BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

# Debit Card-i

Applicable to:
1. Debit card-i issuers
2. Debit card-i acquirers

Issued on: 2 December 2016

BNM/RH/PD 034-2

## Table of contents

# PART A OVERVIEW

## 1 Introduction

1.1 These requirements aim to safeguard the integrity of the debit card-i system, thereby preserving consumer confidence and promoting its wider adoption in Malaysia.

1.2 Part C of this policy document outlines specific requirements and minimum standards to be observed by debit card-i issuers and acquirers.

1.3 Part D of this policy document outlines risk management principles and requirements for debit card-i issuers and acquirers.

## 2 Applicability

2.1 This policy document is applicable to all debit card-i issuers and acquirers.

2.2 The requirements of this policy document apply to debit card-i products offered to:
(a) individuals;
(b) micro, small and medium enterprises (SMEs); and
(c) corporate cardholders,
with the exception of requirements under sections 9 to 15 under Part C which only apply to debit card-i products offered to individual, micro and small enterprises. However, issuers are encouraged to adopt similar standards under these sections for debit card-i products offered to medium and large enterprises.

## 3 Legal provisions

3.1 The requirements in this policy document are issued pursuant to:
(a) Sections 43(1), 57(1) and 135(1) of the Islamic Financial Services Act 2013 (IFSA); and
(b) Sections 41 and 42(C)(1) of the Development Financial Institutions Act 2002 (DFIA).

## 4 Effective date

4.1 This is an enhanced version of the Debit Card-i policy document which came into effect on 28 February 2014. Requirements which have effective dates other than 28 February 2014 are as follows:
(a) Paragraphs 10.2, 10.3, 10.4, 10.6 and 13.1: 1 January 2017;

(b) Paragraphs 12.3, 12.4, 13.4(a) and 24.13(b): 1 April 2017;
(c) Paragraph 24.8 - Implementation of "Chip and PIN" technology:
  (i) at automated teller machine (ATM): 1 January 2015; and
  (ii) at point-of-sale (POS) terminals: 1 January 2017.

## 5 Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the IFSA or DFIA, as the case may be, unless otherwise defined in this policy document.

5.2 For the purpose of this policy document–

| | |
|---|---|
| **"S"** | denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action; |
| **"G"** | denotes guidance which may consist of statements or information intended to promote common understanding and advise or recommendations that are encouraged to be adopted; |
| "debit card-i" | refers to a payment instrument that is linked to a deposit account, current account, savings account or other similar account at a financial institution that can be used-<br>(i) to pay for goods and services;<br>(ii) to withdraw cash from automated teller machine or withdraw cash at participating retail outlets through debit card-i usage by debiting the user's account; or<br>(iii) for the purposes of (i) and (ii). |
| "issuer" | refers to a person who has obtained approval from Bank Negara Malaysia (the Bank) under section 11 of the IFSA to issue debit card-i |
| "user" | refers to any person whom a debit card-i has been issued to and here on referred to as cardholder; |
| "acquirer" | refers to any person that provides merchant acquiring services; |
| "financial institution" | refers to any person licensed under the IFSA or FSA or prescribed under the DFIA; |

| | |
|---|---|
| "micro, small and medium-sized enterprises" | is as per the definition in the circular on New Definition of Small and Medium Enterprises (SMEs) issued by the Bank. |

## 6 Policy documents superseded

6.1 This policy document supersedes the policy document on Debit Card-i issued on 28 February 2014.

# PART B APPROVED SHARIAH CONCEPT

## 7 Shariah concept

**S** 7.1 The underlying Shariah concept that is applicable to debit card-i is ujrah (fee). Under this concept, ujrah (fee) will be charged to customer in consideration of identified services, benefits and privileges. Such services may include payment facility for goods and services, and cash withdrawal from customer's account via automated teller machine.

## 8 Shariah requirements

**S** 8.1 Any privileges granted by card issuer shall only include services and benefits that are in compliance with Shariah.

**S** 8.2 The fee shall only be charged on services, benefits and privileges provided.

# PART C BUSINESS CONDUCT

### A. FEES AND CHARGES

## 9 Guiding principles on fees and charges

**S** 9.1 In determining the type and quantum of fees and charges on debit card-i, issuers shall ensure compliance with the Guidelines on Imposition of Fees and Charges on Financial Products and Services.

**S** 9.2 Upon the issuance of a debit card-i, issuers may impose a fee for the card. However, issuers shall not charge cardholders an annual fee during the same year the debit card-i is issued.

### B. LIABILITY

## 10 Liability for unauthorised transactions

**S** 10.1 Issuers shall provide an effective and convenient means including having a dedicated contact number by which cardholders can notify the issuers of any lost, stolen or unauthorised use of their debit card-i. Issuers shall also implement procedures for acknowledging receipt and verification of the notification of the lost, stolen or unauthorised use of the debit card-i.

**S** 10.2 Issuers shall not hold cardholders liable for card-present unauthorised transactions which require Personal Identification Number (PIN) verification, unless issuers can prove that the cardholder has:

(a) acted fraudulently;
(b) delayed in notifying the issuer as soon as reasonably practicable after having discovered the loss or unauthorised use of the debit card-i;
(c) voluntarily disclosed the PIN to another person; or
(d) recorded the PIN on the debit card-i, or on anything kept in close proximity with the debit card-i, and could be lost or stolen with the debit card-i.

