



**BANK NEGARA MALAYSIA**  
CENTRAL BANK OF MALAYSIA

**Anti-Money Laundering and  
Counter Financing of Terrorism  
(AML/CFT) – Electronic Money and Non-  
Bank Affiliated Charge & Credit Card  
(Sector 4)**

## Table of Contents

<b>PART A</b>	<b>OVERVIEW</b>	<b>1</b>
1.	Introduction	1
2.	Objective	2
3.	Scope	2
4.	Legal Provisions	3
5.	Applicability	3
6.	Effective Date	4
7.	Compliance Date	4
8.	Policies Superseded	4
9.	Relationship with Existing Policies	5
10.	Definition and Interpretation	5
<b>PART B</b>	<b>AML/CFT REQUIREMENTS</b>	<b>17</b>
11.	Applicability to Foreign Branches and Subsidiaries	17
12.	Risk-Based Approach Application	18
13.	Customer Due Diligence (CDD)	20
14.	Politically Exposed Persons (PEPs)	33
15.	New Products and Business Practices	34
16.	Wire transfer	35
17.	Money or Value Transfer Services (MVTs)	39
18.	Reliance on Third Parties	40
19.	Non Face-to-Face Business Relationship	42
20.	Higher Risk Countries	43
21.	Failure to Satisfactorily Complete CDD	44
22.	Management Information System	44
23.	Record Keeping	45
24.	AML/CFT Compliance Programme	46
25.	Suspicious Transaction Report	56
26.	Combating the Financing of Terrorism	61
27.	Non-Compliance	63

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 1 of 64
------------------	---	---	--------------

## **PART A OVERVIEW**

### **1. Introduction**

- 1.1 Money laundering and terrorism financing (ML/TF) continues to be an on-going threat which has the potential to adversely affect the country's reputation and investment climate, which may lead to economic and social consequences. The globalisation of the financial services industry and advancement in technology has posed challenges to regulators and law enforcement agencies as criminals have become more sophisticated in utilising reporting institutions to launder illicit funds and use them as conduits for ML/TF activities.
- 1.2 Since the formation of the National Coordination Committee to Counter Money Laundering (NCC), efforts have been undertaken to effectively enhance the AML/CFT compliance framework of reporting institutions resulting in the introduction of the Standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism (UPW/GP1) and the relevant Sectoral Guidelines. While these efforts have addressed the ML/TF risks and vulnerabilities, there is a need to continuously assess the effectiveness of our AML/CFT framework to ensure that it continues to evolve in line with developments in international standards and the global environment.
- 1.3 Prior to 2012, the Financial Action Task Force (FATF) undertook a comprehensive review of the 40+9 Recommendations, which aimed at bringing the Recommendations more up-to-date with the evolving financial, law enforcement and regulatory environment besides addressing new and emerging threats. The 2012 revision, the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (FATF 40 Recommendations),

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 2 of 64
------------------	---	---	--------------

sought to clarify and strengthen many of its existing obligations as well as to reduce duplication in the Recommendations. One of the new Recommendations introduced is on the obligation of countries to adopt a risk-based approach in identifying, assessing and understanding the countries' ML/TF risks, which places further expectation on reporting institutions to assess and mitigate ML/TF risks.

- 1.4 Premised on the foregoing paragraphs, reporting institutions must conduct their business in conformity with high ethical standards and be on guard against undertaking any business transaction that is or may be connected with or may facilitate ML/TF. These underlying principles become the basis upon which the integrity and soundness of the Malaysian financial system must be safeguarded.

## **2. Objective**

- 2.1 This document is formulated in accordance with the provisions of the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA) and the FATF 40 Recommendations and is intended to ensure that reporting institutions understand and comply with the requirements and obligations imposed on them.

## **3. Scope**

- 3.1 This document sets out the:
- (a) obligations of reporting institutions with respect to the requirements imposed under the AMLATFA;
  - (b) requirements imposed on reporting institutions in implementing a comprehensive risk-based approach in managing ML/TF risks; and

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 3 of 64
------------------	---	---	--------------

- (c) roles of the reporting institutions' Board of Directors and Senior Management (or its equivalent) in putting in place the relevant AML/CFT measures.

#### **4. Legal Provisions**

- 4.1 This document is issued pursuant to:
- (a) Sections 13, 14, 15, 16, 17, 18, 19, 20, 66E and 83 of the AMLATFA;
  - (b) Section 47(1) and in particular, Paragraph 47(2)(h) of the Financial Services Act 2013 (FSA);
  - (c) Section 57(1) and in particular, Paragraph 57(2)(h) of the Islamic Financial Services Act 2013 (IFSA); and
  - (d) Section 74 of the Money Services Business Act 2011 (MSBA).

#### **5. Applicability**

- 5.1 This document is applicable to:
- (a) reporting institutions in the First Schedule to the AMLATFA:
    - (i) issuers of charge cards and credit cards which are not affiliated with any licensed bank under the FSA, any licensed Islamic bank under the IFSA and prescribed institutions licensed under the Development Financial Institutions Act 2002 (DFIA);
    - (ii) issuers of electronic money, a designated payment instrument as prescribed in the Financial Services (Designated Payment Instruments) Order 2013;
    - (iii) issuers of electronic money who are also licensed as money service business under MSBA; and
    - (iv) any other persons as specified by Bank Negara Malaysia:

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 4 of 64
------------------	---	---	--------------

- (b) branches and subsidiaries of reporting institutions referred to in Paragraph 5.1(a); and
- (c) all products and services offered by reporting institutions referred to in Paragraph 5.1(a).

5.2 Where reporting institutions are subject to more than one document relating to AML/CFT matters issued pursuant to section 83 of the AMLATFA, the more stringent requirement shall apply.

## **6. Effective Date**

6.1 This document comes into effect on 15 September 2013.

## **7. Compliance Date**

7.1 Compliance to the requirements outlined in this document shall take effect immediately, unless otherwise specified by Bank Negara Malaysia.

## **8. Policies Superseded**

- 8.1 This document supersedes:
- (a) the Standard Guidelines on Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) (UPW/GP1) issued in November 2006 (amended February 2009);
  - (b) the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Sectoral Guidelines 4 for Non-Bank Affiliated Charge and Credit Card Issuers(UPW/GP1[4]) issued in April 2007; and
  - (c) the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Sectoral Guidelines 9 for Electronic Money Issuers (UPW/GP1[9]) issued in August 2009.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 5 of 64
------------------	---	---	--------------

## 9. Relationship with Existing Policies

9.1 This document shall be read together with other documents issued by Bank Negara Malaysia relating to compliance with AML/CFT requirements.

## 10. Definition and Interpretation

10.1 The terms and expressions used in this document shall have the same meanings assigned to it under the AMLATFA, FSA and IFSA, as the case may be, unless otherwise defined in this document.

10.2 For the purpose of this document:

“accurate”	Refers to information that has been verified for accuracy.
“beneficial owner”	<p>Refers to any 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 those natural persons who exercise ultimate effective control over a legal person or arrangement.</p> <p>Reference to “ultimately owns or control” or “ultimate effective control” refers to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.</p>

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 6 of 64
------------------	---	---	--------------

“beneficiary”	<p>Depending on the context:</p> <p>In trust law, a beneficiary refers to the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period.</p> <p>In wire transfer, refers to the natural or legal person or legal arrangement identified by the originator as the receiver of the requested wire transfer.</p> <p>In clubs, societies and charities, refers to the natural persons, or groups of natural persons who receive charitable, humanitarian or other types of services of the clubs, societies and charities.</p>
---------------	---



BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 7 of 64
------------------	---	---	--------------

“beneficiary institutions”	Refers to the institution which receives the wire transfer from the ordering institution directly or through an intermediary institution and makes the fund available to the beneficiary.
“Board of Directors”	Refers to a governing body or a group of directors. A director includes any person who occupies a position of a director, however styled, of a body corporate or unincorporated, and includes in the case of: (a) a corporation, the same meaning assigned to it in sub-section 4(1) of the Companies Act 1965; (b) a sole proprietorship, means the sole proprietor; and (c) a partnership, means the senior or equity partners.
“Core Principles”	Refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, Objectives and Principles for Securities Regulation issued by the International Organisation of Securities Commissions, and the Insurance Core Principles issued by the International Association of Insurance Supervisors.
“cover payment”	Refers to a wire transfer that combines a payment message sent directly by the ordering institution to the beneficiary institution where the routing of the funding instruction (the cover) is carried out or performed through one or more intermediary institutions.
“cross-border wire transfer”	Refers to any wire transfer where the ordering institution and beneficiary institution are located in different

