GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING FOR CAPITAL MARKET INTERMEDIARIES

Date Issued: 15 January 2014
## CONTENTS

<table>
<thead>
<tr>
<th>Para</th>
<th>Topics</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>PART I: INTRODUCTION AND APPLICABILITY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Applicability</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Definitions</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>General Description of Money Laundering</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>General Description of Terrorism Financing</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>General Principles And Policies To Combat Money Laundering And Terrorism Financing</td>
<td>6</td>
</tr>
<tr>
<td>PART II: RISK-BASED APPROACH APPLICATION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Risk-Based Approach Application</td>
<td>8</td>
</tr>
<tr>
<td>7.1</td>
<td>Risk Assessment and Profiling</td>
<td>8</td>
</tr>
<tr>
<td>7.2</td>
<td>Risk Management and Mitigation</td>
<td>9</td>
</tr>
<tr>
<td>PART III: CUSTOMER DUE DILIGENCE (CDD)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Customer Due Diligence (CDD)</td>
<td>10</td>
</tr>
<tr>
<td>8.1</td>
<td>CDD at the Point of Establishing a Business Relationship</td>
<td>10</td>
</tr>
<tr>
<td>8.2</td>
<td>On-going CDD</td>
<td>12</td>
</tr>
<tr>
<td>8.3</td>
<td>Risk based Approach in conducting CDD</td>
<td>13</td>
</tr>
<tr>
<td>8.4</td>
<td>Enhanced CDD measures</td>
<td>15</td>
</tr>
<tr>
<td>8.5</td>
<td>Politically Exposed Persons (PEPs)</td>
<td>15</td>
</tr>
<tr>
<td>8.6</td>
<td>High Risk Countries</td>
<td>16</td>
</tr>
<tr>
<td>8.7</td>
<td>Reliance on Third Parties to Conduct CDD</td>
<td>17</td>
</tr>
<tr>
<td>8.8</td>
<td>Failure to Satisfactorily Complete CDD</td>
<td>18</td>
</tr>
<tr>
<td>9</td>
<td>Group Wide ML/TF Programmes</td>
<td>18</td>
</tr>
<tr>
<td>PART IV: RECORD KEEPING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Record Keeping</td>
<td>19</td>
</tr>
</tbody>
</table>
## PART V: SUSPICIOUS TRANSACTIONS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Reporting of Suspicious Transactions</td>
<td>21</td>
</tr>
<tr>
<td>12</td>
<td>Confidentiality of Reporting</td>
<td>23</td>
</tr>
</tbody>
</table>

## PART VI: COMPLIANCE AND TRAINING PROGRAMMES

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Internal Programmes, Policies, Procedures and Controls</td>
<td>24</td>
</tr>
</tbody>
</table>

## PART VII: COMBATING TERRORISM FINANCING

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Identification and Designation</td>
<td>26</td>
</tr>
</tbody>
</table>

## APPENDICES

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix 1</td>
<td>Submission of Suspicious Transactions Report</td>
<td>27</td>
</tr>
</tbody>
</table>
PART I: INTRODUCTION AND APPLICABILITY

1. INTRODUCTION

1.1 The Guidelines on Prevention of Money Laundering and Terrorism Financing for Capital Market Intermediaries (Guidelines) are issued pursuant to Section 83 and section 66E of the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA) and section 377 of the Capital Markets and Services Act 2007 (CMSA).

1.2 These Guidelines are drawn up in accordance with the AMLATFA and the Financial Action Task Force (FATF) 40 Recommendations.

1.3 These Guidelines are issued to provide guidance for the reporting institutions to comply with the obligations imposed under the AMLATFA.


1.5 These Guidelines are made in addition to and not in derogation of any other guidelines issued by the Securities Commission Malaysia (SC) or any requirements as provided for under the securities laws and the AMLATFA. Therefore, reporting institutions must comply with all other relevant guidelines and requirements.

1.6 A reporting institution that is jointly regulated by Bank Negara Malaysia (BNM) and the SC, is required to comply with these guidelines and the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Banking and Deposit-Taking Institutions (Sector 1) issued by BNM. Where there are differing requirements between the said guidelines, the more stringent requirements shall apply.

1.7 Non-compliance with any of the provisions in these Guidelines will subject the reporting institution to actions under the AMLATFA, CMSA or any other relevant provisions under the laws of which these Guidelines are subject to.

2. APPLICABILITY

2.1 These Guidelines are applicable to the reporting institution, including its branches and majority-owned subsidiaries outside Malaysia carrying out the activities as listed in the First Schedule of the AMLATFA.

2.2 In the case of foreign operations, where anti-money laundering and counter financing terrorism (AML/CFT) measures of the host country are less stringent than the Malaysian standards, a reporting institution is required to ensure that its foreign branches and majority-owned subsidiaries apply AML/CFT measures which are consistent with the Malaysian standards, to the extent that the host country laws and regulations permit.
2.3 If the host country does not permit the proper implementation of the AML/CFT measures consistent with the Malaysian standards, the reporting institution is required to apply appropriate additional measures to mitigate the money laundering and terrorism financing (ML/TF) risks, and inform the SC on the AML/CFT gaps and additional measures implemented to manage the ML/TF risks arising from the identified gaps.