**S** 10.3 Issuers shall not hold cardholders liable for card-present unauthorised transactions which require signature verification or the use of a contactless card, unless issuers can prove that the cardholder has:

(a) acted fraudulently;
(b) delayed in notifying the issuer as soon as reasonably practicable after having discovered the loss or unauthorised use of the debit card-i;
(c) left the debit card-i or an item containing the debit card-i unattended, in places visible and accessible to others, except at the cardholder's place of residence. However, cardholders are expected to exercise due care in safeguarding the debit card-i even at cardholder's place of residence; or
(d) voluntarily allowed another person to use the debit card-i.

**S** 10.4 Issuers must ensure that appropriate investigations are carried out. Any decision to pass on liability for unauthorised transactions must be supported by sufficient evidence to prove that one of the conditions specified in paragraph 10.2 or 10.3, as the case may be, has been met.

**S** 10.5 Issuers shall have clear processes in place to register any notification of lost, stolen or unauthorised use of debit card-i and take immediate action upon notification by the cardholders, to prevent further use of the debit card-i. Cardholders shall not be held liable for any unauthorised transactions charged to the debit card-i after the cardholders have notified issuers verbally or in writing, of the lost, stolen or unauthorised use of the debit card-i.

**S** 10.6 Issuers shall not hold cardholders liable for losses incurred if the cause of the losses is due to any of the following:

(a) failure of the issuer to send reminders to cardholders as per the requirements in paragraphs 12.3 and 13.4(a);
(b) failure of the issuer to provide customer hotlines which are operational at all times for cardholders to notify the issuer of any lost, stolen or unauthorised use of the debit card-i;
(c) a technical breakdown or other deficiency in issuer's systems or equipment;
(d) weaknesses or vulnerability in security features and controls adopted by the issuer;
(e) a transaction that involved the use of a forged debit card-i;
(f) for transactions requiring PIN verification, a transaction that occurred before the cardholder received the PIN or changed the default PIN for the first time;

(g) fraudulent or negligent conduct of the employees or agents of the card issuer or merchants; or
(h) a transaction, excluding a recurring transaction, that occurred after the cardholder has notified the issuer of the lost, stolen or unauthorised use of the debit card-i.

## C. DISCLOSURE AND TRANSPARENCY REQUIREMENTS

**S** This section shall be read together with the general policy requirements stipulated in the Guidelines on Product Transparency and Disclosure.

**G** Disclosure is effective when product information is given to the cardholders at a time that is most relevant to enable the cardholders to make informed decisions at each of the three stages of the contractual process, which is the pre-contractual stage, at the point of entering into a contract, and during the term of the contract.

**S** Issuers shall provide a product disclosure sheet (as per the format provided in Appendix 1 of this policy document) containing key information for cardholders to make informed decisions. The product disclosure sheet shall be provided before the cardholders sign up for the debit card-i, and at the point of entering into a contract, if there are material changes in the information. Issuers shall also ensure that the product disclosure sheet is made available in Bahasa Malaysia, upon request.

### 11 Pre-contractual stage

**S** 11.1 Basic features
(a) Issuers shall inform cardholders of the key features of the debit card-i, including the underlying Shariah contract governing the debit card-i.
(b) If an ATM card also functions as a debit card-i, issuers shall clearly inform cardholders of such feature.

**S** 11.2 Fees and other charges
(a) Issuers shall disclose to the cardholders in the product disclosure sheet all applicable fees and charges in relation to the debit card-i, including the amount and frequency of payment.

**S** 11.3 Promotional items
(a) Cardholders shall be made aware of the conditions tied to any promotional item and the implications of not complying with such conditions, if any.

### 12 At the point of entering into a contract

**S** 12.1 Terms and conditions
(a) Issuers shall make written terms and conditions for usage of the debit card-i readily available to cardholders. The document shall contain a clear and

concise description of the major terms and conditions which impose liabilities or obligations on cardholders (in respect of both principal and supplementary cards). Such terms shall be described in plain language, which is easily understood by cardholders.

(b) Issuers shall advise cardholders to read and understand the terms and conditions before signing the agreement and using the debit card-i. Issuers shall take reasonable steps to draw cardholders' attention to the terms that have implications on liability.

(c) Issuers shall inform cardholders on the pre-authorisation amount which will be charged to cardholders' accounts when cardholders use the debit card-i at automated fuel dispensers for petrol purchases. Cardholders shall also be informed that the issuers may hold the amount up to 3 working days after the transaction date before releasing any excess amount held from the cardholders' account.

(d) Issuers shall ensure that customer service staff and the sales and marketing representatives are able to answer queries on the debit card-i terms and conditions. The hotlines for the customer service shall be published in the brochures, account statements, web pages and at the back of the debit card-i.

**S** 12.2 Usage of debit card-i outside Malaysia

(a) Cardholders shall be informed of the relevant charges for retail transactions made outside Malaysia.

(b) Cardholders shall also be informed of the transaction fees and currency conversion fees applicable on the use of the debit card-i for making cash withdrawals overseas.

**S** 12.3 Cardholders' responsibilities

Issuers shall provide a clear and prominent notice to cardholders at the point of entering into a contract, of cardholders' responsibilities to:

(a) abide by the terms and conditions for the use of the debit card-i;

(b) take reasonable steps to keep the debit card-i and PIN secure at all times, including at the cardholder's place of residence. These include not:

i. disclosing the debit card-i details or PIN to any other person;

ii. writing down the PIN on the debit card-i, or on anything kept in close proximity with the card;

iii. using a PIN selected from the cardholder's birth date, identity card, passport, driving licence or contact numbers; and

iv. allowing any other person to use the debit card-i and PIN.

