identification and Verification

3.1 The mandatory components of CDD as outlined in the Policy Documents entail the following processes:

Paragraph 14 of the Policy Documents on CDD:

Identification of customer, beneficial owner and whenever applicable, person conducting transaction
Objective: To enable reporting institutions to distinguish the individual from any other person they are dealing with and whether the person is acting on behalf of another.

Verification of the information through reliable and independent documentation, electronic data or any other measures deemed necessary
Objective: To ensure that the information about the individual is accurate and up-to-date.

Understanding the purpose and nature of business relationship between the reporting institutions and the customer
Objective: To assess whether the business relationship is in line with the reporting institutions' expectation and to provide the reporting institutions with a meaningful basis for ongoing monitoring.

3.2 Similar verification measures should be adopted for persons conducting transactions on behalf of a customer.

Customer identification

3.3 Reporting institutions are required to obtain, at minimum, a prescriptive list of identification information from customers and beneficial owners. However, it should be noted that the list is non-exhaustive, hence additional information may be obtained by reporting institutions, based on their risk appetite to facilitate risk profiling, wherever necessary.

Paragraph 14 of the Policy Documents:

Minimum list of identification information as outlined in the Policy Documents[2]:

- Full name;
- National Registration Identity Card (NRIC), number or passport number or reference number of any other official documents of the customer or beneficial owner;
- Residential or mailing address;
- Date of birth;
- Nationality;
- Occupation;
- Name of employer or nature of self-employment or nature of business;
- Contact number; and
- Purpose of transaction.

Reporting institutions may obtain additional information based on AML/CFT risks appetites

- Example: e-mail address, gender, marital status.

What constitutes 'identity'?

Identity refers to official identity that is based on characteristics, attributes or identifiers of a person that establish the person's uniqueness in the population, recognized by the country for regulatory or other official purposes. The identity of an individual has a number of principal and fixed aspects, which include given name, date of birth, official identification number or biometric characteristics e.g. facial and thumbprint.

There may also be information that are fluid but are central to distinguish the identity of a person from the population, particularly for persons with common names including nationality, residential address, employment and business career. This information, however, may change over time.[3]

[2] For financial sector's reporting institutions, lesser information may be obtained from customers if they qualify for Simplified CDD under the Policy Documents for FIs, that, include full name, NRIC, number or passport number or reference number of any other official documents of the customer or beneficial owner, residential or mailing address, date of birth, nationality. The 'simplified CDD' regime is not applicable to DNFBPs.

[3] Refer to paragraph on Electronic Evidence.

Customer Verification

3.4 Reporting institutions should verify information of their customers and beneficial owners, collected during identification stage or at any point of the business relationship, as per verification requirements.

3.5 Verification of identity must be based on documents or information obtained from a reliable source, which is independent of the customer.

Documents, data or information issued or made available by an official body are to be regarded as being independent of a person even if they are provided or made available to the reporting institutions by or on behalf of that person.

Additionally, for electronic or digital data and information, their reliability and independence would depend on the assurance levels of the systems or sources in light of ML/TF, fraud, and other risks including cybersecurity risks[4].

4.0 Application of Risk-Based Approach

4.1 Reporting institutions may adopt a risk-based approach to determine the manner of performing verification, in ensuring it is satisfactorily completed:

(a) the extent or volume of information collected;

(b) types of reliable document, data and information; and

(c) the manner/technology used.

4.2 In this regard, reporting institutions should take into account any higher risk circumstances as laid out in the Policy Documents[5], which include, but are not limited to:

(a) the nature of the product or service sought by customers;

(b) the nature and length of any existing or previous relationship between customers and the reporting institutions;

[4] Refer to paragraph on Electronic Evidence.
[5] Please refer to paragraph 10 of the Policy Documents.

(c) the nature and extent of any assurance from other reporting institutions that may be relied on; and

(d) whether the customer is physically present.

4.3 For transactions involving cross-border wire transfer under Paragraph 19.2.1(a) of the Policy Documents[6], reporting institutions may rely on the residential address or date of birth obtained and verified during the CDD process or during on-going CDD, if the reporting institution is satisfied that such information are up to date.

