BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Debit Card and Debit Card-i

Applicable to -

1. Approved issuers of debit card and debit card-i
2. Registered merchant acquirers of debit card and debit card-i

Issued on: 19 December 2025 BNM/RH/PD 028-140

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 Debit card and debit card-i usage continues to grow and remains a key payment instrument in Malaysia. In tandem with the continued increase in usage of payment cards, particularly for e-commerce transactions both domestically and internationally, the potential exposure of payment cards to fraud has also risen which could impact the integrity of the payment system. This limited review aims to enhance business conduct, strengthen risk management, and improve fraud prevention and case handling of debit cards, to preserve users' confidence in the overall payment card ecosystem.

2 Applicability

2.1 This policy document is applicable to all debit card and debit card-i (debit card products) issuers and acquirers, with the exception of paragraphs 8.1, 8.2, 8.3 and 9.1 which are only applicable to debit card-i issuers.

2.2 The requirements of this policy document shall apply to issuers of debit card products offered to:

(a) Individuals;
(b) Micro, small and medium enterprises (MSMEs); and
(c) Corporate cardholders,

with the exception of requirements under sections 10, 11, 14 and 16 under Part C which shall only apply to issuers of debit card products issued to individuals, micro and small enterprises. However, issuers are encouraged to adopt similar standards under these sections for debit card products offered to medium enterprises and other corporate cardholders.

3 Legal provisions

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

(a) Sections 18(2), 33(1), 47(1), 49 and 123(1) of the Financial Services Act 2013 (FSA);
(b) Sections 29(1), 29(2), 43(1), 57(1) and 135(1) of the Islamic Financial Services Act 2013 (IFSA); and
(c) Sections 33(E)(1), 33(E)(2), 41(1) and 42(C)(1) of the Development Financial Institutions Act 2002 (DFIA).

3.2 The guidance in this policy document is specified pursuant to section 266 of the FSA, section 277 of the IFSA, and section 126 of the DFIA.

4 Effective date

4.1 This policy document comes into effect immediately upon issuance.

4.2 Requirements which have other effective dates are as follows:
(a) Paragraphs 17 and 18 which come into effect on 1 April 2026;
(b) Paragraph 11.2 on -
(i) new debit card products which comes into effect on 1 June 2026;
(ii) existing debit card products which comes into effect on 1 January 2027; and
(c) Paragraphs 25.4, 25.6, 28.3, 28.4, 29.1, 31.1, 32, 34.2, 34.3(e) and 34.4(f) which come into effect on 1 January 2027.

5 Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the FSA, 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;

"acquirer" refers to any person who has been registered by the Bank under section 18(1) of the FSA to provide merchant acquiring services;

"Bank" refers to Bank Negara Malaysia;

"debit card" 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 -
(i) To pay for goods and services;
(ii) To withdraw cash from automated teller machines or withdraw cash at participating retail outlets through debit card usage by debiting the user's account; or
(iii) For the purposes of (i) and (ii) above.

"debit card-i" refers to an Islamic payment instrument based on Shariah principles that is linked to an investment account, deposit account, current account, savings account or other similar account at a financial institution that can be used-

(i) To pay for goods and services;
(ii) To withdraw cash from automated teller machines or withdraw cash at participating retail outlets through debit card usage by debiting the user's account; or
(iii) For the purposes of (i) and (ii) above.

"financial institution" refers to any person licensed under the FSA or the IFSA or a prescribed institution under the DFIA;

"issuer" refers to a person who has obtained approval from the Bank under section 11 of the FSA to issue debit card, or section 15 of the FSA or section 11 of the IFSA to issue debit card-i;

"micro, small and medium-sized enterprises" is as defined in the Guideline for SME Definition issued by the SME Corporation Malaysia[1];

"representatives" and "agents" refer to any individual or firm acting on behalf of an issuer or acquirer;

"senior management" refers to the chief executive officer (CEO) and senior officers, who are employed by a financial institution or an affiliate of the financial institution. This includes, at minimum, senior management roles listed in Appendix 2 of the Policy Document on Responsibility Mapping[2]; and

"user" refers to any person whom a debit card product has been issued to and here on referred to as a cardholder.

6 Related legal instruments and policy documents

6.1 This policy document must be read together with other relevant legal instruments and policy documents that have been issued by the Bank, including any amendments or reissuances thereafter in particular -
(a) Guidelines on Imposition of Fees and Charges on Financial Products and Services issued on 10 May 2012;
(b) Policy Document on Outsourcing issued on 23 October 2019;
(c) Policy Document on Risk-Based Authentication for Online Payment Card Transactions issued on 4 November 2020;
(d) Policy Document on Merchant Acquiring Services issued on 15 September 2021;
(e) Policy Document on Business Continuity Management issued on 19 December 2022;
(f) Policy Document on Fair Treatment of Financial Consumers issued on 27 March 2024;
(g) Specification letter on Requirements on Card-Not-Present for Toll-Related Transactions issued on 17 April 2024;

[1] Issued in 2013, including any amendments or modifications made thereof.
[2] Issued on 29 December 2023, including any amendments reissuances thereafter.