(c) notify the issuer as soon as reasonably practicable after having discovered that the debit card-i is lost, stolen, an unauthorised transaction had occurred or the PIN may have been compromised;

(d) notify the card issuer immediately upon receiving short message service (SMS) transaction alert if the transaction was unauthorised;

(e) notify the card issuer immediately of any change in the cardholder's contact number;

(f) use the debit card-i responsibly, including not using the debit card-i for unlawful activity; and

(g) check the account statement and report any discrepancy without undue delay.

**S** 12.4 Liability for unauthorised transactions

(a) Issuers shall inform cardholders through clear and prominent notices that they would not be liable for card-present unauthorised transactions which require PIN verification, provided the cardholders have not:

(i) acted fraudulently;

(ii) delayed in notifying the issuers as soon as reasonably practicable after having discovered the loss or unauthorised use of the debit card-i;

(iii) voluntarily disclosed the PIN to another person; or

(iv) recorded the PIN on the debit card-i or on anything kept in close proximity with the card.

(b) Issuers shall inform cardholders through clear and prominent notices that they would not be liable for card-present unauthorised transactions which require signature verification or the use of a contactless card, provided the cardholders have not:

(i) acted fraudulently;

(ii) delayed in notifying the issuers as soon as reasonably practicable after having discovered the loss or unauthorised use of the debit card-i;

(iii) left the debit card-i or an item containing the card unattended in places visible and accessible to others; or

(iv) voluntarily allowed another person to use the debit card-i.

## 13 During the term of the contract

**S** 13.1 Statement

(a) For accounts without a passbook, issuers shall at least provide a monthly e-statement to cardholders, containing transaction details and the dates when those transaction amounts were posted to the account.

(b) If there are requests from cardholders for hardcopy statements, issuers shall facilitate the requests without any fee, unless otherwise approved by the Bank.

**S** 13.2 Closure of account

(a) Issuers shall allow cardholders to close their accounts at any time without being subjected to a cumbersome account closure procedure.

(b) Issuers shall disclose any penalty charge applicable to early closure of account within a specified time frame.

**S** 13.3 Change to the terms and conditions

(a) Should there be any change in the terms and conditions, issuers shall provide at least 21 calendar days' notice to cardholders before the new terms and conditions take effect. Necessary arrangement shall be made such as obtaining consent from contracting parties prior to any action made which is against the agreed terms and conditions.

(b) Any change in fees and charges applicable to the accounts shall be communicated by the issuers to cardholders at least 21 calendar days prior to the effective date of the change.

(c) Communication shall be done in writing or via electronic means to the cardholders.

**S** 13.4 Cardholders' responsibilities and awareness of fraud prevention measures

(a) Issuers shall send notices to cardholders at least once in every calendar year after card issuance to remind cardholders of the cardholders' responsibilities in paragraph 12.3.

(b) Issuers shall maintain on-going efforts to raise cardholders' awareness on potential liability for card-present unauthorised transactions due to the conditions specified in paragraphs 10.2 and 10.3, measures to prevent debit card-i fraud, including the need to safeguard the debit card-i and PIN.

(c) The reminders and information on fraud prevention measures shall be communicated to cardholders using channels that are effective in reaching the cardholders.

## D. MARKETING REQUIREMENTS

### 14 Advertisement

**S** 14.1 Issuers shall ensure that advertisements and promotional materials on debit card-i products are clear, fair and not misleading.

**S** 14.2 Issuers shall establish processes for an independent review of advertisement and promotional materials on debit card-i products, for instance by the Compliance Unit or Legal Unit and Shariah Committee to ensure that they are clear and not misleading.

**S** 14.3 For print media advertisement, the advertisement shall clearly and conspicuously disclose material information about any debit card-i offer that is likely to affect cardholders' decisions. Legible font size shall be used to bring cardholders' attention to any important information, relevant fees and charges and eligibility criteria to enjoy the benefits being offered.

**S** 14.4 Promotional materials shall provide adequate information on the key terms and conditions of the debit card-i product. The materials shall also contain information on the annual fee and any other applicable charges to facilitate comparisons by cardholders. The information shall be presented in plain language and in legible font size.

**S** 14.5 Issuers shall state prominently important terms and conditions associated with offers of free gifts, prizes, discounts or vouchers for the promotion of debit card-i in print advertisements, or in the marketing materials for new cardholders, or together with the account statements for existing cardholders.

**S** 14.6 In advertising special features or promotions in print or electronic media, the applicable eligibility criteria to enjoy the privileges shall be disclosed up-front with the announcement. The "applicable eligibility criteria" are those that are imperative to the advertised feature/promotion in addition to the basic terms and

conditions of holding the debit card-i. Issuers shall not merely indicate in a footnote that “terms and conditions apply”.

**S** 14.7 Advertisements or other promotional materials shall not describe any debit card-i feature as “free” or at “no cost” if there are conditions attached or other forms of charges will be imposed on cardholders.

## 15 Issuers’ other obligations

**S** 15.1 Issuers shall ensure that sales and customer service representatives (including call centres) are adequately trained and knowledgeable in the key features, benefits and risks of the debit card-i products, including the underlying Shariah contract.

**S** 15.2 Issuers shall apply due care and diligence when preparing information for use by sales and customer service representatives so that the information is sufficient, accurate, appropriate and comprehensive in substance and form. This is to ensure that cardholders are adequately informed by the sales and marketing representatives of the terms (including fees and charges), benefits and material limitations of the debit card-i product or services being offered.