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 8 of 64
------------------	---	---	--------------

	countries. This term also refers to any chain of wire transfer in which at least one of the institutions involved is located in a different country.
“customer”	Refers to both account holder and non-account holder. The term also refers to a client.
“customer due diligence”	Refers to any measures undertaken pursuant to section 16 of the AMLATFA.
“domestic wire transfers”	Refers to any wire transfer where the ordering institution and beneficiary institution are located in Malaysia. This term therefore refers to any chain of wire transfer that takes place entirely within the borders of Malaysia, even though the system used to transfer the payment message may be located outside Malaysia.
“financial group”	Refers to a group that consists of a holding company incorporated in Malaysia or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subjected to AML/CFT policies and procedures at the group level.
“financial holding company”	Refers to a company approved as a financial holding company under section 112 of the FSA or section 124 of the IFSA, as the case may be.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 9 of 64
------------------	---	---	--------------

“Government-linked company”	Refers to a corporate entity that may be private or public (listed on a stock exchange) where the government owns an effective controlling interest, or is owned by any corporate entity where the government is a shareholder.
“G”	Denotes “Guidance” which may consist of such information, advice or recommendation intended to promote common understanding and sound industry practices which are encouraged to be adopted.
“higher risk”	<p>Refers to circumstances where the reporting institutions assess the ML/TF risks as higher, taking into consideration, and not limited to the following factors:</p> <p>(a) Customer risk factors:</p> <ul style="list-style-type: none"> <li>• the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the reporting institution and the customer);</li> <li>• non-resident customer;</li> <li>• legal persons or arrangements that are personal asset-holding vehicles;</li> <li>• companies that have nominee shareholders or shares in bearer form;</li> <li>• businesses that are cash-intensive;</li> <li>• the ownership structure of the company appears unusual or excessively complex given the nature of the company’s business;</li> <li>• high net worth individuals;</li> <li>• persons from locations known for their high rates</li> </ul>

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 10 of 64
------------------	---	---	---------------

	<p>of crime (e.g. drug producing, trafficking, smuggling);</p> <ul style="list-style-type: none"> <li>• businesses or activities identified by the FATF as having higher risk for ML/TF;</li> <li>• legal arrangements that are complex (e.g. trust, nominee); and</li> <li>• persons who match the red flag criteria of the reporting institutions.</li> </ul> <p>(b) Country or geographic risk factors:</p> <ul style="list-style-type: none"> <li>• countries having inadequate AML/CFT systems;</li> <li>• countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;</li> <li>• countries having significant levels of corruption or other criminal activities; and</li> <li>• countries or geographic areas identified as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.</li> </ul> <p>In identifying countries and geographic risk factors, reporting institutions may 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 United Nations.</p>
--	--

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 11 of 64
------------------	---	---	---------------

	<p>(c) Product, service, transaction or delivery channel risk factors:</p> <ul style="list-style-type: none"> <li>• anonymous transactions (which may include cash);</li> <li>• non face-to-face business relationships or transactions;</li> <li>• payment received from multiple persons and/or countries that do not fit into the person’s nature of business and risk profile; and</li> <li>• payment received from unknown or un-associated third parties.</li> </ul>
“higher risk countries”	Refers to countries that are listed by FATF on its Public Statement or the Government of Malaysia, with either on-going or substantial ML/TF risks or strategic AML/CFT deficiencies that pose a risk to the international financial system.
“home supervisor”	Refers to Bank Negara Malaysia, Securities Commission and Labuan Financial Services Authority.
“intermediary institution”	Refers to the institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution.
“international organisations”	Refers to entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 12 of 64
------------------	---	---	---------------

	<p>are not treated as residential institutional units of the countries in which they are located. Examples of international organisations include the following:</p> <ul style="list-style-type: none"> <li>(a) United Nations and its affiliated international organisations;</li> <li>(b) regional international organisations such as the Association of Southeast Asian Nations, the Council of Europe, institutions of the European Union, the Organisation for Security and Co-operation in Europe and the Organization of American States;</li> <li>(c) military international organisations such as the North Atlantic Treaty Organization; and</li> <li>(d) economic organisations such as the World Trade Organization.</li> </ul>
“legal arrangement”	Refers to express trusts or other similar legal arrangements.
“legal person”	Refers to any entities other than natural persons that can establish a permanent customer relationship with a reporting institution or otherwise own property. This includes companies, bodies corporate, foundations, partnerships, or associations and other similar entities.
“money services business”	Refers to the definition under the Money Services Business Act 2011.
“money or value transfer services	Refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 13 of 64
------------------	---	---	---------------

(MVTs)”	stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTs provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods.
“ordering institution”	Refers to the institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
“originator”	Refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering institution to perform the wire transfer.
“person”	Includes a body of persons, corporate or unincorporate.
“politically exposed persons (PEPs)”	<p>Refers to:</p> <ul style="list-style-type: none"> <li>(a) foreign PEPs – individuals who are or who have been entrusted with prominent public functions by a foreign country. For example, Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials;</li> <li>(b) domestic PEPs – individuals who are or have been entrusted domestically with prominent public</li> </ul>

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 14 of 64
------------------	---	---	---------------

	<p>functions. For example Heads of State or Government, senior politicians, senior government, judiciary or military officials, senior executives of state owned corporations and important political party officials; or</p> <p>(c) persons who are or have been entrusted with a prominent function by an international organisation which refers to members of senior management. For example, directors, deputy directors and members of the board or equivalent functions.</p> <p>The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.</p>
“S”	Denotes a “Standard”, requirement or specification that must be complied with. Failure to comply may result in one or more enforcement actions.
“satisfied”	Where reference is made to a reporting institution being “satisfied” as to a matter, the reporting institution must be able to justify its assessment to the supervisory authority.
“Senior Management”	Refers to any person(s) having authority and responsibility for planning, directing or controlling the activities of a reporting institution including the management and administration of a reporting institution.



BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 15 of 64
------------------	---	---	---------------

“serial payment”	Refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering institution to the beneficiary institution directly or through one or more intermediary institutions (e.g. correspondent banks).
“straight - through processing”	Refers to payment transactions that are conducted electronically without the need for manual intervention.
“third parties”	<p>Refers to reporting institutions that are supervised by a relevant competent authority and that meet the requirements under Paragraph 18 on Reliance of Third Parties, namely persons or businesses who are relied upon by the reporting institution to conduct the customer due diligence process.</p> <p>This reliance on third parties often occurs through introductions made by another member of the same financial group or by another financial institution. It may also occur in business relationships between insurance companies and insurance brokers or between mortgage providers and brokers. Those third parties include foreign regulated financial institutions, insurance companies and brokers.</p> <p>This definition does not include outsourcing or agency relationships because the outsourced person or agent is regarded as synonymous with the reporting institution.</p>

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 16 of 64
------------------	---	---	---------------

“unique transaction reference number”	Refers to a combination of letters, numbers, or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.
“wire transfer”	Refers to any transaction carried out on behalf of an originator through an institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary institution, irrespective of whether the originator and the beneficiary are the same person.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 17 of 64
------------------	---	---	---------------

## **PART B AML/CFT REQUIREMENTS**

### **11. Applicability to Foreign Branches and Subsidiaries**

- S** 11.1 Reporting institutions are required to closely monitor the reporting institution's foreign branches or subsidiaries operating in jurisdictions with inadequate AML/CFT laws and regulations as highlighted by the FATF or the Government of Malaysia.
- S** 11.2 Reporting institutions are required to ensure that their foreign branches and subsidiaries apply AML/CFT measures in a manner that is consistent with the AML/CFT requirements in Malaysia. Where the minimum AML/CFT requirements of the host country are less stringent than those of Malaysia, the reporting institution must apply Malaysia's AML/CFT requirements, to the extent that host country laws and regulations permit.
- S** 11.3 If the host country does not permit the proper implementation of AML/CFT measures in a manner that is consistent with the AML/CFT requirements in Malaysia, the reporting institution is required to apply appropriate additional measures to manage the ML/TF risks, and report to their supervisors in Malaysia on the AML/CFT gaps and additional measures implemented to manage the ML/TF risks arising from the identified gaps.
- G** 11.4 In addition, the reporting institution may consider ceasing the operations of the said branch or subsidiary that is unable to put in place the necessary mitigating control as required under Paragraph 11.3.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 18 of 64
------------------	---	---	---------------

## 12. Risk-Based Approach Application

### 12.1 Risk Management Functions

- S** 12.1.1 In the context of “Risk-Based Approach”, the intensity and extensiveness of risk management functions shall be proportionate to the nature, scale and complexity of the reporting institution’s activities and ML/TF risk profile.