2.4 Where the reporting institution is unable to put in place the necessary mitigating measures as required under Paragraph 2.3 above, the reporting institution may consider ceasing the operations of the branch or subsidiary.

3. DEFINITIONS

3.1 Unless otherwise defined, all words used in these Guidelines shall have the following meaning and shall have the same meaning as defined in the CMSA and AMLATFA:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>constituent document</td>
<td>in relation to a body corporate or an unincorporated body, means any document or instrument that—</td>
</tr>
<tr>
<td></td>
<td>• constitutes, establishes or incorporates the body;</td>
</tr>
<tr>
<td></td>
<td>• sets out its governing and administrative structure; or</td>
</tr>
<tr>
<td></td>
<td>• sets out the scope of its functions, business, powers or duties.</td>
</tr>
<tr>
<td>FIED</td>
<td>means the Financial Intelligence and Enforcement Department of Bank Negara Malaysia.</td>
</tr>
<tr>
<td>legal arrangement</td>
<td>means an express trust or other similar legal arrangement.</td>
</tr>
<tr>
<td>legal person</td>
<td>means any entity other than a natural person that can establish a permanent customer relationship with a reporting institution or otherwise own property. This can include company, body corporate, foundation, partnership, or association and other relevantly similar entity.</td>
</tr>
<tr>
<td>politically-exposed person (PEP)</td>
<td>means:</td>
</tr>
<tr>
<td></td>
<td>• Foreign PEP i.e. individual who is or who has been entrusted with prominent public functions by a foreign country, for example Head of State or of government, senior politician, senior government, judicial or military official, senior executive of state owned corporation, important political party official;</td>
</tr>
<tr>
<td></td>
<td>• Domestic PEP i.e. individual who is or has been entrusted domestically with prominent public functions, for example Head of State or of government, senior politician, senior government, judicial or military official, senior executive of state owned corporation, important political party official; or</td>
</tr>
</tbody>
</table>
| **** | **Person who is or has been entrusted with a prominent function by an international organisation which refers to member of senior management, i.e. director, deputy director and member of the board or equivalent functions.**

The definition of PEP is not intended to cover middle ranking or more junior individual in the foregoing categories. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>reporting institution</strong></td>
<td>means a person carrying on regulated activities under the CMSA as specified under the First Schedule of the AMLATFA.</td>
</tr>
<tr>
<td><strong>third party</strong></td>
<td>means a financial institution that is supervised and monitored and that meets the requirements under Paragraph 8.7 of these Guidelines, who is relied upon by the reporting institution to conduct the due diligence process. Reliance on third party often occurs through introductions made by another member of the same group or by another reporting institution. This definition does not include outsourcing or agency relationship because the outsourced service provider or agent is regarded as synonymous with the reporting institution.</td>
</tr>
<tr>
<td><strong>beneficial owner</strong></td>
<td>means the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes that person who exercises ultimate effective control over a legal person or arrangement. Reference to “ultimately owns or controls” and “ultimate effective control” refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.</td>
</tr>
</tbody>
</table>

4. **GENERAL DESCRIPTION OF MONEY LAUNDERING**

4.1 In principle, money laundering generally involves proceeds of unlawful activities that are related directly or indirectly, to any serious offence, that is processed through transactions, concealments, or other similar means, so that they appear to have originated from a legitimate source.

4.2 The process of money laundering comprises of three stages, during which there may be numerous transactions that could alert a reporting institution to the money laundering activities. These stages are:

(a) **Placement**: the physical disposal of benefits of unlawful activities by introducing illegal funds (generally in the form of cash) into the financial
system;

(b) **Layering:** the separation of benefits of unlawful activities from their source by creating layers of financial transactions designed to disguise the audit trail; and

(c) **Integration:** where integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds.

4.3 The illegal funds laundered through the capital market sector may be generated by unlawful activities both from outside and from within the sector. For illegal funds generated outside the sector, transactions involving capital market products may be used as the mechanism for concealing or obscuring the source of these funds.

5. **GENERAL DESCRIPTION OF TERRORISM FINANCING**

5.1 Financing of terrorism generally refers to carrying out transactions involving funds or property, whether from a legitimate or illegitimate source, that may or may not be owned by terrorists, or those have been, or are intended to be used to assist the commission of terrorist acts, and/or the financing of terrorists and terrorist organisations.

5.2 Section 3(1) of the AMLATFA defines a "terrorism financing offence" as any offence under section 130N, 130O, 130P or 130Q of the *Penal Code*, which are essentially:

(a) providing or collecting property for terrorist acts;

(b) providing services for terrorism purposes;

(c) arranging for retention or control of terrorist property; or

(d) dealing with terrorist property.