**S** 15.3 Issuers shall establish procedures and take reasonable steps to ensure that cardholders’ expressed preference (e.g. not to be contacted on new product offers) are duly respected.

**S** 15.4 Issuers shall put in place adequate verification procedures to confirm the identity of debit card-i applicant to prevent the use of stolen information (e.g. identity theft) for debit card-i applications.

# E. OTHER REQUIREMENTS

## 16 Opt-in requirement for card-not-present and overseas transactions

**S** 16.1 Subject to paragraph 16.2 below, issuers must by default block any cardholder from making any card-not-present transaction which is not authenticated via strong authentication method such as dynamic password or any **overseas** transaction using a debit card-i.

**S** 16.2 Issuers must only allow a cardholder to make a card-not-present transaction which is not authenticated via strong authentication method such as dynamic password or an overseas transaction using a debit card-i, provided that the cardholder has expressly opted-in to conduct such transactions. For cardholders who wish to opt-in card-not-present or overseas transactions, issuers are required to inform the cardholders of the risks of such transactions, and also provide the cardholders with an option to subsequently disable such transactions.

## 17 Cardholder information

**S** 17.1 Issuers shall comply with the requirements on disclosure of customer information as specified under section 10 (under general policy requirements) of the Guidelines on Product Transparency and Disclosure.

## 18 Complaints management

**S** 18.1 Issuers shall comply with the complaints management requirements as specified in the Guidelines on Complaints Handling.

**S** 18.2 Issuers shall provide cardholders with information on how complaints may be made and the contact details of the issuer's complaints unit.

**S** 18.3 In the event an issuer extends the time period for the completion of an investigation beyond 14 calendar days from the date a disputed transaction is first reported, whether orally or in writing, the issuer shall:

(a) At a minimum, provisionally credit the full amount of the disputed transaction of RM5,000, whichever is lower (including any profit where applicable), into the cardholder's account no later than 14 calendar days from the date the cardholder provides the issuer with the following information, whether orally or in writing:
   (i) cardholder's name;
   (ii) affected account;
   (iii) date of disputed transaction;
   (iv) amount of the disputed transaction; and
   (v) reason why the cardholder believes that it is a disputed transaction;

(b) Credit the remaining amount of the disputed transaction (including any profit where applicable) no later than 30 calendar days from the date of the first crediting where the issuer has provisionally credited an amount into the cardholder's account in accordance with paragraph 18.3(a) which is lesser that the amount of the disputed transaction; and

(c) Allow the cardholder the full use of the provisionally credited funds.

**S** 18.4 In implementing paragraph 18.3, issuers shall provide adequate warning to cardholders of the actions that can be taken by the issuers against cardholders for any attempt to make false claims on the disputed transactions.

## 19 Usage of debit card-i for unlawful activities

**S** 19.1 Issuers shall include in the terms and conditions a clause specifying that the debit card-i is not to be used for any unlawful activities[1]. Issuers shall immediately terminate the debit card-i facility if the cardholders are discovered to have used the debit card-i for an unlawful activity.

[1] Activities which are forbidden by the law such as illegal online betting.

# PART D RISK MANAGEMENT

**S** The rapid pace of technological innovations has changed the scope, complexity and magnitude of risks that issuers and acquirers face in carrying out the debit card-i business. Issuers and acquirers shall have adequate processes and controls in place to manage and respond to such risks, including operational risks associated with the debit card-i business.

## 20 Effective management oversight

**S** 20.1 The Board of Directors and senior management of issuers and acquirers shall establish effective oversight measures, checks and balances, and risk management mechanism over the risks associated with their debit card-i operations, which include, among others, the following:

(a) Establishment of a comprehensive risk management process and internal controls for managing and monitoring risks associated with debit card-i operations.

(b) Establishment of processes for the review, approval and implementation of appropriate policies and procedures governing the debit card-i operations to ensure that the risks in the debit card-i operations are adequately mitigated.

(c) Oversight of the development and continued maintenance of the security infrastructure that safeguards the debit card-i systems and data from internal and external threats.

(d) Audit by an independent party[2] shall be conducted and undertaken with reasonable frequency to ascertain and detect weaknesses for prompt corrective measures to be taken in a timely manner.

(e) Establishment of a comprehensive and on-going due diligence and oversight process to manage outsourced arrangements and other third-party arrangements supporting the debit card-i operations.

**S** 20.2 The Board of Directors and senior management of issuers and acquirers shall also ensure that a strong management information system (MIS) is in place to support decision making, analysis and risk management.

## 21 Comprehensive security policies, procedures and controls

**S** Issuers and acquirers shall implement and enforce relevant policies and procedures to ensure confidentiality, integrity and availability of data as well as to ensure that the system and network infrastructure are safe and secure.

**S** 21.1 Robust security controls such as, intrusion detection and intrusion prevention systems and firewalls shall be put in place to secure the system and network infrastructure. In this regard, penetration tests shall be performed regularly to detect vulnerabilities for timely corrective measures to be taken to address security weaknesses.

[2] Internal or external auditor

**S** 21.2 Procedural and administrative controls on critical processes shall be put in place. Critical processes include, but are not limited to, the following:

(a) PIN generation and printing

PIN generation and printing processes are tasks that shall be performed in a highly secure environment. In this regard, the following shall, at the minimum, be observed:

(i) Usage of hardware-based PIN generation and verification.

(ii) Generated PINs shall be protected from being accessed or viewed by unauthorised persons.