### 12.2 Risk Assessment

- S** 12.2.1 Reporting institutions are required to take appropriate steps to identify, assess and understand their ML/TF risks in relation to their customers, countries or geographical areas and products, services, transactions or delivery channels.
- S** 12.2.2 In assessing ML/TF risks, reporting institutions are required to have the following processes in place:
- (a) documenting their risk assessments and findings;
  - (b) considering all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;
  - (c) keeping the assessment up-to-date through a periodic review; and
  - (d) having appropriate mechanisms to provide risk assessment information to the supervisory authority.
- S** 12.2.3 Reporting institutions are required to conduct additional assessment as and when required by the supervisory authority.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 19 of 64
------------------	---	---	---------------

- G** 12.2.4 Reporting institutions may be guided by the results of the National Risk Assessment issued by Bank Negara Malaysia in conducting their own risk assessments.

### 12.3 Risk Control and Mitigation

- S** 12.3.1 Reporting institutions are required to:
- (a) have policies, controls and procedures to manage and mitigate ML/TF risks that have been identified;
  - (b) monitor the implementation of those policies, controls, procedures and to enhance them if necessary; and
  - (c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

### 12.4 Risk Profiling

- S** 12.4.1 Reporting institutions are required to conduct risk profiling on their customers.
- S** 12.4.2 A risk profile must consider the following factors:
- (a) customer risk (e.g. resident or non resident, type of customers, occasional or one-off, legal person structure, types of PEP, types of occupation);
  - (b) country or geography (e.g. location of business, origin of customers);
  - (c) products, services, transactions or delivery channels (e.g. cash-based, face-to-face, non face-to-face, cross-border); and
  - (d) any other information suggesting that the customer is of higher risk.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 20 of 64
------------------	---	---	---------------

**S** 12.4.3 The risk control and mitigation measures implemented by reporting institutions shall commensurate with the risk profile of a particular customer or type of customer.

**S** 12.4.4 Upon the initial acceptance of the customer, reporting institutions are required to regularly review and update the customer's risk profile based on their level of ML/TF risks.

### **13. Customer Due Diligence (CDD)**

#### **13.1 When CDD is required**

**S** 13.1.1 Reporting institutions are required to conduct CDD on the customer and the person conducting the transaction, when:

- (a) establishing business relations, where applicable;
- (b) when the customer's purse size is equivalent to RM5,000 and above, in relation to electronic money issuers;
- (c) when customer conduct any reload, usage or withdrawal transaction amounting to RM3,000 and above, in relation to electronic money issuers;
- (d) providing wire transfer services;
- (e) it has any suspicion of ML/TF, regardless of the amount;  
or
- (f) it has any doubt about the veracity or adequacy of previously obtained information.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 21 of 64
------------------	---	---	---------------

## 13.2 What is required

**S**

### 13.2.1 Reporting institutions are required to:

- (a) identify the customer and verify that customer's identity using reliable, independent source 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 the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a 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 and intended nature of the business relationship.

**S**

13.2.2 In conducting CDD, reporting institutions are required to comply with the requirements for combating the financing of terrorism under Paragraph 26.

## 13.3 Timing of Verification

**S**

13.3.1 Reporting institutions are required to verify the identity of the customer and beneficial owner before, or during, the course of establishing a business relationship.

**G**

13.3.2 In certain circumstances where the ML/TF risks are assessed as low and verification is not possible at the point of establishing the business relationship, the reporting institution may complete verification after the establishment

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 22 of 64
------------------	---	---	---------------

of the business relationship to allow some flexibilities for its customer and beneficial owner to furnish the relevant documents.

- S** 13.3.3 Where delayed verification applies, the following conditions must be satisfied:
- (a) this occurs as soon as reasonably practicable;
  - (b) the delay is essential so as not to interrupt the reporting institution's normal conduct of business;
  - (c) the ML/TF risks are effectively managed; and
  - (d) there is no suspicion of ML/TF risks.
- S** 13.3.4 The term "reasonably practicable" under Paragraph 13.3.3(a) shall not be later than ten working days or any other period as may be specified by Bank Negara Malaysia.
- S** 13.3.5 Reporting institutions are required to adopt risk management procedures relating to the conditions under which the customer may utilise the business relationship prior to verification and procedures to mitigate or address the risk of delayed verification.
- G** 13.3.6 The measures that reporting institutions may take to manage such risks of delayed verification may include limiting the number, types and/or amount of transactions that can be performed.



BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 23 of 64
------------------	---	---	---------------

### 13.4 Specific CDD Measures

#### *Individual Customer and Beneficial Owner*

- S** 13.4.1 In conducting CDD on an individual customer and beneficial owner, the reporting institution is required to obtain at least the following information:
- (a) full name;
  - (b) National Registration Identity Card (NRIC) number or passport number or reference number of any other official documents bearing the photograph of the customer or beneficial owner;
  - (c) residential and mailing address;
  - (d) date of birth;
  - (e) nationality;
  - (f) contact number (home, office or mobile); and
  - (g) purpose of transaction.
- S** 13.4.2 In the case of issuers of charge cards and credit cards which are not affiliated with any licensed bank under the FSA and licensed Islamic banks under the IFSA, the relevant reporting institution is further required to obtain the following information:
- (a) occupation type; and
  - (b) name of employer or nature of self-employment/nature of business.
- G** 13.4.3 Reporting institutions can accept any other official documents bearing the photograph of the customer or beneficial owner, as the case may be, under Paragraph 13.4.1(b) provided that the reporting institution can be satisfied with the authenticity of the documents which

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 24 of 64
------------------	---	---	---------------

contain the necessary required information.

**S** 13.4.4 Reporting institutions shall verify the documents referred to under Paragraph 13.4.1(b) by requiring the customer or beneficial owner, as the case may be, to furnish the original document and make a copy of the said document. However, where biometric identification method is used, verification is deemed to be satisfied.

**S** 13.4.5 Where there is any doubt, reporting institutions are required to request the customer or beneficial owner, as the case may be, to produce other supporting official identification documents bearing their photographs, issued by an official authority or an international organisation, to enable their identity to be ascertained and verified.

*Legal Persons*

**S** 13.4.6 For customers that are legal persons, reporting institutions are required to understand the nature of the customer's business, its ownership and control structure.

**S** 13.4.7 Reporting institutions are required to identify the customer and verify its identity through the following information:

- (a) name, legal form and proof of existence, such as Memorandum/Article/Certificate of Incorporation/Partnership (certified true copies/duly notarised copies, may be accepted) or any other reliable references to verify the identity of the customer;
- (b) the powers that regulate and bind the customer such as directors' resolution, as well as the names of relevant

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 25 of 64
------------------	---	---	---------------

- persons having a senior management position; and
- (c) the address of the registered office and, if different, a principal place of business.

**S**

13.4.8 Reporting institutions are required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

- (a) the identity of the natural person(s) (if any) who ultimately has a controlling ownership interest in a legal person. At a minimum, this includes the following:
- (i) identification document of Directors/ Shareholders with equity interest of more than twenty five percent/Partners (certified true copy/duly notarised copies or the latest Form 24 and 49 as prescribed by the Companies Commission of Malaysia or equivalent documents for Labuan companies or foreign incorporations, or any other equivalent documents for other types of legal person are acceptable);
  - (ii) authorisation for any person to represent the company or business either by means of a letter of authority or directors' resolution; and
  - (iii) relevant documents such as NRIC for Malaysian/permanent resident or passport for foreigner, to identify the identity of the person authorised to represent the company or business in its dealings with the reporting institution.
- (b) to the extent that there is doubt as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) referred to in Paragraph 13.4.8(a) or

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 26 of 64
------------------	---	---	---------------

where no natural person(s) exert control through ownership interests, the identity of the natural person (if any) exercising control of the legal person through other means; and

- (c) where no natural person is identified under Paragraphs 13.4.8(a) or (b) above, the identity of the relevant natural person who holds the position of senior management.