Beneficial owner

4.4 The verification process for a beneficial owner is different from an individual customer. Although the identity of both customer and beneficial owner must be verified through an independent and reliable source, reporting institutions are only expected to take appropriate and reasonable measures so that they are satisfied with the identity of the beneficial owner, having regard to ML/TF risks associated with the customer and business relationship.

Recommended Practice for Reasonable Measures include:

- Make use of records of beneficial owners in the public domain, ask customers for relevant data, or require evidence of the beneficial owner's identity, on the basis of documents or information obtained from a reliable source which is independent of the customer.
- In low risk situations, it may be reasonable for the reporting institution to confirm the beneficial owner's identity based on the information supplied by the customer. This may include a declaration confirming and recognizing the identity of the beneficial owner, be it by the customer, trustees or other persons whose identities have been verified.

Framework for the application of risk-based approach

4.5 Reporting institutions should consider incorporating in their AML/CFT risk management policies and procedures a framework for the application of risk-based approach with regards to the verification of customers.

[6] Applicable to PD for Financial Institutions only.

Recommended Practice

The framework may include:

- a correlation list of the documents, information or data accepted for each risk class.
- assessment of the level of integrity, reliability and independence of each document, data or information. Where appropriate, the level of reliability required may be the result of the combined use of two or more supporting documents.

5.0 Reliable and Independent Sources of Documents, Information and Data

5.1 There is no restriction on the form of evidence to be taken by reporting institutions in verifying the identity. Reporting institutions may accept either physical documents, electronic or digital information and data, or a combination of both.

Documentary evidence

5.2 In the event where reporting institutions use documentary evidence to verify a person's identity, reporting institutions are encouraged to sight the original copies of the documents and retain records of them, in line with record keeping requirements in the Policy Documents.

5.3 Documents purporting to offer evidence of identity differ in their level of integrity, reliability and independence and may come from a number of sources as follows:

(a) Documents issued for the purpose of official identification bearing photographs and without photographs;

(b) Documents issued by courts, government departments, public sector bodies, or local authorities;

(c) Bank statements, or credit/debit card statements issued by regulated financial sector in Malaysia; and

(d) Documents issued by other regulated organizations, for instance a regulated utility company.

5.4 Reporting institutions are recommended to verify customers' identity using the following types of documents which are viewed as offering a high level of reliability and independence for verification:

Official and valid identification documents issued by certain government departments with photograph

Features that contribute to reliability:

- Primary identification document (ID) that is widely recognised, used and accepted by government and private sector in Malaysia as identification, authentication and authorisation for specific services.
- The photograph enables reporting institutions to conduct visual review to reduce risk of impersonation and identity theft.

Examples:

- ID issued by the National Registration Department including NRIC, MyTentera, MyPR, and MyKAS.
- Passport issued by Immigration Department of Malaysia.
- Driving licence bearing photograph issued by the Road Transport Department of Malaysia in view of its interlinkages with NRIC.

5.5 Reporting institutions may also accept official and valid identification documents issued by certain government departments without photograph. In this instance, reporting institutions are recommended to increase the level of reliability and corroborative value of the documents with other additional independent and reliable documents as set out in paragraph 5.3 above.

Official and valid identification documents issued by government departments without photograph, with additional corroborating documents.

- Examples, MyKid, birth certificate and pension card.

Features that contribute to reliability:

- ID that is recognised by the government and private sector in Malaysia as identification, authentication and authorisation for specific services.

Supported by corroborative documents such as –

- In case of a child below the age of 12, ID of the parent/guardian.
- Current bank statements issued by banks including development financial institutions licensed and incorporated in Malaysia.
- Current utility bills for specific duration as determined by reporting institutions.
- Quit rent and assessment notice as issued by state municipal councils.

5.6 For foreigners, reporting institutions are recommended to accept only official and valid foreign passport issued by a foreign government, and if applicable, a visa to enter Malaysia.