(iii) The process of generating the PIN has to be strictly controlled. In this regard, PIN generation and printing area shall be strictly restricted to authorised personnel only.

(iv) Regeneration of the same PIN for the same card/account shall be prohibited.

(v) At least one independent party (which may be personnel independent of the process) shall be present to observe and check that the PIN generation and printing processes are undertaken in accordance with accepted procedures.

(b) Personalisation[3] process

(i) Personalisation process shall be performed in a secure environment. Access to personalisation machine, reader and data shall be strictly restricted and controlled.

(ii) Data used for personalisation shall be classified as confidential information and issuers shall ensure confidentiality and safety of the data that has been sent, stored and processed. These data shall be deleted upon completion of the process.

(iii) Sensitive keys used to perform personalisation shall be kept in a secure manner. Adequate policy and procedures shall be established to govern the management of such keys to ensure that they are safeguarded to prevent any unauthorised usage.

(iv) Periodic card inventory reconciliation and audit shall be performed on blank cards.

(v) Card personalisation centre shall ensure that the following controls are in place:

- Adequate physical and logical security controls.
- Segregation of duties and dual control.
- Network security control.

When the card personalisation process is outsourced, controls shall be in place to ensure that the data sent for personalisation to the outsourced vendors are secured. The issuers must monitor the outsourced vendor to ensure that the above requirements are met.

[3] A process of injecting/encoding customer data into the blank card's chip/magstripe; and embossing the cards with customer's details, e.g. name and expiry date.

**S** 21.3 Effective segregation of functions on handling of debit card-i and PIN shall be observed at all stages of processing, particularly the following:

(a) Card processing (e.g. embossing and encoding processes) and PIN generation functions.

(b) Physical management of card and PIN, including mailing (if applicable).

**S** 21.4 Effective dual control over critical functions shall be implemented. Critical functions include the following:

(a) Setting and maintaining all system parameters.

(b) PIN generation processes and handling of secret keys or codes and other security features.

(c) Handling and safekeeping of blank cards.

(d) Handling of returned and undelivered debit card-i.

**S** 21.5 Necessary measures shall be taken to ensure the confidentiality of debit card-i data and information.

(a) Confidential data and sensitive information shall be protected from unauthorised viewing or modification during transmission and storage.

(b) Sensitive information shall be encrypted from end to end during transmission over the network.

(c) Minimal account information shall be printed on sales draft to minimise the risk of misuse of information to conduct fraudulent “card-not-present” transactions.

(d) Storage of sensitive authentication data, e.g. magnetic stripe data, PIN and validation code (e.g. card verification value (CVV) used to verify card-not-present transactions) shall not be allowed as this information may be used by fraudsters to generate fake debit card-i and create fraudulent transactions.

(e) Confidential data and sensitive information shall only be accessible and managed by authorised parties.

**S** 21.6 Proper identification and authentication method (e.g. passwords and PINs) shall be adopted to avoid unauthorised usage of debit card-i as well as unauthorised access to system, network and data. For more robust security, the following shall be adopted at the minimum:

(a) PIN shall be at least six digits in length. Password shall be alphanumeric and at least six characters in length. Where possible, the use of strong PIN/password shall be adopted.

(b) Maximum PIN/password tries shall be limited to three on an accumulated basis.

(c) PIN shall not be stored permanently in any format or media. Passwords shall be securely maintained.

(d) If the PIN/password is computer-generated and is not chosen by the cardholder, mandatory PIN/password change shall be adopted before the first transaction is permitted.

(e) Cardholders shall be allowed to change the PIN/password at any time.

(f) Cardholders shall be advised that they shall not use a PIN/password selected from the cardholder’s birth date, identity card, passport, driving licence or contact numbers to mitigate unauthorised use of their debit card-i in the event their cards are lost or stolen.

**S** 21.7 Disposal of debit card-i related materials/assets, such as damaged or returned cards, reports and embossing machines shall be performed in a controlled environment.

## 22 Robust operational reliability and business continuity

**S** A high level of system availability is required to maintain public confidence. Issuers and acquirers shall ensure that they have the resources and capacity in terms of hardware, software and other operating capabilities to deliver consistently reliable and secure services.

**S** 22.1 Measures to ensure operational reliability include, but are not limited to, the following:

(a) Strong internal controls for system and personnel administration.
(b) Comprehensive and well-documented operational and technical procedures to ensure operational reliability.
(c) Sufficient capacity to support business requirements.
(d) A robust business continuity and disaster recovery plan, including a highly reliable backup system.

## 23 Outsourcing risk management

**S** Outsourcing does not reduce the fundamental risk associated with debit card-i operations. Neither does it absolve the issuers and acquirers from their responsibilities of having to manage the risks of their debit card-i operations. As such, issuers and acquirers that outsource any part of their debit card-i operations shall observe the minimum requirements set out below.

**S** 23.1 Prior to entering into any outsourcing arrangement, the following shall, at the minimum, be considered:

(a) Availability of sufficient expertise within the issuer/acquirer to oversee and manage the outsourcing relationship.
(b) Scope and nature of services/operations to be outsourced would not compromise the controls and risk management of the debit card-i business:
    (i) The outsourcing of such processes does not take away the critical decision making function of the issuers and acquirers.
    (ii) The outsourcing of such processes does not threaten strategic flexibility and process control of the issuers and acquirers.
    (iii) The outsourcing of such functions would not impair the image, integrity and credibility of the issuers and acquirers.

**S** 23.2 Issuers and acquirers shall also perform appropriate due diligence review of the integrity, competency and financial viability of the outsourcing service provider before the arrangements are formalised.