6. **GENERAL PRINCIPLES AND POLICIES TO COMBAT MONEY LAUNDERING AND TERRORISM FINANCING**

6.1 There is a common obligation in the AMLATFA not to facilitate ML/TF. A reporting institution is required to take the necessary steps in order to prevent ML/TF and have a system in place for reporting suspected ML/TF transactions to the FIED.

6.2 In combating ML/TF, the board of directors of a reporting institution must ensure the following:

(a) **Compliance with laws:** A reporting institution must ensure that laws and regulations are adhered to, that business is conducted in conformity with high ethical standards, and that service is not provided where there is
good reason to suppose that transactions are associated with ML/TF activities.

(b) **Co-operation with law enforcement agencies:** A reporting institution must co-operate fully with relevant law enforcement agencies. This includes taking appropriate measures such as timely disclosure of information by the reporting institution to the FIED and the relevant law enforcement agencies.

(c) **Establishing policies, procedures and training:** A reporting institution must issue and adopt policies and procedures which are consistent with the principles set out under the AMLATFA and these Guidelines. A reporting institution must also ensure that its board of directors and employees are well versed and fully understand these policies and procedures. A reporting institution must also provide adequate training to its board of directors and employees to keep abreast on matters under the AMLATFA and these Guidelines. To promote adherence to these principles, the reporting institution must implement specific policies and procedures including for customer identification, retention of financial transaction documents and reporting of suspicious transactions.

(d) **Risk-based approach:** A reporting institution must ensure that the depth and breadth of its policies and procedures to identify, assess, monitor, manage and mitigate ML/TF risks commensurate with the nature, scale and complexity of its activities.

(e) **Customer Due Diligence:** A reporting institution must have an effective procedure for verifying its customers and obtaining satisfactory evidence of its customer's identity.

6.3 The board of directors in establishing the appropriate policies and procedure for the prevention of ML/TF, must consider carefully the specific nature of its business, organisational structure, type of customer and transaction, etc. to satisfy itself that the measures taken by them are adequate and appropriate to follow the spirit of the suggested measures in these Guidelines.

6.4 The board of directors must also ensure the reporting institution regularly reviews its policies, procedures and controls to ensure its effectiveness and that they are in line with international developments, particularly the FATF Recommendations on combating money laundering and the financing of terrorism and proliferation.
PART II: RISK-BASED APPROACH APPLICATION

7. RISK BASED APPROACH APPLICATION

7.1 Risk Assessment and Profiling

7.1.1 In formulating policies and procedures for the prevention of ML/TF, a reporting institution must take appropriate steps to identify and assess its ML/TF risks, in relation to its customers, products, services, transactions and countries.

7.1.2 The assessment and profiling processes must incorporate the following:

(a) documenting the reporting institution’s risk assessments and findings;

(b) considering all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;

(c) keeping the reporting institution’s risk assessment up-to-date taking into account changes in surrounding circumstances affecting the reporting institution;

(d) having a scheduled periodic assessment or as and when specified by the SC; and

(e) having appropriate mechanisms to provide risk assessment information to the SC.

7.1.3 A reporting institution is also required to identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. The reporting institution must undertake risk assessments prior to the launch or use of such products, practices and technologies and take appropriate measures to manage and mitigate such risks.

7.1.4 In assessing the level of risk of a customer from a particular country, the reporting institution shall assess the standards of prevention of ML/TF in that country based on the reporting institution’s knowledge, experience and other reliable sources of that country. The higher the risk, the greater the due diligence measures that should be applied when undertaking business with the customer from that country.

7.1.5 A reporting institution is required to also implement and maintain appropriate policies and procedures for its representatives and employees to assist them to conduct risk profiling of their customer during the establishment of the business relationship. In determining the risk profile of a particular customer, the reporting institution must take into account, among others the following factors:

(a) customer risks (example residents or non residents, type of customer, occasional or one off, legal person, structure, types of PEP or types of occupation);
(b) geographical location of business or country of origin of customers;

(c) products, services, transactions or delivery channel (example cash-based, face-to-face or non face-to-face or cross-border); and

(d) any other information suggesting that the customer is of higher risks.

7.2 Risk Management and Mitigation

7.2.1 A reporting institution is required to:

(a) have policies, procedures and controls, which are approved by the board of directors, to enable it to manage and mitigate effectively the ML/TF risks that have been identified;

(b) monitor the implementation of those policies, procedures and controls and to enhance them if necessary; and

(c) take enhanced measures to manage and mitigate the risks where higher risks are identified.
PART III: CUSTOMER DUE DILIGENCE

8. CUSTOMER DUE DILIGENCE (CDD)

8.1 CDD At The Point of Establishing Business Relationship

8.1.1 Section 16 of the AMLATFA amongst others clearly sets out customer identification requirements for reporting institutions. A reporting institution is expected to obtain satisfactory evidence of the identity and legal existence of the customer and beneficial owner at the point of establishing the business relationship.