In the event where foreigners are unable to produce passport, such as refugees, reporting institutions should consider:

- Keeping records of their assessment on the challenges and proposed measures to verify the identity of the customer (at minimum, the name or date of birth).
- Accepting as identity evidence; a document, letter, or statement from United Nations or its agency (examples, United Nations High Commissioner for Refugees cards) or appropriate person who knows the individual, that indicates that the person is who she/he says she/he is.

5.7 Reporting institutions are advised to refrain from accepting an expired passport and/or visa, if applicable, at the initial stage of establishing business relationship with foreign customers.

Recommended Practice

- Passport and other international documents should be valid for a period for at least six (6) months before expiry dates at the time of CDD. The validity of these documents must be monitored as part of the on-going due diligence process.

5.8 Reporting institutions should take cognizance of the type of documents which are more easily forged than others.

5.9 Reporting institutions should consider prescribing appropriate measures and controls that leads to a reasonable conclusion that the documents presented are not forged or falsified. This includes referring to other regulatory sources as set out in paragraph 5.15 and additional measures in paragraph 5.16 below:

Examples of Current Practice

Use of NRIC reader

- **FIs**:
  Reporting institutions commonly require NRIC for identification and verification where the card terminal is used to read biometric (thumbprint) and NRIC information.

- **DNFBPs:**
  Businesses employ the use of NRIC reader that links the NRIC to its holder via thumbprint to avoid misuse of NRIC to conduct transactions such as false signing of legal documents in the client's capacity. There is also an initiative at the association level to develop a system that links details of the customer to the NRIC reader for verification purpose. This system is being deployed by the industry players.

Electronic evidence

5.10 Reporting institutions may use electronic or digital data and information to verify identity, for example digital identity or e-KYC solutions, either on its own or taken together with documentary evidence.

5.11 Similar to documentary evidence, electronic or digital data and information are also subject to the reliability and independence test.

5.12 In assessing whether an electronic or digital data and information is sufficiently reliable and independent to prove identity for the purpose of CDD, reporting institutions are recommended to:

(a) understand the assurance levels of the systems or sources including the underlying data they relied on, technology, architecture and governance to determine their reliability and independence;

(b) given the assurance levels, make a risk-based determination of whether it is appropriately reliable, independent in light of the ML/TF, fraud, and other risks including cybersecurity risks; and

(c) fulfill requirements as set out in the Electronic Know-Your-Customer (e-KYC) Policy Document[7].

5.13 Reporting institutions are advised to incorporate within their AML/CFT risk management policies and procedures information on-

(a) the assessment of factors in paragraph 5.12 above; and

(b) determination whether there is a need for additional measures as specified in paragraph 5.16 to supplement the use of electronic evidence in certain circumstances including in higher ML/TF risk situations or by virtue of reporting institutions own AML/CFT, anti-fraud and general risk management policies.

5.14 Reporting institutions shall document and record their internal assessments to be made available to supervisors or the competent authority upon request.

5.15 Reporting institutions are encouraged to refer to policy documents or guidances issued by Bank Negara Malaysia and other standard setting bodies, pertaining to verification through this means.

Additional verification measures

5.16 Reporting institutions should consider applying additional verification measures to mitigate the risk of impersonation fraud in circumstance where there is uncertainty over the customers' identity. This includes whenever:

(a) copies of original documents are used;

(b) customers are not met face-to-face in the process of establishing relationship;

(c) there is a need to supplement the use of electronic or digital data and information for verification; or

(d) there is doubt on the legitimacy and authenticity of the documents provided by the customer.

[7] BNM/RH/PD 030-10 Issued on: 30 June 2020

5.17 The additional verification measures may consist of anti-fraud measures that the reporting institutions routinely undertake as part of their existing CDD procedures.