**S** 23.3 Approval from the Board of Directors of issuers and acquirers to outsource their functions must be obtained and documented.

**S** 23.4 The outsourcing service providers must provide a written undertaking to the issuers and acquirers to comply with the secrecy provision pursuant to section 133 of the FSA and section 145 of the IFSA.

**S** 23.5 The external and internal auditors of the issuers and acquirers must be able to review the books and internal controls of the outsourcing service providers. Issuers and acquirers shall ensure that any weaknesses highlighted during the audit are well-documented and promptly rectified by the outsourcing service providers especially where such weaknesses may affect the integrity of the internal controls of the issuers and acquirers.

**S** 23.6 The outsourcing agreement shall be comprehensive and include the following:

(a) Clearly defined roles, responsibilities and obligations of the service provider.

(b) Clear provisions for the Bank to enter the premises of the service provider to conduct examination and investigation with regard to the services outsourced, should the need arise.

(c) Conditions under which the outsourcing arrangement may be terminated.

**S** 23.7 The issuers and acquirers must also have a contingency plan in the event that the arrangement with the outsourcing service provider is suddenly terminated. This is to mitigate any significant discontinuity in the work that is supposed to be conducted by the service provider.

(a) The contingency plan must be reviewed from time to time to ensure that the plan is current and ready for implementation in the event of sudden termination of the service provider.

(b) The contingency plan must also be approved by the Board of Directors of the issuers and acquirers.

**S** 23.8 Although the operational activities of debit card-i are outsourced, reporting and monitoring mechanisms shall be put in place by issuers and acquirers to ensure that the integrity and quality of work conducted by the outsourced service provider is maintained.

**S** 23.9 Regular reviews shall be conducted on the outsourcing service provider to ensure the suitability and performance of the service providers.

**S** 23.10 Periodic independent internal and/or external audits shall be conducted on the outsourced operations with at least the same scope of review as if the operations had been conducted in-house.

## 24 Fraud risk management

**S** Issuers and acquirers shall be vigilant of the evolving typologies of fraud and monitor such developments on an on-going basis.

**S** 24.1 Issuers and acquirers shall deploy effective and efficient fraud detection and monitoring mechanism.

(a) Fraud detection and monitoring of transactions shall be conducted on an on-line real time basis.

(b) The fraud detection and monitoring mechanism shall be able to capture high risk transactions and trigger any detection of unusual transactions.

(i) Issuers shall put in place criteria for high risk transactions and merchants to facilitate early detection of fraud.

(ii) Issuers shall put in place procedures to facilitate early detection of unusual transaction pattern or trend that could be indicative of fraud and take necessary action to block/delay these transactions for further investigation.

**S** 24.2 Issuers and acquirers shall establish comprehensive fraud investigation, analysis and reporting procedures.

(a) Issuers and acquirers shall conduct regular analysis to understand the fraud trend and modus operandi.

(b) Adequate risk management processes, systems and controls shall be in place, and where necessary, strengthened, to mitigate fraud risk. This include taking into account developments in fraud trend and material changes in the business strategy which may increase exposure to potential fraud risk.

(c) Assessment of fraud incidents shall be reported to senior management and the Board on a regular basis. Reporting to the Bank shall be in accordance to the fraud reporting requirement imposed by the Bank from time to time.

### Fraud prevention mechanism

**S** Fraud may take place at different stages of the debit card-i process, i.e. card application, card delivery, card activation, change of cardholder's contact details as well as when the card is used by the cardholder. In this regard, issuers and acquirers shall put in place effective measures to address fraud risk. The fraud risk management measures shall be reviewed periodically for proactive actions to be taken to address any inadequacies in such measures.

***Minimum fraud mitigation measures for card application, delivery and activation***

**S** 24.3 The following shall be observed at the point of collecting debit card-i applications from applicants:

(a) Issuers shall ensure the confidentiality of the data and information provided by the applicant. Necessary measures shall be put in place to ensure that the information provided by the applicant would not be misused by the persons authorised by the issuer to collect the

application(s).

(b) Issuers or any persons acting on behalf of the issuers to collect debit card-i applications are prohibited from photocopying the applicants' other debit card-i. This is because debit card-i security features which are used for cardholder authentication are available on the card itself such as card number, CVV and expiry date of the debit card-i.

**S** 24.4 The following controls shall be taken into consideration when processing debit card-i applications:

(a) The identity of the applicant must be verified to ensure that the applicant exists and is the person applying for the card.

(b) Key information provided by the applicant must be verified for accuracy.

(c) Issuers must ensure the confidentiality of the data and information provided by the applicant.

**S** 24.5 Issuers are prohibited from sending out active debit card-i to its cardholders. Stringent activation procedures, which shall include proper verification process that cannot be easily bypassed by fraudsters and by its own employees, must be implemented.

***Requirements when changing cardholder's contact details***

**S** 24.6 To mitigate the risk of account takeover, issuers shall put in place effective measures to verify any request it receives for change of mailing address, shipment of new or replacement card or PIN and telephone numbers.

**G** 24.7 The following are some practices that issuers may consider to adopt to mitigate the risk of account takeover:

(a) Allow request for change of contact details only if it is made in person at the issuer's premises.

(b) Allow such request through secured electronic mode (e.g. electronic banking) but subject to further verification before updating the contact details.

(c) Send written correspondence to the previous address for verification before shipping any card or PIN to the new address.