8.1.2 A reporting institution must not keep anonymous accounts or accounts in fictitious names.

8.1.3 A reporting institution is required to—

(a) identify the customer (including foreign body corporate) and verify such customer’s identity using reliable, independent source of documents, data or information;

(b) verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person;

(c) identify and take reasonable measures to verify the identity of the beneficial owner, using relevant information or data obtained from reliable source, such that the reporting institution is satisfied that it knows who the beneficial owner is; and

(d) understand and where relevant obtain information on the purpose of opening an account and intended nature of the business relationship.

8.1.4 A customer who fails to provide evidence of his identity must not be allowed to engage in business relations with the reporting institution. Additional measures must be undertaken to determine whether to proceed with the business relationship, where initial checks fail to identify the customer or give rise to suspicions that the information provided is false.

**CDD requirements for legal persons and legal arrangements**

8.1.5 For customers that are legal persons or legal arrangements, a reporting institution is required to understand the nature of the customer's business, its ownership and control structure. A reporting institution is required to undertake the following:

(a) identify its customers and verify their identity through the following information:

(i) name, legal form and proof of existence, for instance the certified true copy or duly notarized copy of the constituent documents, as the case may be, or any other reliable references;
(ii) the powers that regulate and bind the customer such as directors’ resolution, as well as the names of relevant persons having a senior management position; and

(iii) the address of the registered office and the principal place of business.

(b) identify and take reasonable measures to verify the identity of the beneficial owners—

I. in relation to the identity of the natural person (if any) who ultimately has controlling ownership interest in a legal person, by way of—

(i) duly certified true copy/duly notarised copy of the latest Forms 24 and 49 as prescribed by the Companies Commission of Malaysia or equivalent document for a foreign body corporate; constituent document of a partnership, club, society and charity (as the case may be); and identification document of the shareholders with an equity interest of more than twenty five per cent (25%), directors, partners and office bearers (as the case may be);

(ii) authorisation for any person to represent the company/business either via a letter of authority or directors resolution;

(iii) relevant document such as NRIC for Malaysians/permanent residents or passport for foreigners, to identify the identity of the person authorised to represent the company/business in its dealing with the reporting institution; and

(iv) to the extent, there is a doubt as to whether the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interest, the identity of the natural person (if any) who exercises control of the legal person or arrangement through other means or who holds the position of senior management.

II. in relation to legal arrangements, by way of:

(i) in the case of a trust, the identity of the settlor, the trustee or the protector, the beneficiary or class of beneficiaries and any other natural person exercising ultimate effective control over the trust (including through a gain of control/ownership); or

(ii) in the case of other types of legal arrangement, the identity of the person in equivalent or similar position referred to in II(i) above.

8.1.6 Notwithstanding the above, a reporting institution is exempted from obtaining the constituent document and from identifying and verifying the directors and shareholders of legal persons which fall under the following categories:

(a) public-listed companies/corporations listed on Bursa Malaysia or majority-owned subsidiaries of such public listed companies;
(b) foreign public-listed companies—

(i) listed on exchanges recognised by Bursa Malaysia. A reporting institution may refer to the directive in relation to recognised stock exchanges issued by Bursa Malaysia; and

(ii) not listed in high risks jurisdictions with AML/CFT deficiencies;

(c) government linked companies in Malaysia;

(d) state owned corporations and companies in Malaysia;

(e) authorised person as operator of a designated payment system, a registered person (as the case may be) under the Financial Services Act 2012 and the Islamic Financial Services Act 2012;

(f) entities licensed under the Labuan Financial Services and Securities Act 2010 and the Labuan Islamic Financial Services and Securities Act 2010;

(g) persons licensed or registered under the Capital Markets and Services Act 2007; and

(h) prescribed institutions under the Development Financial Institutions Act 2002.

8.2 Ongoing CDD

8.2.1 A reporting institution must conduct ongoing due diligence and scrutiny of its customers throughout the course of the business relationship. Such measures shall include:

(a) monitoring and detecting patterns of transactions undertaken throughout the course of that business relationship to ensure that the transactions being conducted are consistent with the reporting institution’s knowledge of the customer, its business, and risk profile, including where necessary, the source of funds; and

(b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and are relevant, by undertaking periodic reviews of existing records, particularly for higher risk categories of customer.

8.2.2 A reporting institution must apply CDD measures to existing customers on the basis of materiality and risk and conduct due diligence on such existing relationship at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of the data verified.

8.2.3 For customers that are of higher risk, the reporting institution must monitor the customers’ accounts on a regular basis for suspicious transactions. One method may be to 'flag' such accounts on the reporting institution's computer. This would assist employees of the reporting institution in carrying out future transactions to take note of the 'flag' and pay extra attention to the transactions conducted by that
customer in the account.

8.2.4 A reporting institution should consider reclassifying a customer as higher risk and consider lodging a suspicious transaction report (STR) with the FIED under the following circumstances:

(a) following initial acceptance of the customer, the pattern of account activity of the customer is inconsistent and does not fit in with the reporting institution’s profile knowledge of the customer;

(b) the transaction appears unusual and not in line with the customer’s normal trading pattern; or

(c) there is a material change in the way the account is operated.