**S** 13.4.9 Where there is any doubt as to the identity of persons referred to under Paragraphs 13.4.7 and 13.4.8, the reporting institution shall:

- (a) conduct a basic search or enquiry on the background of such person to ensure that the person has not been or is not in the process of being dissolved or liquidated, or is a bankrupt; and
- (b) verify the authenticity of the information provided by such person with the Companies Commission of Malaysia, Labuan Financial Services Authority or any other relevant agencies.

**S** 13.4.10 Reporting institutions are exempted from obtaining a copy of the Memorandum and Articles of Association or certificate of incorporation and from identifying and verifying the directors and shareholders of the legal person which fall under the following categories:

- (a) public listed companies or corporations listed in Bursa Malaysia;
- (b) foreign public listed companies:

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 27 of 64
------------------	---	---	---------------

- listed in recognised exchanges; and
  - not listed in higher risk countries;
- (c) foreign financial institutions that are not from higher risk countries;
- (d) government-linked companies in Malaysia;
- (e) state-owned corporations and companies in Malaysia;
- (f) an authorised person, an operator of a designated payment system, a registered person, as the case may be, under the FSA and the IFSA;
- (g) persons licensed or registered under the Capital Markets and Services Act 2007;
- (h) licensed entities under the Labuan Financial Services and Securities Act 2010 and Labuan Islamic Financial Services and Securities Act 2010; or
- (i) prescribed institutions under the Development Financial Institutions Act 2002.

**G** 13.4.11 Reporting institutions may refer to the Directives in relation to Recognised Stock Exchanges (R/R6 of 2012) issued by Bursa Malaysia in determining foreign exchanges that are recognised.

*Legal Arrangements*

**S** 13.4.12 For customers that are legal arrangements, reporting institutions are required to understand the nature of the customer's business, its ownership and control structure.

**S** 13.4.13 Reporting institutions are required to identify the customer and verify its identity through the following information:

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 28 of 64
------------------	---	---	---------------

- (a) name, legal form and proof of existence, or any reliable references to verify the identity of the customer;
- (b) the powers that regulate and bind the customer, as well as the names of relevant persons having a senior management position; and
- (c) the address of the registered office, and if different, a principal place of business.

**S** 13.4.14 Reporting institutions are required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

- (a) for trusts, the identity of the settler, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership); or
- (b) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

**G** 13.4.15 Reporting institutions may rely on a third party to verify the identity of the beneficiaries when it is not practical to identify every beneficiary.

**S** 13.4.16 Where reliance is placed on third parties under Paragraph 13.4.15, reporting institutions are required to comply with Paragraph 18 on Reliance on Third Parties.

*Clubs, Societies and Charities*

**S** 13.4.17 For customers that are clubs, societies or charities, reporting institutions shall conduct CDD and require the

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 29 of 64
------------------	---	---	---------------

customers to furnish the relevant identification and constituent documents (or other similar documents) including certificate of registration and the identification and verification of the office bearer or any person authorised to represent the club, society or charity, as the case may be.

- S** 13.4.18 Reporting institutions are required to take reasonable measures to identify and verify the beneficial owners of the customers.

*Non-Bank Affiliated Charge & Credit Card Sector Only*

- S** 13.4.19 Reporting institutions are required to conduct CDD on the supplementary or corporate cardholders (secondary persons) apart from primary cardholders.

- S** 13.4.20 Reporting institutions shall also take reasonable steps to ensure that the primary cardholders and secondary persons are not listed persons in the UN Consolidated List and in any other orders issued pursuant to Part VIA of the AMLATFA. Reporting institutions are required to comply with the requirements for combating the financing of terrorism under Paragraph 26.

**13.5 Enhanced CDD**

- S** 13.5.1 Reporting institutions are required to perform enhanced CDD where the ML/TF risks are assessed as higher risk. An enhanced CDD, shall include, at least, the following:
- (a) obtaining CDD information under Paragraph 13.4;
  - (b) obtaining additional information on the customer and beneficial owner (e.g. volume of assets and other

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 30 of 64
------------------	---	---	---------------

information from public database);

- (c) inquiring on the source of wealth or source of funds. In the case of PEPs, both sources must be obtained; and
- (d) where applicable, obtaining approval from the Senior Management of the reporting institution before establishing (or continuing, for existing customer) such business relationship with the customer. In the case of PEPs, Senior Management refers to Senior Management at the head office.

**G**

13.5.2 In addition to Paragraph 13.5.1, reporting institutions may also consider the following enhanced CDD measures in line with the ML/TF risks identified:

- (a) obtaining additional information on the intended level and nature of the business relationship;
- (b) updating more regularly the identification data of customer and beneficial owner;
- (c) inquiring on the reasons for intended or performed transactions; and
- (d) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

### 13.6 On-Going Due Diligence

**S**

13.6.1 Reporting institutions are required to conduct on-going due diligence on the business relationship with its customers. Such measures shall include:

- (a) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the



BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 31 of 64
------------------	---	---	---------------

reporting institution’s knowledge of the customer, their 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 relevant, by undertaking reviews of existing records particularly for higher risk customers.

**G** 13.6.2 In conducting on-going due diligence, reporting institutions may take into consideration the economic background and purpose of any transaction or business relationship which:

- (a) appears unusual;
- (b) is inconsistent with the expected type of activity and business model when compared to the volume of transaction;
- (c) does not have any apparent economic purpose; or
- (d) casts doubt on the legality of such transactions, especially with regard to complex and large transactions or involving higher risk customers.

**S** 13.6.3 The frequency of the on-going due diligence, enhanced on-going due diligence as the case may be, shall commensurate with the level of ML/TF risks posed by the customer based on the risk profiles and nature of transactions.

**S** 13.6.4 Reporting institutions are required to increase the number and timing of controls applied, and to select patterns of transactions that need further examination, when conducting enhanced on-going due diligence.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 32 of 64
------------------	---	---	---------------

### 13.7 Existing Customer – Materiality and Risk

- S** 13.7.1 Reporting institutions are required to apply CDD requirements to existing customers on the basis of materiality and risk.
- S** 13.7.2 Reporting institutions are required to conduct CDD on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.
- G** 13.7.3 In assessing materiality and risk of the existing customer under Paragraph 13.7.1, reporting institutions may consider the following circumstances:
- (a) the nature and circumstances surrounding the transaction including the significance of the transaction;
  - (b) any material change in the way the account or business relationship is operated; or
  - (c) insufficient information held on the customer or change in customer’s information.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 33 of 64
------------------	---	---	---------------

## **14. Politically Exposed Persons (PEPs)**

### **14.1 General**

**S** 14.1.1 The requirements set out under this Paragraph are applicable to family members or close associates of all types of PEPs.

### **14.2 Foreign PEPs**

**S** 14.2.1 Reporting institutions are required to put in place a risk management system to determine whether a customer or a beneficial owner is a foreign PEP.

**S** 14.2.2 Upon determination that a customer or a beneficial owner is a foreign PEP, the requirements of enhanced CDD as set out under Paragraph 13.5 must be conducted.

### **14.3 Domestic PEPs or person entrusted with a prominent function by an international organisation**

**S** 14.3.1 Reporting institutions are required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person entrusted with a prominent function by an international organisation.

**S** 14.3.2 If the customer or beneficial owner is assessed as domestic PEP or a person entrusted with a prominent function by an international organisation, reporting institutions are 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.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 34 of 64
------------------	---	---	---------------

- S** 14.3.3 The assessment of the ML/TF risks, as specified under Paragraph 14.3.2, shall take into account the profile of the customer under Paragraph 12.4.2 on Risk Profiling.
- S** 14.3.4 The requirements of enhanced CDD as set out under Paragraph 13.5 must be conducted in respect of domestic PEPs or person entrusted with a prominent function by an international organisation who are assessed as higher risk.
- G** 14.3.5 Reporting institutions may apply CDD measures similar to other customers for domestic PEPs or persons entrusted with a prominent function by an international organisation if the reporting institution is satisfied that the domestic PEPs or persons entrusted with a prominent function by an international organisation are not assessed as higher risk.