***Implementation of "Chip and PIN" technology***

**S** 24.8 In line with efforts to enhance the security features of debit card-i, all issuers and acquirers shall enable chip and PIN verification for debit card-i transactions at point-of-sale (POS) terminals and cash withdrawals at automated teller machines (ATMs).

***Implementation of strong authentication method for non face-to-face transactions***

**S** 24.9 Non face-to-face transactions, i.e. card-not-present transactions, especially online payments, present a higher fraud risk level compared to face-to-face debit card transactions. Issuers and acquirers shall authenticate cardholders for online transactions using strong authentication method, such as dynamic password/PIN and multi-factor authentication (e.g. mobile PKI), to mitigate the risk of unauthorised use of debit card-i for online transactions.

***Implementation of transaction alerts***

**S** 24.10 Issuers shall provide transaction alerts via SMS to their cardholders, unless cardholders have opted to receive transaction alerts via other channels, such as e-mail. This shall be applicable to the following:
(a) Purchase transactions at POS terminals.
(b) Online transactions.
(c) Cash withdrawal transactions.
(d) Mail and telephone order transactions.

**S** 24.11 Issuers shall provide an alternative way to alert cardholders if they do not wish to send transaction alerts via SMS to foreign-registered mobile numbers. Issuers shall obtain written consent from the cardholders for this arrangement.

**S** 24.12 Issuers shall take into consideration the following criteria to identify high risk transactions and trigger transaction alerts:
(a) Transaction type, e.g. transaction at high risk merchants[4].
(b) Transaction location, e.g. transaction in high risk countries[5].
(c) Transaction amount, e.g. transaction exceeding certain amount.
(d) Transaction velocity, e.g. transaction exceeding certain number per day.

**S** 24.13 Issuers shall provide transaction alerts to cardholders in the event any of the following triggers are met:
(a) Transactions exceeding a specified threshold amount. In this regard, issuers shall set the threshold amount to trigger an alert. The threshold amount or any upward revision to the threshold amount requires endorsement from the Bank. Issuers shall also allow cardholders to set their own preferred threshold amount for the transaction alert. If cardholders do not set the preferred threshold amount, issuers shall send transaction alerts based on the default threshold amount set by the issuer. Cardholders shall be informed of their rights to set their own preferred threshold for the alert.
(b) For contactless transactions, a **reasonable threshold amount** shall be set. Issuers shall notify the Bank of the threshold amount or any upward revision to the threshold amount.
(c) First time use of new card.
(d) All card-not-present transactions.

[4,5] To be identified by the issuer/industry.

(i) Issuers are not required to send transaction alerts for recurring auto-debit transactions. However, issuers shall take the necessary steps to ensure the auto-debit transaction is a genuine transaction and disputes, if any, are handled appropriately so that cardholders are sufficiently safeguarded.

(e) High risk transactions (please refer to paragraph 24.12).

**S** 24.14 By default, the alert must be sent for transactions meeting the specified criteria as stated in paragraphs 24.10 and 24.13, except where the cardholders opt not to receive any alerts. In this regard, issuers must ensure that the debit cardholders:

(a) understand the risks associated with their decision; and

(b) submit such request in writing.

**G** 24.15 Issuers may consider sending transaction alerts for circumstances other than the above.

**S** 24.16 To ensure the effectiveness of the alerts, issuers must ensure that the contact numbers of their cardholders are kept up-to-date. As such, issuers must highlight to their cardholders the criticality of providing updated contact numbers to them. Issuers shall authenticate that the contact details are provided by the debit cardholders.

**S** 24.17 To mitigate abuse, issuers shall not provide any contact number as part of the message in the SMS alert.

**G** 24.18 Issuers should advise cardholders to contact their card centre and use the contact number indicated at the back of their debit card-i.

**S** 24.19 Issuers shall not transfer the cost of sending SMS alerts to their cardholders.

**G** 24.20 Issuers may stop sending transaction alert for transactions which require PIN verification at POS terminals and cash withdrawal transactions only after the full implementation of chip and PIN technology and for online transactions after the adoption of strong authentication method.

**Transaction and ATM withdrawal limit**

**S** 24.21 Cardholders shall be allowed to set their preferred limit for transactions at POS terminal and ATM withdrawals.

**Exchange of information and dissemination**

**G** 24.22 Sharing of information regarding fraud experiences and modus operandi is encouraged among issuers and acquirers as this will enhance efforts to combat fraud.

**G** 24.23 Issuers and acquirers should also be resourceful in gathering relevant information from the industry, their overseas counterparts and the card associations. Having first-hand information will assist them to decide on specific

measures to strengthen their defence mechanism against fraudsters.

**G** 24.24 Close cooperation with law enforcers and regulators should also be established to facilitate sharing of fraud experiences and modus operandi to combat fraud.

**Contactless verification requirements**

**S** 24.25 Issuers shall set a maximum amount for each contactless transaction as well as an appropriate cumulative limit for contactless transactions which do not entail any cardholder verification.

**S** 24.26 To promote confidence in the use of contactless debit card-i by providing cardholders with the ability to manage the cumulative transaction limit, issuers shall undertake the following:

(a) Provide cardholders with the facility to set a lower cumulative transaction limit for contactless transactions minimally via issuers' branches;

(b) Provide cardholders with the facility to turn off the contactless functionality in contactless debit card-i minimally via issuers' branches; and

(c) Raise awareness among cardholders about the facilities set out in paragraphs (a) and (b) minimally via the issuers' websites and product disclosure sheet.