8.2.5 While extra care should be exercised in such cases, the reporting institution must weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of money laundering or financing of terrorism and consider whether to refuse to do any business with such customers.

8.2.6 The frequency of the ongoing CDD shall commensurate with the level of ML/TF risks posed by the customer based on the risk profile and nature of transactions.

8.2.7 The reporting institution is required to undertake a renewed CDD when:

(a) there is a suspicion of ML/TF risks; or

(b) there is a doubt about the veracity or adequacy of previously obtained identification data.

8.3 Risk-based Approach in Conducting CDD

8.3.1 A reporting institution must adopt a risk based approach in determining whether to apply a CDD or an enhanced CDD based on the customers’ background, transaction types or specific circumstances.

8.3.2 The following are circumstances of higher risk that a reporting institution should consider exercising greater scrutiny when approving the opening of an account and when conducting transactions:

(a) Customer risk factors:

- The business relationship is conducted in unusual circumstances.
- Non-resident customer.
- Legal persons or arrangements that are personal asset-holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Businesses that are cash-intensive.
- The ownership structure of a company appears unusual or excessively complex given the nature of the company’s business.
- High net worth individuals and entities.
- Persons from jurisdictions known for their high crime rates (e.g. drug producing, trafficking, smuggling).
- Businesses/activities identified by the FATF as having higher risk for ML/TF.
- Domestic PEPs.
- Persons entrusted with prominent function by international organisations.
- Legal arrangements that are complex.
- Any persons who match the ‘flag’ criteria of the reporting institution.

(b) Country or geographic risk factors:
- Countries having inadequate AML/CFT systems.
- Countries subject to sanctions, embargos or similar measures issued by international organisations such as the United Nations.
- Countries having significant levels of corruption or other criminal activities.
- Countries or geographic areas identified as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

(c) Product, service, transaction or delivery channel risk factors:
- Anonymous transactions (which may include cash transactions).
- Non-face-to-face business relationships or transactions.
- Payment received from multiple persons and/or countries that do not fit into the customer’s nature of business and risk profile.
- Payment received from unknown or unassociated third parties.

8.3.3 Subject to Paragraph 8.6 below, a reporting institution in identifying country and geographic risk factors, must refer to credible sources such as mutual evaluation reports, detailed assessment reports, follow up reports and other relevant reports published by international organisations such as the FATF, Asia Pacific Group on Money Laundering, United Nations, World Bank and International Monetary Fund.
Note:
A non-exhaustive list of websites that may be referred to in assessing the ML/TF risk exposure is published on the SC’s website.

8.4 Enhanced CDD measures

8.4.1 Upon determining a customer as “high risk”, a reporting institution must undertake enhanced CDD measures on the customer and, where applicable, the beneficial owner. These measures must include:

(a) obtaining additional information and verification on the customer and beneficial owner, particularly for non-face to face transactions (e.g. volume of assets and other information from public database);

(b) obtaining additional information on the intended level and nature of the business relationship;

(c) enquiring on the source of wealth and source of funds;

(d) updating on a more regular basis, the identification data of the customer and the beneficial owner;

(e) obtaining approval from the senior management before establishing (or continuing for existing customer) such business relationship with the customer; and

(f) conducting enhanced ongoing monitoring on the business relationship.

8.5 Politically Exposed Persons (PEPs)

8.5.1 The requirements set out in Paragraph 8.5 herein are also applicable to family members or close associates of PEPs.

8.5.2 A reporting institution is required to have in place a risk management system to determine whether a customer or a beneficial owner is a foreign PEP.

8.5.3 Upon determination that a customer or a beneficial owner is a foreign PEP, the requirements of enhanced CDD as set out in Paragraph 8.4 are automatically applicable.

8.5.4 A reporting institution is required to have in place reasonable measures to determine whether a customer or the beneficial owner is a domestic PEP or person entrusted with a prominent function by an international organisation. The reporting institution is required to assess the level of ML/TF risks posed by the business relationship with the domestic PEP or person entrusted with a prominent function.
by an international organisation based on sufficient and appropriate information gathered through publically available information or other reasonable means.

8.5.5 For a high risk domestic PEP or high risk person entrusted with a prominent function by an international organisation, the requirements of enhanced CDD as set out in Paragraph 8.4 are applicable.

8.5.6 For a domestic PEP or person entrusted with a prominent function by an international organisation that is assessed as low risk, the reporting institution may apply the standard CDD measures.

8.6 High Risk Countries

8.6.1 A reporting institution is required to conduct enhanced CDD for any business relationship and transaction with any person from countries identified by–

(a) the FATF as issued under the “FATF Public Statement” – on jurisdictions subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the ongoing and substantial ML/TF risks emanating from such jurisdictions; or

(b) the Government of Malaysia as having ongoing or substantial ML/TF risks.

8.6.2 In addition to the enhanced CDD measures required under Paragraph 8.6.1 above, a reporting institution is required to apply appropriate countermeasures, proportionate to the risk, for higher risk countries as follows:

(a) limiting business relationships or financial transactions with identified countries or persons located in the country concerned;

(b) where relevant, conduct enhanced external audit, by increasing the intensity and frequency, for branches and subsidiaries of the reporting institution or financial group, located in the country concerned; and

(c) conduct any other measures as may be specified by the SC.