## **15. New Products and Business Practices**

- S** 15.1 Reporting institutions are required to identify and assess the ML/TF risks that may arise in relation to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.
- S** 15.2 Reporting institutions are required to:
- (a) undertake the risk assessment prior to the launch or use of such products, practices and technologies; and
  - (b) take appropriate measures to manage and mitigate the risks.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 35 of 64
------------------	---	---	---------------

## 16. Wire transfer

### 16.1 General

- S** 16.1.1 The requirements under this Paragraph are applicable to cross-border wire transfers and domestic wire transfers including serial payments and cover payments conducted by the relevant electronic money issuers.
- S** 16.1.2 Reporting institutions must comply with the requirements on combating the financing of terrorism under Paragraph 26 in carrying out wire transfer.
- S** 16.1.3 Reporting institutions shall not execute the wire transfer if it does not comply with the requirements specified in this Paragraph.
- S** 16.1.4 Reporting institutions are required to maintain all originator and beneficiary information collected in accordance with record keeping requirements under Paragraph 23.

### 16.2 Ordering Institutions

#### *Cross-border wire transfers*

- S** 16.2.1 Reporting institutions which are ordering institutions are required to ensure that the message or payment instruction for all cross-border wire transfers involving an amount equivalent to RM3,000 and above are accompanied by the following:
- (a) Required and accurate originator information pertaining to:

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 36 of 64
------------------	---	---	---------------

- (i) name;
- (ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction; and
- (iii) address (or in lieu of the address, date and place of birth).

(b) Required beneficiary information pertaining to:

- (i) name; and
- (ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction.

**S** 16.2.2 Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country; and ordering institutions are required to include the originator's account number or unique transaction reference number.

**S** 16.2.3 Ordering institutions are required to ensure that the message or payment instruction for all cross-border wire transfers below RM3,000 are accompanied by the following:

(a) Required originator information pertaining to:

- (i) the name of the originator; and
- (ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 37 of 64
------------------	---	---	---------------

(b) Required beneficiary information pertaining to:

- (i) the name of the beneficiary; and
- (ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction.

**S** 16.2.4 The information required under Paragraph 16.2.3 need not be verified for accuracy except when there is a suspicion of ML/TF.

*Domestic wire transfers*

**S** 16.2.5 Ordering institutions are required to ensure that the information accompanying the wire transfer includes originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary institution and relevant authorities by other means.

**S** 16.2.6 Where the information accompanying the domestic wire transfer can be made available to the beneficiary institution and relevant authorities by other means, the ordering institution shall include only the originator's account number or if there is no account number, a unique identifier, within the message or payment form, provided that this account number or unique identifier will permit the transaction to be traced back to the originator or the beneficiary. Ordering institutions are required to provide the information within three working days of receiving the request either from the beneficiary institution or from the relevant authorities and must provide the information to law enforcement agencies

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 38 of 64
------------------	---	---	---------------

immediately upon request.

### 16.3 Intermediary Institutions

- S** 16.3.1 For cross-border wire transfers, intermediary institutions are required to retain all originator and beneficiary information that accompanies a wire transfer.
- S** 16.3.2 Where the required originator or beneficiary information accompanying a cross-border wire transfer cannot be transmitted due to technical limitations, intermediary institutions are required to keep a record in accordance with record keeping requirements under Paragraph 23.
- S** 16.3.3 Intermediary institutions are required to take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack the required originator information or required beneficiary information.
- S** 16.3.4 Intermediary institutions are required to have effective risk-based policies and procedures for determining:
- (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
  - (b) the appropriate follow-up action.

### 16.4 Beneficiary Institutions

- S** 16.4.1 Beneficiary institutions are required to take reasonable measures, including post-event or real-time monitoring



BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 39 of 64
------------------	---	---	---------------

where feasible, to identify cross-border wire transfers that lack the required originator information or required beneficiary information.

**S** 16.4.2 For cross-border wire transfers of an amount equivalent to RM3,000 and above, beneficiary institutions are required to verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with record keeping requirements under Paragraph 23.

**S** 16.4.3 Beneficiary institutions are required to have effective risk-based policies and procedures for determining:

- (a) when to execute, reject, or suspend a wire transfer lacking the required originator or required beneficiary information; and
- (b) the appropriate follow-up action.

## **17. Money or Value Transfer Services (MVTS)**

**S** 17.1 Reporting institutions offering MVTS either directly or as an agent to MVTS operators or providers are required to comply with all of the relevant requirements under Paragraph 16 on Wire Transfer in the countries in which they operate, directly or through their agents.

**S** 17.2 Where the reporting institutions offering MVTS control both the ordering and the beneficiary side of a wire transfer, the reporting institutions are required to:

- (a) take into account all the information from both the ordering and beneficiary sides in order to determine whether a suspicious

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 40 of 64
------------------	---	---	---------------

transaction report has to be filed; and

- (b) file a suspicious transaction report in any country affected by the suspicious wire transfer and make relevant transaction information available to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia.

## 18. Reliance on Third Parties

### *Customer Due Diligence*

- G** 18.1 Reporting institutions may rely on third parties to conduct CDD or to introduce business.
- S** 18.2 The ultimate responsibility and accountability of CDD measures shall remain with the reporting institution relying on the third parties.
- S** 18.3 Reporting institutions shall have in place internal policies and procedures to mitigate the risks when relying on third parties, including those from jurisdictions that have been identified as having strategic AML/CFT deficiencies that pose a ML/TF risk to the international financial system.
- S** 18.4 Reporting institutions are prohibited from relying on third parties located in the higher risk countries that have been identified with on-going or substantial ML/TF risks.
- S** 18.5 The relationship between reporting institutions and the third parties relied upon by the reporting institutions to conduct CDD shall be governed by an arrangement that clearly specifies the rights, responsibilities and expectations of all parties. At the minimum, reporting institutions must be satisfied that the third party:

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 41 of 64
------------------	---	---	---------------

- (a) can obtain immediately the necessary information concerning CDD as required under Paragraphs 13.4;
- (b) has an adequate CDD process;
- (c) has measures in place for record keeping requirements;
- (d) can provide the CDD information and provide copies of the relevant documentation immediately upon request; and
- (e) is properly regulated and supervised by the respective authorities.

**G** 18.6 Reporting institutions may obtain an attestation from the third party to satisfy itself that the requirements in Paragraph 18.5 have been met.

**G** 18.7 Reporting institutions may obtain written confirmation from the third party that it has conducted CDD on the customer or beneficial owner, as the case may be, in accordance with Paragraph 13.

**G** 18.8 The requirements under Paragraphs 18.1, 18.3 and 18.5 may be fulfilled if the reporting institution relies on a third party that is part of the same financial group subject to the following conditions:

- (a) the group applies CDD and record keeping requirements and AML/CFT programmes in line with the requirements in this document;
- (b) the implementation of those CDD and record keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority; and
- (c) any higher country risk is adequately mitigated by the financial group's AML/CFT policies.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 42 of 64
------------------	---	---	---------------

*On-going Due Diligence*

- S** 18.9 Reporting institutions shall not rely on third parties to conduct on-going due diligence of its customers.

