Title
Debit Card-i

Issuance Date
28-Feb-2014

Effective Date
The policy document: **28 February 2014**

Paragraph 23.8 - Implementation of "Chip and PIN" technology at:
(a) Automated teller machine (ATM): **1 January 2015**
(b) Point-of-sale terminals (POS): **1 January 2017**

Applicability
DFIA
IFSA

Summary
Part 1 of the policy document outlines specific requirements and minimum standards to be observed by debit card-i issuers and acquirers while Part 2 of the policy document outlines the risk management principles and requirements for debit card-i issuers and acquirers.

Issuing Department
Consumer and Market Conduct
Islamic Banking and Takaful
Payment Systems Policy

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Debit Card-i

Issued on: 28 February 2014

OVERVIEW 1

1. INTRODUCTION 1
2. APPLICABILITY 1
3. SCOPE 1
4. LEGAL PROVISIONS 1
5. EFFECTIVE DATE 2
6. INTERPRETATION 2

PART 1 4

A. APPROVED SHARIAH CONCEPT APPLIED IN DEBIT CARD-i 4

7. SHARIAH CONCEPT 4
8. SHARIAH REQUIREMENTS 4

B. FEES AND CHARGES 4

9. GUIDING PRINCIPLE ON FEES AND CHARGES 4

C. DISCLOSURE AND TRANSPARENCY REQUIREMENTS 4

10. PRE-CONTRACTUAL STAGE 5
11. AT THE POINT OF ENTERING INTO A CONTRACT 6
12. DURING THE TERM OF THE CONTRACT 7

D. LIABILITY 9

13. LIABILITY FOR UNAUTHORISED TRANSACTIONS 9

E. MARKETING REQUIREMENTS 10

14. ADVERTISEMENT 10
15. ISSUER'S OTHER OBLIGATIONS 11

F. OTHER REQUIREMENTS 12

16. CARDHOLDER INFORMATION 12
17. COMPLAINTS MANAGEMENT 12
18. USAGE OF DEBIT CARD-i FOR UNLAWFUL ACTIVITIES 12

PART 2 13

G. RISK MANAGEMENT 13

19. EFFECTIVE MANAGEMENT OVERSIGHT 13
20. COMPREHENSIVE SECURITY POLICIES, PROCEDURES AND CONTROLS 14
21. ROBUST OPERATIONAL RELIABILITY AND BUSINESS CONTINUITY 17
22. OUTSOURCING RISK MANAGEMENT 18
23. FRAUD RISK MANAGEMENT 20

24. SPECIFIC REQUIREMENTS FOR ACQUIRERS 26

25. COMPLIANCE WITH OTHER REQUIREMENTS 27

APPENDICES 28

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.

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 individuals; micro, small and medium enterprises (SMEs); and corporate cardholders with the exception of requirements under sections 9 to 15 under Part 1 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. SCOPE

3.1 Part 1 of this policy document outlines specific requirements and minimum standards to be observed by debit card-i issuers and acquirers.

3.2 Part 2 of this policy document outlines risk management principles and requirements for debit card-i issuers and acquirers.

4. LEGAL PROVISIONS

4.1 The requirements in this policy document are issued pursuant to:

(a) Section 43(1), 57(1) and 135(1) of the Islamic Financial Services Act 2013 (IFSA); and

(b) Sections 41 and 126 of the Development Financial Institutions Act 2002 (DFIA).

5. EFFECTIVE DATE

5.1 This policy document comes into effect on 28 February 2014.

(a) Paragraph 23.8: Implementation of "Chip and PIN" technology:

(i) at automated teller machine (ATM) comes into effect on 1 January 2015; and

(ii) at point-of-sale (POS) terminals comes into effect on 1 January 2017

6. INTERPRETATION

6.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the IFSA.

6.2 In the event that the terms or expressions are defined otherwise, it is only for the purpose of clarification but shall be consistent with the meanings assigned to them under the IFSA.

6.3 For the purpose of this policy document:

"S" denotes a standard, requirement or specification that must be complied with. Failure to comply may result in one or more enforcement actions.

"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.

"Debit card-i" refers to an Islamic payment instrument based on Shariah principles that is linked to a deposit account at a financial institution that can be used –

(i) to pay for goods and services;

(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

(iii) for the purposes of (i) and (ii).

"Issuer" refers to a person who has obtained approval from Bank Negara Malaysia (BNM) under section 11 of the IFSA or section 15 of the Financial Services Act 2013 (FSA) 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 BNM.