8.6.3 For business relationship and transaction with any person from countries identified by–

(a) the FATF as issued under the “FATF Public Statement”- on jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies; or

(b) the Government of Malaysia as having strategic AML/ CFT deficiencies and have not made sufficient progress in addressing the deficiencies

the reporting institution is required to assess the risk and where the risk is identified as higher risk, the reporting institution is required to conduct enhanced CDD as set out in Paragraph 8.4 above.
8.7 **Reliance on Third Parties to Conduct CDD**

8.7.1 A reporting institution may rely on a third party to conduct CDD at the point of establishing a business relationship. However, the ultimate responsibility and accountability of such CDD measures shall remain with the reporting institution.

8.7.2 A reporting institution shall have in place internal policies and procedures to mitigate the risks when relying on a third party, including those from foreign jurisdictions. However, the reporting institution must ensure that the third party adequately applies the FATF Recommendations in determining the extent to which reliance could be placed on such third party.

8.7.3 A reporting institution is prohibited from relying on a third party located in higher risk countries that have been identified as having ongoing or substantial ML/TF risks.

8.7.4 The relationship between a reporting institution and the third party relied upon to conduct the CDD, shall be governed by an arrangement that clearly specifies the rights, responsibilities and expectations of all parties. At the minimum, the reporting institution must be satisfied that the third party—

(a) can obtain immediately the necessary information concerning the CDD in Paragraph 8.1 above;

(b) has adequate CDD and enhanced CDD processes;

(c) has measures in place for record keeping requirements;

(d) can provide the CDD or enhanced CDD information and provide copies of the relevant documentation immediately upon request;

(e) is properly regulated and supervised by the respective authorities; and

(f) complies with the provisions of any applicable laws.

8.7.5 In addition to the requirements set out in Paragraph 8.7.4 above, a reporting institution that relies on a third party that is part of the same group is subject to the following conditions:-

(a) the group applies CDD and record keeping requirements and AML/CFT programmes in line with these Guidelines;

(b) the implementation of those CDD and record keeping requirements and AML/CFT programmes are supervised at a group level by the relevant supervisory authority; and

(c) any higher country risk is adequately mitigated by the financial group’s AML/CFT policies.
8.8  Failure to Satisfactorily Complete CDD

8.8.1 A reporting institution must not commence any business relation, or execute any transaction, or in the case of existing customers, must terminate such business relationship, if the customer fails to comply with the CDD requirements.

8.8.2 A reporting institution must also consider lodging a STR in relation to such customer with the FIED.

9.  GROUP-WIDE ML/TF PROGRAMMES

9.1 Where applicable, a reporting institution is required to implement appropriate group-wide ML/TF programmes appropriate to its holding company, branches and majority-owned subsidiaries. Such ML/TF programmes must include:

(a) policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

(b) the provision at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and

(c) adequate safeguards on the confidentiality and use of information exchanged.
PART IV: RETENTION OF RECORDS

10. RECORD KEEPING

10.1 A reporting institution must keep record of all transactions and ensure they are up to-date and relevant. The records must at least include the following information for each transaction:

(a) documents relating to the identification of the customer in whose name the account is opened or transaction is executed;

(b) the identification of the beneficial owner or the person on whose behalf the account is opened or transaction is executed;

(c) records of the relevant account pertaining to the transaction executed;

(d) the type and details of transaction involved;

(e) the origin and the destination of the funds, where applicable; and

(f) such other information as the SC and BNM may specify in writing.

10.2 A reporting institution is required to maintain records for a period of at least seven (7) years from:

(a) in the case of record obtained through the CDD and enhanced CDD process, the date the account is closed; or

(b) in the case of transaction records, the date the transaction is completed or terminated.

10.3 A reporting institution must retain a record beyond the retention period provided in Paragraph 10.2 above, if the record is in relation to:

(a) a STR that has been lodged to FIED;

(b) a transaction that is subject to an ongoing investigation by any law enforcement agency; or

(c) a transaction that is subject to prosecution in court,

until it is confirmed that the case is closed or records are no longer required.

10.4 A reporting institution must retain, maintain and update the relevant records (including CDD records) in such a way that:

(a) the relevant law enforcement agencies, and internal and external auditors of the reporting institution will be able to judge reliably the reporting institution's transactions and its compliance with the AMLATFA;

(b) any transaction effected via the reporting institution can be reconstructed;
and

(c) the reporting institution can satisfy within a reasonable time any enquiry or order from the relevant law enforcement agencies as to the disclosure of such relevant record.
PART V: SUSPICIOUS TRANSACTIONS

11. REPORTING OF SUSPICIOUS TRANSACTIONS

11.1 A reporting institution must clarify the economic background and purpose of any transaction or business relationship if it appears unusual in relation to the reporting institution’s knowledge of the customer, or if the economic purpose or legality of the transaction is not immediately clear. Special attention should also be paid to all complex and unusual patterns of transaction.