**19. Non Face-to-Face Business Relationship**

- G** 19.1 Reporting institutions may establish non face-to-face business relationships with its customers.
- S** 19.2 Non face-to-face relationships can only be established if the reporting institutions have in place policies and procedures to address any specific risks associated with non face-to-face business relationships.
- S** 19.3 Reporting institutions are required to be vigilant in establishing and conducting business relationships via information communication technology.
- S** 19.4 Reporting institutions are required to establish appropriate measures for identification and verification of customer's identity that shall be as effective as that for face-to-face customer and implement monitoring and reporting mechanisms to identify potential ML/TF activities.
- G** 19.5 Reporting institutions may use the following measures to verify the identity of non face-to-face customer such as:
- (a) requesting additional documents to complement those which are required for face-to-face customer;
  - (b) developing independent contact with the customer; or
  - (c) verifying customer information against any database maintained by the authorities.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 43 of 64
------------------	---	---	---------------

## 20. Higher Risk Countries

- S** 20.1 Reporting institutions are required to conduct enhanced CDD for business relationships and transactions with any person from countries identified by the FATF or the Government of Malaysia as having on-going or substantial ML/TF risks.
- S** 20.2 Where ML/TF risks are assessed as higher risk, reporting institutions are required to conduct enhanced CDD for business relationships and transactions with any person from countries identified by the FATF or the Government of Malaysia as having strategic AML/CFT deficiencies that have not made sufficient progress in addressing those deficiencies.
- S** 20.3 In addition to the enhanced CDD requirement under Paragraph 20.1, reporting institutions are required to apply appropriate countermeasures, proportionate to the risk, for higher risk countries listed as having on-going or substantial ML/TF risks, as follows:
- (a) limit business relationship or financial transactions with identified countries or persons located in the country concerned;
  - (b) review and amend, or if necessary terminate, correspondent banking relationships with financial institutions in the country concerned;
  - (c) conduct enhanced external audit, by increasing the intensity and frequency, on branches and subsidiaries of the reporting institution located in the country concerned;
  - (d) submit a report with a summary of exposure to customers and beneficial owners from the country concerned to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia on an annual basis; and

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 44 of 64
------------------	---	---	---------------

(e) conduct any other measures as may be specified by Bank Negara Malaysia.

## 21. Failure to Satisfactorily Complete CDD

- S** 21.1 Reporting institutions shall not open the account, commence business relations or perform any transaction in relation to a potential customer, or shall terminate business relations in the case of an existing customer, if the reporting institution is unable to comply with the CDD requirements.
- S** 21.2 In the event of failure to comply with the CDD requirements, reporting institutions must consider lodging a suspicious transaction report under Paragraph 25.

## 22. Management Information System

- S** 22.1 Reporting institutions must have in place an adequate management information system (MIS), either electronically or manually, to complement its CDD process. The MIS is required to provide the reporting institution with timely information on a regular basis to enable the reporting institution to detect irregularity and/or any suspicious activity.
- S** 22.2 The MIS shall commensurate with the nature, scale and complexity of the reporting institution's activities and ML/TF risk profile.
- S** 22.3 The MIS shall include, at a minimum, information on multiple transactions over a certain period, large transactions, anomaly in transaction patterns, customer's risk profile and transactions exceeding any internally specified threshold.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 45 of 64
------------------	---	---	---------------

**S** 22.4 The MIS shall be able to aggregate customer's transactions from multiple accounts and/or from different systems.

**G** 22.5 The MIS may be integrated with the reporting institution's information system that contains its customer's normal transaction or business profile, which is accurate, up-to-date and reliable.

### **23. Record Keeping**

**S** 23.1 Reporting institutions are required to keep the relevant records including any accounts, files, business correspondence and documents relating to transactions, in particular, those obtained during the CDD process. This includes documents used to verify the identity of customers and beneficial owners, and results of any analysis undertaken. The records maintained must remain up-to-date and relevant.

**S** 23.2 Reporting institutions are required to keep the records for at least six years following the completion of the transaction, the termination of the business relationship or after the date of the occasional transaction.

**S** 23.3 In situations where the records are subjected to on-going investigation or prosecution in court, they shall be retained beyond the stipulated retention period until such time reporting institutions are informed by the relevant law enforcement agency that such records are no longer required.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 46 of 64
------------------	---	---	---------------

- S** 23.4 Reporting institutions are required to retain the relevant records in a form that is admissible as evidence in court and make such available to the supervisory authorities and law enforcement agencies in a timely manner.

## **24. AML/CFT Compliance Programme**

### **Policies, Procedures and Controls**

- S** 24.1 Reporting institutions are required to implement programmes to mitigate against ML/TF, which correspond to its ML/TF risks and the size of its business.

### **24.2 Board of Directors**

- S** 24.2.1 *General*
- (a) Members of Board of Directors (Board members) shall understand their roles and responsibilities in managing ML/TF risks faced by the reporting institution.
  - (b) Board members must be aware of the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services.
  - (c) Board members must understand the AML/CFT measures required by the laws including the AMLATFA, subsidiary legislation and instruments issued under the AMLATFA, and the industry's standards and best practices as well as the importance of implementing AML/CFT measures to prevent the reporting institution from being abused by money launderers and financiers of terrorism.



BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 47 of 64
------------------	---	---	---------------

**S**

**24.2.2 Roles and Responsibilities**

The Board of Directors have the following roles and responsibilities:

- (a) maintain accountability and oversight for establishing AML/CFT policies and minimum standards;
- (b) approve policies regarding AML/CFT measures within the reporting institution, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism;
- (c) establish appropriate mechanisms to ensure the AML/CFT policies are periodically reviewed and assessed in line with changes and developments in the reporting institution's products and services, technology as well as trends in ML/TF;
- (d) establish an effective internal control system for AML/CFT and maintain adequate oversight of the overall AML/CFT measures undertaken by the reporting institution;
- (e) define the lines of authority and responsibility for implementing the AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;
- (f) ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF;
- (g) assess the implementation of the approved AML/CFT policies through regular reporting and updates by the

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 48 of 64
------------------	---	---	---------------

Senior Management and Audit Committee; and

- (h) establish MIS that is reflective of the nature of the reporting institution's operations, size of business, complexity of business operations and structure, risk profiles of products and services offered and geographical coverage.

### 24.3 Senior Management

**S** 24.3.1 Senior Management is accountable for the implementation and management of AML/CFT compliance programmes in accordance with policies and procedures established by the Board, requirements of the law, regulations, guidelines and the industry's standards and best practices.

#### **S** 24.3.2 *Roles and Responsibilities*

The Senior Management have the following roles and responsibilities:

- (a) be aware of and understand the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services offered and to be offered including new products, new delivery channels and new geographical coverage;
- (b) formulate AML/CFT policies to ensure that they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken by the reporting institution and its geographical coverage;
- (c) establish appropriate mechanisms and formulate procedures to effectively implement AML/CFT policies

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 49 of 64
------------------	---	---	---------------

and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;

- (d) undertake review and propose to the Board the necessary enhancements to the AML/CFT policies to reflect changes in the reporting institution's risk profiles, institutional and group business structure, delivery channels and geographical coverage;
- (e) provide timely periodic reporting to the Board on the level of ML/TF risks facing the reporting institution, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML/CFT which may have an impact on the reporting institution;
- (f) allocate adequate resources to effectively implement and administer AML/CFT compliance programmes that are reflective of the size and complexity of the reporting institution's operations and risk profiles;
- (g) appoint a compliance officer at management level at Head Office and designate a compliance officer at management level at each branch or subsidiary;
- (h) provide appropriate level of AML/CFT training for its employees at all levels throughout the organisation;
- (i) ensure that there is a proper channel of communication in place to effectively communicate the AML/CFT policies and procedures to all levels of employees;
- (j) ensure that AML/CFT issues raised are addressed in a timely manner; and
- (k) ensure the integrity of its employees by establishing

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 50 of 64
------------------	---	---	---------------

appropriate employee assessment system.