PART 1

A. APPROVED SHARIAH CONCEPT APPLIED IN DEBIT CARD-i

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.

B. FEES AND CHARGES

9. GUIDING PRINCIPLE 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.

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, that 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.

10. PRE-CONTRACTUAL STAGE

S 10.1 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 10.2 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 10.3 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.

11. AT THE POINT OF ENTERING INTO A CONTRACT

S 11.1 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. 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 11.2 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 11.3 Cardholders' responsibilities

Issuers shall highlight to cardholders at the point of entering into a contract, of their responsibilities to:

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

(b) safeguard the debit card-i and Personal Identification Number (PIN). Cardholders shall be advised not to disclose the debit card-i details or PIN to anyone;

(c) report lost debit card-i/PIN as soon as reasonably practicable;

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

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

S 11.4 Liability for unauthorised transaction

(a) Issuers shall inform the cardholders, through clear and prominent notices, that the maximum liability unauthorised transaction(s) as a consequence of a lost or stolen debit card-i shall be limited at RM250, provided the cardholders have not acted fraudulently or have not failed to inform the issuers as soon as reasonably practicable after having found that their debit card-i are lost or stolen.

(b) Issuers shall warn the cardholders that their liability for loss may exceed the maximum amount of RM250 if the cardholders are found to have acted fraudulently or failed to inform the issuers as soon as reasonably practicable after having found that their debit card-i are lost or stolen.

S 11.5 Change of contact details

(a) Issuers shall inform cardholders of the importance of notifying the issuers of any change in contact details.

12. DURING THE TERM OF THE CONTRACT

S 12.1 Statement

(a) For accounts without a passbook, issuers shall provide an account statement to cardholders at least once a quarter, containing information on transaction records and the dates when those amounts were posted

to the account. The frequency of the account statement to be mailed shall be made known to the cardholders.

(b) If the cardholders request for additional statements, issuers shall inform the cardholders of the charges, if any, upon the request of such statements.

(c) For cardholders that opt to receive e-statements, issuers shall ensure that the information on the e-statement is the same as the hardcopy statement.

S 12.2 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 12.3 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 the cardholders at least 21 calendar days prior to the effective date of the change.

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

12.4 Awareness of fraud prevention measures

S (a) Issuers shall maintain on-going efforts to raise cardholders' awareness on measures to prevent debit card-i fraud, including the need to safeguard the debit card-i and PIN.

G (b) The information on fraud prevention measures may be communicated via the account statement.

D. LIABILITY

13. LIABILITY FOR UNAUTHORISED TRANSACTIONS

S 13.1 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 13.2 Cardholders' maximum liability for unauthorised transactions as a consequence of a lost or stolen debit card-i shall be confined to a limit specified by issuers, which shall not exceed RM250, provided the cardholders have not acted fraudulently or have not failed to inform the issuers as soon as reasonably practicable after having found that their debit card-i are lost or stolen.

S 13.3 Where the amount imposed on the cardholders for unauthorised transactions due to lost or stolen debit card-i is in excess of the maximum liability limit, the issuers have to prove that the cardholders have acted fraudulently or failed to inform the issuers as soon as reasonably practicable after having found that their debit card-i are lost or stolen.

S 13.4 Issuers shall have clear processes in place to register any notification of lost or stolen debit card-i and take immediate action upon notification by the cardholders, to prevent further use of the lost or stolen 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, that their debit card-i are lost or stolen.

S 13.5 Issuers shall maintain on-going efforts to increase awareness of the cardholders' potential liability for unauthorised transactions if they have acted fraudulently or have failed to inform the issuers as soon as reasonably practicable upon discovery of the loss or theft of the debit card-i. The

information may be communicated via SMS alerts, account statements and notices displayed on the issuers' websites.

E. 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 promotion 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 Promotion 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 promotion 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. ISSUER'S 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.

F. OTHER REQUIREMENTS

16. CARDHOLDER INFORMATION

S 16.1 Issuers shall comply with the requirements on disclosure of customer information as specified under section 10 (under general policy requirements) of the Guidelines on Products Transparency and Disclosure.

17. COMPLAINTS MANAGEMENT

S 17.1 Issuers shall comply with the complaints management requirements as specified in the "Guidelines on Complaints Handling" issued by BNM.

S 17.2 Issuers shall provide cardholders with information on how complaints may be made and the contact details of the issuer's complaints unit.