11.2 A reporting institution must also consider whether the transactions involve a number of factors which when taken together may raise a suspicion that the transactions may be connected with certain unlawful activities.

11.3 In considering whether a transaction is suspicious, a reporting institution must take into account, among others, the following factors:

(a) the nature of, or unusual circumstances, surrounding the transaction;
(b) the known business background of the person conducting the transaction;
(c) the production of seemingly false identification in connection with any transaction, the use of aliases and a variety of similar but different addresses;
(d) the behaviour of the person or persons conducting the transactions; and
(e) the person or group of persons with whom they are dealing.

11.4 If in bringing together all relevant factors, a reporting institution (including its licensed representatives and employees) has reasonable grounds to suspect that the transaction or the funds utilized are the proceeds of an unlawful activity or related to terrorism financing, such transactions should be reported immediately to the FIED via a lodgment of a STR.

11.5 Where the reporting institution decides that there are no reasonable grounds for suspicion to warrant a lodgment of a STR, the reporting institution must establish the grounds for such decision. In this regard, the compliance officer must ensure that the reporting institution’s decision together with all supporting documentary evidence is recorded and maintained.

11.6 The reporting institution must ensure that the compliance officer maintains a complete file on all internal STRs received by him from the reporting institution’s employees attached with supporting documentary evidence.

11.7 The fact that a STR may have been filed with the FIED previously should not preclude the reporting institution from lodging a fresh STR if a new suspicion arises.

11.8 A reporting institution is required to report all suspicious transactions, including attempted transactions, regardless of the amount of the
transaction. Reporting institutions should be aware that in some cases, suspicion may be formed after a considerable time from the date of the transaction, in view of subsequent additional information.

11.9 It is the obligation of the licensed representative or employee of the reporting institution to alert the reporting institution of a suspicious transaction upon becoming suspicious when dealing with customers.

11.10 STRs must be lodged to the FIED in accordance with the method as provided in Appendix 1 herein.

11.11 A reporting institution is required to have in place strong mechanisms for reporting suspicious transactions, including having an appointed AML/CFT compliance officer, and where appropriate, having a unit primarily responsible for complying with the AML/CFT requirements on reporting of suspicious transactions.

11.12 The compliance officer in a reporting institution should act as a central reference point within the organisation for all AML/CFT matters, including:

(a) analysing identified suspicious transactions;

(b) reviewing regularly exception reports of large or irregular transactions generated by the reporting institution’s internal system or ad hoc reports made by front-line employees; and

(c) lodging of STRs to the FIED.

11.13 The compliance officer has the sole discretion and independence to report suspicious transactions.

11.14 The board of directors must ensure that the compliance officer has the necessary authority, resources and support to discharge his obligation independently and effectively in complying with the reporting institution’s compliance policies and procedures on AML/CFT, particularly on reporting suspicious transactions.

11.15 When required by FIED, a reporting institution must provide additional information and documentation and respond promptly to any further enquiries with regard to the STR lodged.

11.16 A reporting institution must also ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preservation of secrecy.

11.17 Where a reporting institution forms a suspicion of ML/TF and reasonably believes that performing the CDD process would tip off the customer, the reporting institution is permitted not to pursue the CDD process and is required to file a STR.
11.18 For the avoidance of doubt, unless permitted by law, a reporting institution and its directors, officers and employees are prohibited from disclosing the fact that a STR or related information is being filed with the FIED.

Note:
Some examples of suspicious transactions are published on SC’s website. The list is non exhaustive and only provides examples of ways in which money may be laundered through the capital market.

12. CONFIDENTIALITY OF REPORTING

12.1 It shall be an offence to disclose to anyone any information that a suspicion has been formed or that information has been communicated to the FIED and the SC or to infer that these have occurred.

12.2 A person does not commit an offence under Paragraph 12.1 above, where such a disclosure is made pursuant to the provisions of the AMLATFA.

12.3 No civil, criminal or disciplinary proceedings shall be brought against a person who:

(a) discloses or supplies any information in any report made under the AMLATFA; or

(b) supplies any information in connection with such a report, whether at the time the report is made or afterwards;

unless the information is disclosed or supplied in bad faith.
PART VI: COMPLIANCE AND TRAINING PROGRAMMES

13. INTERNAL PROGRAMMES, POLICIES, PROCEDURES AND CONTROLS

13.1 Pursuant to the provisions of the AMLATFA, a reporting institution shall adopt, develop and implement internal programmes, policies, procedures and controls having regard to the ML/TF risks and size of business. These programmes shall include:

(a) procedures to ensure high standards of integrity of its directors, employees or persons acting on behalf of the reporting institution, and adopt a screening system to evaluate the personnel when hiring;

(b) regular independent audit function to check on the compliance and effectiveness of the reporting institution’s AML/CFT framework in relation to the AMLATFA and provisions of these Guidelines. In this regard, such audit findings and any necessary corrective measures to be undertaken must be tabled to the board of directors;

(c) effective internal control systems to assess, profile and address ML/TF issues; and

(d) structured and on-going training programmes for directors and employees to enhance compliance with the reporting institution’s policies and procedures on AML/CFT.