#### 24.4 **Compliance Management Arrangements at the Head Office**

- S** 24.4.1 The Compliance Officer acts as the reference point for AML/CFT matters within the reporting institution.
- S** 24.4.2 The Compliance Officer is required to be “fit and proper” to carry out his AML/CFT responsibilities effectively.
- G** 24.4.3 For the purposes of Paragraph 24.4.2, “fit and proper” may include minimum criteria relating to:
- (a) probity, personal integrity and reputation; or
  - (b) competency and capability.
- S** 24.4.4 The Compliance Officer must have the necessary knowledge and expertise to effectively discharge his roles and responsibilities, including being informed of the latest developments in ML/TF techniques and the AML/CFT measures undertaken by the industry.
- G** 24.4.5 Reporting institutions may encourage the Compliance Officer to pursue professional qualifications in AML/CFT so that they are able to carry out their obligations effectively.
- S** 24.4.6 Reporting institutions are required to ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented.
- S** 24.4.7 The Compliance Officer has a duty to ensure the following:
- (a) the reporting institution’s compliance with the

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 51 of 64
------------------	---	---	---------------

AML/CFT requirements;

- (b) proper implementation of the AML/CFT policies;
- (c) the appropriate AML/CFT procedures, including CDD, record-keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism, are implemented effectively;
- (d) the AML/CFT mechanism is regularly assessed to ensure that it is effective and sufficient to address any change in ML/TF trends;
- (e) the channel of communication from the respective employees to the branch or subsidiary compliance officer and subsequently to the Compliance Officer is secured and that information is kept confidential;
- (f) all employees are aware of the reporting institution's AML/CFT measures, including policies, control mechanism and the channel of reporting;
- (g) internal generated suspicious transaction reports by the branch or subsidiary compliance officers are appropriately evaluated before submission to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia; and
- (h) the identification of ML/TF risks associated with new products or services or arising from the reporting institution's operational changes, including the introduction of new technology and processes.

**S**

24.4.8 Reporting institutions are required to inform, in writing, the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, within ten working days, on the

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 52 of 64
------------------	---	---	---------------

appointment or change in the appointment of the Compliance Officer, including such details as the name, designation, office address, office telephone number, fax number, e-mail address and such other information as may be required.

#### 24.5 **Employee Screening Procedures**

**S** 24.5.1 The screening procedures shall apply upon hiring the employee and throughout the course of employment.

**S** 24.5.2 Reporting institutions are required to establish an employee assessment system that is commensurate with the size of operations and risk exposure of reporting institutions to ML/TF.

**S** 24.5.3 The employee assessment system shall include an evaluation of an employee's personal information, including employment and financial history.

#### 24.6 **Employee Training and Awareness Programmes**

24.6.1 For the purpose of this Paragraph, reference to employees includes agents.

**S** 24.6.2 Reporting institutions are required to conduct awareness and training programmes on AML/CFT practices and measures for their employees. Such training must be conducted regularly and supplemented with refresher courses.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 53 of 64
------------------	---	---	---------------

- S** 24.6.3 The employees must be made aware that they may be held personally liable for any failure to observe the AML/CFT requirements.
- S** 24.6.4 The reporting institution must make available its AML/CFT policies and procedures for all employees and its documented AML/CFT measures must contain at least the following:
- (a) the relevant documents on AML/CFT issued by Bank Negara Malaysia or relevant supervisory authorities; and
  - (b) the reporting institution's internal AML/CFT policies and procedures.
- S** 24.6.5 The training conducted for employees must be appropriate to their level of responsibilities in detecting ML/TF activities and the risks of ML/TF faced by reporting institutions.
- S** 24.6.6 Employees who deal directly with the customer shall be trained on AML/CFT prior to dealing with customers.
- G** 24.6.7 Training for all employees may provide a general background on ML/TF, the requirements and obligations to monitor and report suspicious transactions to the Compliance Officer and the importance of CDD.
- G** 24.6.8 In addition, training may be provided to specific categories of employees:
- (a) *Front-Line Employees*  
Front-line employees may be trained to conduct effective on-going CDD, detect suspicious

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 54 of 64
------------------	---	---	---------------

transactions and on the measures that need to be taken upon determining a transaction as suspicious. Training may also be provided on factors that may give rise to suspicion, such as dealing with occasional customers transacting in large cash volumes, PEPs, higher risk customers and the circumstances where enhanced CDD is required.

(b) *Employees that Establish Business Relationships*

The training for employees who establish business relationships may focus on customer identification, verification and CDD procedures, including when to conduct enhanced CDD and circumstances where there is a need to defer establishing business relationship with a new customer until CDD is completed satisfactorily.

(c) *Supervisors and Managers*

The training on supervisors and managers may include overall aspects of AML/CFT procedures, in particular, the risk-based approach to CDD, risk profiling of customers, enforcement actions that can be taken for non-compliance with the relevant requirements pursuant to the relevant laws and procedures related to the financing of terrorism.

## 24.7 Independent Audit Functions

**S**

24.7.1 The Board is responsible to ensure regular independent audits of the internal AML/CFT measures to determine their effectiveness and compliance with the AMLATFA, its



BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 55 of 64
------------------	---	---	---------------

regulations, subsidiary legislations, the relevant documents on AML/CFT issued by Bank Negara Malaysia as well as the requirements of the relevant laws and regulations of other supervisory authorities, where applicable.

- S** 24.7.2 The Board is required to ensure that the roles and responsibilities of the auditor are clearly defined and documented. The roles and responsibilities of the auditor include, at a minimum:
- (a) checking and testing the compliance with, and effectiveness of the AML/CFT policies, procedures and controls; and
  - (b) assessing whether current measures are in line with the latest developments and changes to the relevant AML/CFT requirements.
- S** 24.7.3 The scope of independent audit shall include, at a minimum:
- (a) compliance with AMLATFA, its subsidiary legislation and instruments issued under the AMLATFA;
  - (b) compliance with the reporting institution's internal AML/CFT policies and procedures;
  - (c) adequacy and effectiveness of the AML/CFT compliance programme; and
  - (d) reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems.
- S** 24.7.4 The auditor must submit a written audit report to the Board to highlight the assessment on the effectiveness of

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 56 of 64
------------------	---	---	---------------

AML/CFT measures and any inadequacy in internal controls and procedures.

**S** 24.7.5 Reporting institutions are required to ensure that independent audits are carried out at the institution level at least on an annual basis.

**S** 24.7.6 Reporting institutions must ensure that such audit findings and the necessary corrective measures undertaken are submitted to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and its relevant supervisory authorities within ten working days of their submission to its Board.

## **25. Suspicious Transaction Report**

### **25.1 General**

**S** 25.1.1 Reporting institutions are required to promptly submit a suspicious transaction report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia whenever the reporting institution suspects or have reasons to suspect that the transaction (including attempted or proposed), regardless of the amount:

- (a) appears unusual;
- (b) has no clear economic purpose;
- (c) appears illegal;
- (d) involves proceeds from an unlawful activity; or
- (e) indicates that the customer is involved in ML/TF.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 57 of 64
------------------	---	---	---------------

**S** 25.1.2 Reporting institutions must provide the required and relevant information that gave rise to doubt in the suspicious transaction report form, which includes but is not limited to the nature or circumstances surrounding the transaction and business background of the person conducting the transaction that is connected to the unlawful activity.

**S** 25.1.3 Reporting institutions must establish a reporting system for the submission of suspicious transaction reports.

**G** 25.1.4 Reporting institutions may refer to **Appendix I** of this document which provides examples of transactions that may constitute triggers for the purposes of reporting suspicious transactions.

## 25.2 Reporting Mechanisms

**S** 25.2.1 Reporting institutions are required to ensure that the designated branch or subsidiary compliance officer is responsible for channelling all internal suspicious transaction reports received from the employees of the respective branch or subsidiary to the Compliance Officer at the head office. In the case of employees at the head office, such internal suspicious transaction reports shall be channelled directly to the Compliance Officer.

**S** 25.2.2 Reporting institutions are required to have in place policies on the duration upon which internally generated suspicious transaction reports must be reviewed by the Compliance Officer, including the circumstances when the timeframe

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 58 of 64
------------------	---	---	---------------

can be exceeded, where necessary.

**S** 25.2.3 Upon receiving any internal suspicious transaction report whether from the head office, branch or subsidiary, the Compliance Officer must evaluate the grounds for suspicion. Once the suspicion is confirmed, the Compliance Officer must promptly submit the suspicious transaction report. In the case where the Compliance Officer decides that there are no reasonable grounds for suspicion, the Compliance Officer must document and file the decision, supported by the relevant documents.