18. USAGE OF DEBIT CARD-i FOR UNLAWFUL ACTIVITIES

S 18.1 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 found 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 2

G. 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.

19. EFFECTIVE MANAGEMENT OVERSIGHT

S 19.1 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 the 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.

[2] Internal of external auditor

S 19.2 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.

20. 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 20.1 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.

S 20.2 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.

S 20.3 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.

---

[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.

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

S 20.4 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 20.5 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 20.6 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 their date of birth, identity card number or mobile number as their PIN or password to mitigate unauthorised usage of their debit card-i in the event their debit card-i is lost or stolen.

S 20.7 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.

21. 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 21.1 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 of the system to support business requirements.

(d) A robust business continuity and disaster recovery plan, including a highly reliable backup system.

22. 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 22.1 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 22.2 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 22.3 Approval from the Board of Directors of issuers and acquirers to outsource their functions must be obtained and documented.

S 22.4 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 22.5 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 shall 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 22.6 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 BNM 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 22.7 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 22.8 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 22.9 Regular reviews shall be conducted on the outsourcing service provider to ensure the suitability and performance of the service providers.

S 22.10 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.

23. 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 23.1 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 23.2 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 BNM shall be in accordance to the fraud reporting requirement imposed by BNM from

time to time.

Fraud prevention mechanism

S Fraud may take place at different stages of the debit card-i, 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 should 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 23.3 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 cards. 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 23.4 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 23.5 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 23.6 To mitigate the risk of account takeover, issuers shall put in place effective measures to verify any request it received for change of mailing address, and shipment of new or replacement card or PIN and telephone numbers.

G 23.7 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 23.8 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 23.9 Non face-to-face transactions, i.e. card-not-present transactions, especially online payments, presents a higher fraud risk level compared to face-to-face debit card-i transactions. Issuers and acquirers shall authenticate cardholders for online transactions using strong authentication methods, 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 23.10 Issuers shall implement transaction alerts via short message service (SMS) to their debit cardholders, unless cardholders opt 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 23.11 Issuers shall provide an alternative way to alert cardholders if they do not wish to send transaction alerts via SMS to foreign phone numbers. Issuers shall obtain written consent from the cardholders for this arrangement.

S 23.12 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 23.13 Issuers shall send transaction alerts in the event any of the following trigger is 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 BNM. 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

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

the issuer. Cardholders shall be informed of their rights to set their own preferred threshold for the alert.

(b) First time use of new card.

(c) All card-not-present transactions.

(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.

(d) High risk transactions (please refer to 23.12).

S 23.14 By default, the alert must be sent for transactions meeting the specified criteria as stated in paragraphs 23.10 and 23.13, 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 23.15 Issuers may consider sending transaction alerts for circumstances other than the above.

S 23.16 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 23.17 To mitigate abuse, issuers shall not provide any contact number as part of the message in the SMS alert.

G 23.18 Issuers should advise cardholders to contact their card centre and use the contact number indicated at the back of their debit card-i.

S 23.19 Issuers shall not transfer the cost of sending SMS alerts to their cardholders.

G 23.20 Issuers may stop sending transaction alert for purchase transactions 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 23.21 Cardholders shall be allowed to set their preferred limit for transactions at POS terminal and ATM withdrawals.

Exchange of information and dissemination

G 23.22 Sharing of information regarding fraud experiences and modus operandi is encouraged among issuers and acquirers as this will enhance efforts to combat fraud.

G 23.23 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 23.24 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 23.25 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 23.26 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.

24. 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 24.1 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 24.2 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 24.3 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 24.4 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 24.5 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 24.6 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 24.7 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 24.8 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 24.9 Acquirers shall conduct periodic audits on the merchants to ensure that merchants adhere to card acceptance and authorisation procedures to minimise chargeback and disputes.

25. COMPLIANCE WITH OTHER REQUIREMENTS

S 25.1 Issuers shall comply with other relevant requirements issued by BNM from time to time.

APPENDICES

Appendix 1 Product Disclosure Sheet – Debit Card-i

PRODUCT DISCLOSURE SHEET **(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> <Name of Product> <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 term and conditions?

- **Pre-authorisation for payment using debit card-i**
  Pre-authorisation amount of RMXXX will be charged to your payment instrument account / banking 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?

- Your liability for unauthorised transactions.
  (To highlight other key terms and conditions.)

5. What are the major risks?

Your card being stolen or lost. You should notify us immediately after having found that your debit card-i is

lost or stolen.

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-i packages available

- abc
- xyz

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