13.2 The training programmes for the directors and employees must be structured according to their level of responsibilities and conducted on a regular basis. This is to ensure that they are kept up-to-date with the latest developments and be reminded of their responsibilities.

13.3 A reporting institution shall also designate compliance officers at management level in each of its branch, who will be responsible for the application of the AML/CFT internal programmes, policies and procedures.

13.4 It is imperative that the compliance officer appointed by a reporting institution has the necessary knowledge, expertise and the required authority to discharge his responsibilities effectively, including knowledge on the relevant laws and regulations and the latest AML/CFT developments. To this end, a reporting institution should encourage its compliance officers to pursue professional qualifications in AML/CFT, so that they are able to carry out their obligations effectively.

13.5 A reporting institution must also ensure that the roles and responsibilities of the compliance officer are clearly defined and documented. The roles and responsibilities of a compliance officer include ensuring the following:

(a) the reporting institution’s compliance with the AML/CFT requirements;

(b) the appropriate AML/CFT policies and procedures, including customer identification, customer due-diligence, reporting of suspicious transactions, and compliance and training programmes are implemented effectively;
(c) the AML/CFT policies and procedures are regularly assessed and kept up-to-date to ensure that they are effective and sufficient to address any changes in ML/TF trends;

(d) timely reporting of the risk assessment and risk mitigation measures to the board of directors;

(e) all employees are aware of the reporting institution’s AML/CFT framework;

(f) internally generated STRs by the branch/subsidiary compliance officers are appropriately evaluated and recorded before submission to the FIED;

(g) the channel of communication from the respective employees to the branch/subsidiary compliance officer and subsequently to the compliance officer is secured and that information is kept confidential; and

(h) the ML/TF risks associated with new products and services or arising from the reporting institution’s operational changes, including the introduction of new technology and processes, are identified and are brought to the attention of the board of directors.

13.6 Notwithstanding the duties of the compliance officer, the ultimate responsibility for proper supervision, reporting and compliance pursuant to AMLATFA and these Guidelines remains with the reporting institution and its board of directors.

13.7 An independent audit to assess the overall effectiveness of the reporting institution’s AML/CFT framework referred to in Paragraph 13.1(b) above, may be performed by either an external audit firm or the reporting institution’s internal auditor.
PART VII: COMBATING TERRORISM FINANCING

14. IDENTIFICATION AND DESIGNATION

14.1 A reporting institution is required to keep itself updated with the various resolutions passed by the United Nations Security Council (UNSC) on counter terrorism measures, in particular, the UNSC Resolutions 1267 (1999), 1373 (2001), 1988 (2011) and 1989 (2011), which require sanctions against individuals and entities belonging or related to the Taliban and the al-Qaeda organisations.

14.2 In ensuring efficient detection of suspected financing of terrorism, the reporting institution should maintain a database of names and particulars of listed persons in the UN Consolidated List and such orders as may be issued under Sections 66B and 66C of the AMLATFA by the Minister of Home Affairs (collectively referred to as “listed persons”).

\[\text{Note:} \]
The updated and consolidated UNSC List can be obtained at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

14.3 A reporting institution must ensure that the information contained in the database is updated and relevant, and made easily accessible to its employees at the head office, branch and subsidiary.

14.4 A reporting institution must conduct checks on the names of potential and new customers, as well as regular checks on the names of existing customers, against the names in the database. If there is any name match, the reporting institution must take reasonable and appropriate measures to verify and confirm the identity of its customer. Upon such confirmation, the reporting institution must immediately:

(a) freeze without delay the customer’s fund or block the transaction, if it is an existing customer;

(b) reject the customer, if the transaction has not commenced;

(c) lodge a STR with the FIED; and

(d) inform the SC.

14.5 A reporting institution is required to submit a STR when there is an attempted transaction by any of the listed persons.

14.6 A reporting institution must ascertain potential matches with the UN Consolidated List to confirm whether they are true matches to eliminate any "false positives". The reporting institution must make further enquiries from the customer or counter-party (where relevant) to assist in determining whether the match is a true match.
Appendix 1 – Submission of Suspicious Transaction Report

1. A STR should be lodged with the FIED using the prescribed suspicious transaction report form which is available for download on BNM’s website.

2. The lodgment of the STR may be made by any of the following means:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
</table>
| Mail    | The physical forms should be placed in a sealed envelope and addressed to the following:  
  Director  
  Financial Intelligence and Enforcement Department  
  Bank Negara Malaysia  
  Jalan Dato’ Onn  
  50450 Kuala Lumpur  
  (To be opened by addressee only) |
| Fax     | 03-26933625 |
| E-mail  | str@bnm.gov.my |
| FIED’s Financial Intelligence System (FINS), where and if available | [https://bnmapp.bnm.gov.my/fins2](https://bnmapp.bnm.gov.my/fins2) |