**S** 25.2.4 The Compliance Officer must submit the suspicious transaction report in the specified suspicious transaction report form (attached in **Appendix II**) through any of the following modes:

Mail : Director  
Financial Intelligence and Enforcement  
Department  
Bank Negara Malaysia  
Jalan Dato' Onn  
50480 Kuala Lumpur  
(To be opened by addressee only)

Fax : +603-2693 3625

E-mail : [str@bnm.gov.my](mailto:str@bnm.gov.my)

**S** 25.2.5 Where applicable and upon the advice of the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, the compliance officer of a reporting institution must submit its suspicious transaction reports on-line:

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 59 of 64
------------------	---	---	---------------

Website : <https://bnmapp.bnm.gov.my/fins2>

- S** 25.2.6 The Compliance Officer must ensure that the suspicious transaction report is submitted within the next working day, from the date the Compliance Officer establishes the suspicion.
- S** 25.2.7 Reporting institutions must ensure that in the course of submitting the suspicious transaction report, utmost care must be undertaken to ensure that such reports are treated with the highest level of confidentiality. The Compliance Officer has the sole discretion and independence to report suspicious transactions.
- S** 25.2.8 Reporting institutions must provide additional information and documentation as may be requested by the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and to respond promptly to any further enquiries with regard to any report received under Section 14 of the AMLATFA.
- S** 25.2.9 Reporting institutions must ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preserve secrecy.
- S** 25.2.10 Where a suspicious transaction report has been lodged, reporting institutions are not precluded from making a fresh suspicious transaction report as and when a new suspicion arises.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 60 of 64
------------------	---	---	---------------

### 25.3 Tipping Off

- S** 25.3.1 In cases where the 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. In such circumstances, the reporting institution shall proceed with the transaction and immediately file a suspicious transaction report.
- S** 25.3.2 Tipping off in relation to suspicious transaction report is not applicable if:
- (a) the purpose of the disclosure is made to inform the ML/TF risks involved in dealing with the customer within the financial group; or
  - (b) such disclosure is made to a supervisory authority of the reporting institution.
- 25.3.3 Provisions under Paragraph 25.3.2 will not come into effect until such date as may be specified by Bank Negara Malaysia.

### 25.4 Triggers for Submission of Suspicious Transaction Report

- S** 25.4.1 Reporting institutions are required to establish internal criteria (“red flags”) to detect suspicious transactions.
- G** 25.4.2 Reporting institutions may be guided by examples of suspicious transactions provided by Bank Negara Malaysia or other corresponding competent authorities, supervisory authorities and international organisations.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 61 of 64
------------------	---	---	---------------

- S** 25.4.3 Reporting institutions must consider submitting a suspicious transaction report when any of its customer’s transactions or attempted transactions fits the reporting institution’s list of “red flags”.

**25.5 Internally Generated Suspicious Transaction Reports**

- S** 25.5.1 Reporting institutions must ensure that the Compliance Officer maintains a complete file on all internally generated reports and any supporting documentary evidence regardless of whether such reports have been submitted. If there is no suspicious transaction reports submitted to Financial Intelligence and Enforcement Department, Bank Negara Malaysia, the internally generated reports and the relevant supporting documentary evidence must be made available to the relevant supervisory authorities upon request.

**26. Combating the Financing of Terrorism**

- 26.1 Where relevant, references to a customer in this Paragraph include a beneficial owner and beneficiary.
- S** 26.2 Reporting institutions are required to keep 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-Qaida organisation.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 62 of 64
------------------	---	---	---------------

- S** 26.3 Reporting institutions are required to maintain a list of individuals and entities (the Consolidated List) for this purpose. The updated UN List can be obtained at:  
[http://www.un.org/sc/committees/1267/aq\\_sanctions\\_list.shtml](http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml)
- S** 26.4 Reporting institutions are required to 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.
- S** 26.5 Reporting institutions shall ensure that the information contained in the database is updated and relevant, and made easily accessible to its employees at the head office, branch or subsidiary.
- S** 26.6 Reporting institutions are required to conduct checks on the names of new customers, as well as regular checks on the names of existing customers, and potential customers, against the names in the database. If there is any name match, reporting institutions are required to take reasonable and appropriate measures to verify and confirm the identity of its customer. Once confirmation has been obtained, reporting institutions must immediately:
- (a) freeze the customer's funds or block the transaction (where applicable), if it is an existing customer;
  - (b) reject the potential customer, if the transaction has not commenced;
  - (c) submit a suspicious transaction report; and
  - (d) inform the relevant supervisory authorities.
- S** 26.7 Reporting institutions are required to submit a suspicious transaction report when there is an attempted transaction by any of the persons



BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 63 of 64
------------------	---	---	---------------

listed in the Consolidated List or orders made by the Minister of Home Affairs under sections 66B or 66C of the AMLATFA.

- S** 26.8 Reporting institutions are required to ascertain potential matches with the Consolidated List to confirm whether they are true matches to eliminate “false positives”. The reporting institutions are required to make further inquiries from the customer or counter-party (where relevant) to assist in determining whether the match is a true match.
- G** 26.9 Reporting institutions may also consolidate their database with the other recognised lists of designated persons or entities issued by other jurisdictions.

## **27. Non-Compliance**

- S** 27.1 Enforcement actions can be taken against the reporting institutions including its directors, officers and employees for any non-compliance with any provision marked as “S” in this document:
- (a) in accordance with the provisions in sections 22, 66E, 86, 87, 88, 92 and 93 of the AMLATFA; and/or
  - (b) in accordance with the provisions of other laws pursuant to which this document is issued.

BNM/RH/STD 029-2	Financial Intelligence and Enforcement Department	Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Electronic Money and Non-Bank Affiliated Charge & Credit Card (Sector 4)	Page 64 of 64
------------------	---	---	---------------

## Appendix I

### Examples of Transactions that May Trigger Suspicion

1. Discrepancies between the information submitted by the customer and information detected by reporting institutions monitoring systems.
2. Individuals who hold an unusual number of accounts with the same provider.
3. A large and diverse source of funds (*i.e.*, bank transfers, credit card and cash reload from different locations) used to reload the same account.
4. Multiple reference bank accounts from banks located in various locations used to reload the same e-money account frequently.
5. Frequently re-loading of account by third parties.
6. Numerous cash reloads, just under the reporting threshold, of the same account, conducted by the same individual(s) on a number of occasions.
7. Multiple reload by third party followed by the immediate transfer of funds to beneficiary bank account.
8. Multiple occasions of reloading of an account, followed by ATM withdrawals.
9. Multiple withdrawals conducted at different ATMs (including those outside the country where the account was reloaded).
10. Account only used for withdrawals and not for purchases.

RAHSIA



Please send completed form to:
Financial Intelligence & Enforcement Department
Bank Negara Malaysia
Jalan Dato' Onn, 50480 Kuala Lumpur
Fax : 03-2693 3625 E-mail : str@bnm.gov.my

Reference no : \_\_\_\_\_

SUSPICIOUS TRANSACTION REPORT

Electronic Money and Credit/Charge Cards Issuers

- a. This report is made pursuant to the requirement to report suspicious transaction under the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA)
b. Under section 24 of the AMLATFA, no civil, criminal or disciplinary proceedings shall be brought against a person who makes a report unless it was made in bad faith

PART A: INFORMATION ON CUSTOMER

Account holder

1) Individual

Form fields for individual information: Nationality (MALAYSIA), Name, Other/previous name (1, 2, 3), New NRIC no, Old NRIC no, Other identification, Other identification type, Gender.

Contact information

Residential/business address form field

Correspondence address form field

Other address form field



Previous address

--

Email address			
Contact no	- (Off)	- (Res)	- (Mob)
Fax no			

**Employment information**

Business/employment type	
Occupation	
Occupation description	
Employer name	
Employment area	
Other known employment	

**Marital information**

Marital status	
Spouse name	

**Spouse identification**

New NRIC no		Old NRIC no	
Other identification		Other identification type	
Passport no		Place/country of issue	

**PART B: TRANSACTION DETAILS**

Attempted but not completed transaction	<input type="text" value="No"/>
Account no	
Transaction date	- to -
Transaction amount (MYR)	0.00



**PART C: DESCRIPTION OF SUSPICIOUS TRANSACTION**

Grounds for suspicion	Overpayment of account and the customer requests for refund from the Company
	Early settlement of account that does not commensurate with the customer's financial standing
	Payment is credited into a customer's account by a third party with no apparent relation to the customer
	Frequent reload/withdrawal/cash-back of account
	Unwillingness of customer/third party to disclose identity
	Others (Please specify)
<i>Others (please specify)</i>	
Description of suspected criminal activity	
Details of the nature and circumstances surrounding it	
Date of reporting	