5.18 The following are examples of additional measures, which are non-exhaustive and should be undertaken to commensurate with the assessed ML/TF risks:

- Corroborating copies of original documents with the National Registration Department database or the Immigration Department of Malaysia databases, telecommunication companies, sanctions lists issued by credible domestic or international sources.
- Requiring the first payment to be carried out through an account in the customer's name with a bank incorporated and registered in Malaysia.
- Video or conference call with the customer prior to opening the account and before transactions are permitted, for the purpose of comparing the physical identity of a customer with copies of original documents and to verify additional aspects of identity information collected during identification stage.
- Internet sign-on following verification where the customer uses security codes, tokens, or passwords, which have been set up during account opening stage.
- Copies of original documents to be certified by an appropriate person. Appropriate persons refer to solicitors, police, court officials, medical doctor, commissioner of oath, notary, or any credible person authorized to certify documents.

6.0 Illustrations of application of risk-based approach

Verification in 'normal risk' cases

6.1 "Normal risk" here refers to all situations that are not recognised as presenting a high risk or low risk in the context of the individual risk assessment. In this situation, reporting institutions may consider applying documentary and electronic data, source and information as set out above, or a combination thereof.

Recommended practices:

- For local customers, reporting institutions commonly require NRIC for identification and verification, where the card terminal is used to read biometric (thumbprint) and NRIC information.
- Where residential and NRIC address are different, utility bills will be required from customers to justify such mismatch.
- Reporting institutions may also require supplementary documents to justify account-opening purposes (examples: university admission/ offer letter for student accounts, employer referral letter for salary accounts, etc.).
- For student accounts, reporting institutions may also establish a list of learning institutions in demarcating level of ML/TF risk.
- Similar requirements are applied to foreign nationals, where the key difference is, passport and travel visa are used as main photo-bearing government-issued evidences for identity verification purposes.

Verification in 'higher risk' cases

6.2 "Higher risk" here refers to circumstances where reporting institutions assess the ML/TF risks as higher, taking into account risk factors arising from customer, country or geographic location of customer, type of product, service, transaction or delivery channel[8].

6.3 In higher risk situations, reporting institutions' AML/CFT risk management policies and procedures should consider only authorising the use of the documents and information that offer the most reliable information, and where appropriate, require the use of a combination of sources of documents, data and information, to increase level of reliability and verification performed.

[8] Description of 'higher risk' in paragraph 6 of the Policy Documents.

Recommended Practices

Face-to-face verification

Reporting institutions to sight and make copies of valid official identification documents with photograph, or in the case of a foreigner, passports/visa.

Non face-to-face (electronic and digital source of data and information)

Reporting institutions to heighten the assurance levels, by assessing the necessity to conduct additional verification measures to supplement verification.

6.4 Reporting institutions should be guided by the list of verification documents, data or information which are acceptable in higher-risk situations based on a thorough assessment to demonstrate that their high level of reliability is appropriate in view of the high level risk and the nature of the ML/TF risk incurred.

Verification in 'low risk' cases

6.5 Where relevant, if the risk assessment has established a case of low ML/TF risk, and if reporting institutions' AML/CFT risk management policies and procedures explicitly specify that simplified due diligence measures can be applied, or lead to the conclusion that the risk level is low, verification remains obligatory. However, reporting institutions may develop appropriate and proportionate measures in their AML/CFT risk management policies and procedures in view of such lower risks.

6.6 Naturally, all reliable and independent sources of documents and information, which the reporting institutions have identified as eligible for verifying the identity of the customer in a normal risks business relationship, are also applicable in low-risks situations.

However, although a copy or electronic image of a supporting document is insufficiently reliable in itself to be accepted for verification, it could be accepted in certain circumstances where the relationship is subject to strict limitations and safeguards (e.g. limited features of products and services) that can reduce ML/ TF risks.

As an example, for insurance products assessed as low risk products, reporting institutions may obtain attestation from:

- Village Head (“ketua kampung”);
- Human resource department of the corporate customer on the identity of insured members of group policies and board of the corporate entity on the authorized person representing the company; or
- Third party administrator (TPA) or hospital for verification at claims stage.

6.7 Reporting institutions are expected to include, in their due diligence procedures and measures, a correlation table of the supporting documents required for each class of reporting risk, as well as a list of the circumstances in which certain supporting documents need not be submitted.

OVERVIEW OF CDD PROCESS