**S** 24.27 Issuers shall ensure that verification is conducted once transactions exceed the maximum amount or the cumulative limit for contactless transactions, i.e. either in signature or PIN until 31 December 2016. From 1 January 2017, which is the date that chip and PIN is mandated, the cardholder verification method for all payment cards shall only be done via chip and PIN.

## 25 Specific requirements for acquirers

**S** Acquirers shall be vigilant to ensure that they are not used by merchants as a means to obtain funds through illegal means and fraudulent acts. Controls must be put in place both prior to engaging the merchant and on an on-going basis.

**S** 25.1 Acquirers shall establish the criteria for merchant selection and recruitment, and establish policies and procedures for on-going monitoring of their merchant accounts, which shall include risk criteria to evaluate the risk profile of their merchants for appropriate risk management measures to be taken on a timely basis.

***Merchant recruitment***

**S** 25.2 Acquirers shall establish prudent underwriting criteria and procedures for approving new merchants. The criteria for assessing new merchants shall also cover financial strength and relevant background details (e.g. has not been declared a bankrupt, has a clean fraud track record and has not been blacklisted by other acquirers).

**S** 25.3 Acquirers must ensure that the merchant has a legitimate business and is not involved in, or associated with, any illegal activities or schemes, including business activities that are meant to deceive consumers, such as schemes like "scratch and win" and "get-rich-quick".

**S** 25.4 If a third party merchant recruitment agent is engaged, acquirers shall ensure that proper controls are in place to ensure that the third party merchant recruitment agent complies with relevant requirements set out in this policy document.

***Merchant monitoring and audit***

**S** 25.5 Acquirers shall monitor the trend in chargebacks and the merchants' capacity to repay these chargebacks and act accordingly to mitigate any risks associated with engaging such merchants.

**S** 25.6 Acquirers shall take appropriate risk management measures on their high risk merchants, including conducting more frequent audit/checks on these merchants and more stringent monitoring of transactions that pass through these merchants.

**S** 25.7 The relationship with merchants with confirmed fraudulent or illegal activity must be immediately terminated. Whenever the merchant has been terminated or blacklisted due to fraud-related matters by one of the acquirers, other acquirers shall be vigilant and gather relevant information and evidence on the conduct of the said merchant.

**S** 25.8 Acquirers shall conduct continuous due diligence on their merchants to ensure that merchants are not involved in any fraudulent or illegal activity and maintain a "watch list" of suspected collusive merchants, if any. The activities of these merchants shall be closely monitored and investigated. Once identified as collusive, acquirers shall immediately terminate their acquiring relationship with the merchant.

**S** 25.9 Acquirers shall conduct periodic audits on the merchants to ensure that merchants adhere to card acceptance and authorisation procedures to minimise chargeback and disputes.

## 26 Compliance with other requirements

**S** 26.1 Issuers shall comply with other relevant requirements issued by the Bank from time to time.

## Appendix 1 Product Disclosure Sheet - Debit Card-i

| **PRODUCT DISCLOSURE SHEET**<br><br>**(Read this Product Disclosure Sheet before you decide to take out the <Name of Product>. Be sure to also read the general terms and conditions.)** | <Name of Financial Service Provider><br><br><Name of Product><br><br><Date> |
|---|---|

**1. What is this product about?**

This is a debit card-i, a payment instrument which allows you to pay for goods and services from your deposit account at participating retail and service outlets. You are required to maintain a deposit account with us, to be linked to your debit card-i. If you close your deposit account maintained with us, your debit card-i will be automatically cancelled.

**2. What are the fees and charges I have to pay?**

- Annual fee
- Domestic ATM withdrawal fee
- Overseas transaction conversion fee
- Card replacement fee
- Sales draft retrieval fee
- Additional statement request fee
- Others

**3. What are the key terms and conditions?**

- **Pre-authorisation for payment using debit card-i**
  Pre-authorisation amount of RMxx will be charged to your deposit account when you make payment using your debit card-i at automated fuel dispenser. We will only post the exact amount of transaction and release any extra hold amount from your account within 3 working days after the transaction date.

**4. What if I fail to fulfil my obligations?**

- You will be liable for PIN-based unauthorised transactions if you have:
  - acted fraudulently;
  - delayed in notifying us as soon as reasonably practicable after having discovered the loss or unauthorised use of your debit card-i;
  - voluntarily disclosed your PIN to another person; or
  - recorded your PIN on the debit card-i, or on anything kept in close proximity with your debit card-i.

- You will be liable for unauthorised transactions which require signature verification or with contactless card, if you have:
  - acted fraudulently;
  - delayed in notifying us as soon as reasonably practicable after having discovered the loss or unauthorised use of your debit card-i;
  - left your debit card-i or an item containing your debit card-i unattended in places visible and accessible to others; or
  - voluntarily allowed another person to use your debit card-i.

***(To highlight other key terms and conditions)***

**5. What are the major risks?**

The risk of your card being stolen or lost. You should notify us immediately after having discovered the loss or unauthorised use of your debit card-i.

**6. What do I need to do if there are changes to my contact details?**

It is important that you inform us of any change in your contact details to ensure that all correspondences reach you in a timely manner.

**7. Where can I get further information?**

If you have any enquiries, please contact us at:

ABC Bank Berhad
51, Jalan Sultan Ismail
50122 Kuala Lumpur
Tel:
Fax:
E-mail:

**8. Other debit card packages available**

- Abc
- Xyz

The information provided in this disclosure sheet is valid as at dd/mm/yy.

Issued on: 2 December 2016