(h) Policy Document on Product Transparency and Disclosure issued on 3 December 2024;
(i) Policy Document on Complaints Handling issued on 28 March 2025;
(j) Policy Document on Management of Customer Information and Permitted Disclosures issued on 31 October 2025; and
(k) Policy Document on Risk Management in Technology issued on 28 November 2025.

7 Policy documents superseded

7.1 This policy document supersedes the following:
(a) Circular on Debit Card Cash Out Facility issued on 29 October 2007;
(b) Circular on Contactless Functionality in Debit Cards and Prepaid Cards issued on 12 August 2016;
(c) Policy Document on Debit Card issued on 2 December 2016; and
(d) Policy Document on Debit Card-i issued on 2 December 2016.

PART B APPROVED SHARIAH CONCEPT

8 Shariah concept

S 8.1 The underlying Shariah concept that is applicable to debit card-i is *ujrah* (fee). Under this concept, *ujrah* shall only be charged to cardholders in consideration of identified services, benefits and privileges that are Shariah compliant. Such services may include payment facilities for goods and services, and cash withdrawal services from a cardholder's account via automated teller machines (ATMs).

S 8.2 Issuer shall put in place appropriate processes, mechanisms and safeguards to ensure that a debit card-i is not used for non-Shariah compliant transactions.

S 8.3 Issuer shall obtain the Bank's approval prior to changing the underlying Shariah concept for its debit card-i structure.

9 Shariah requirements

S 9.1 Issuer of debit card-i shall only impose fee on Shariah compliant services, benefits and privileges provided.

PART C BUSINESS CONDUCT

10 Fees and charges

S 10.1 In determining the type and quantum of fees and charges on debit card products, the issuer shall ensure compliance with the Guidelines on Imposition of Fees and Charges on Financial Products and Services[3].

G 10.2 Upon the issuance of a debit card product, the issuer may impose a fee for the card.

S 10.3 Notwithstanding paragraph 10.2, the issuer shall not charge cardholders an annual fee during the same year the debit card product is issued.

Disclosure and transparency

11 Key disclosure principles and requirements

S 11.1 Issuer shall comply with the policy requirements stipulated in the Policy Document on Product Transparency and Disclosure[4]. Where information is disclosed through digital channels, issuer shall comply with requirements on digital disclosure outlined in paragraph 11 of the said policy document.

S 11.2 Issuer shall provide a product disclosure sheet (PDS) (in the order and sequence of items as specified in the PDS template provided in Appendix I) for cardholders to make product comparisons and informed decisions. The issuer shall comply with the "Notes on PDS requirements" provided in the PDS template.

Pre-contractual stage

S 11.3 Features of debit card products
In addition to paragraph 11.1, issuer shall inform cardholders of the key features of the debit card product, including its function as an ATM card, where relevant.

S 11.4 Fees and other charges
Issuer shall disclose to the cardholders in the PDS all applicable fees and charges in relation to the debit card product, including the amount and frequency of payment.

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

[3] Issued on 10 May 2012, including any amendments and reissuances thereafter.
[4] Issued on 3 December 2024, including any amendments and reissuances thereafter.

At the point entering into a contract

S 11.5 Terms and conditions

(a) Issuer shall make written terms and conditions for usage of the debit card product 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) Issuer shall advise cardholders to read and understand the terms and conditions before signing the agreement and using the debit card product. Issuer shall take reasonable steps to draw cardholders' attention to the terms that have implications on cardholder liability.

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

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

S 11.6 Usage of debit card products outside Malaysia

Issuer shall inform cardholders of the relevant charges, transaction fees and currency conversion fees applicable on the use of the debit card products for purchase transactions and cash withdrawals outside Malaysia.

S 11.7 Cardholders' responsibilities

Issuer shall provide 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 product;

(b) Take reasonable steps to carry out the following obligations:

i. To not disclose the PIN or security credentials (e.g., passcode) to any other person;

ii. To not allow any other person to use the debit card product;

iii. To not disclose the details of the debit card product to a third party except to facilitate payment and purchase authorisation or to provision the debit card product on a mobile wallet;

iv. To not record or write down the PIN or security credentials on the debit card product, or on anything kept in close proximity with the card;

v. To not use a PIN or security credential that is predictable and can be easily associated to the cardholder such as birth date, identity card, passport, driving license or contact number; and
vi. To keep their security device secure at all times.

(c) Notify the issuer as soon as reasonably practicable after having discovered that the debit card product is lost, stolen, an unauthorised transaction has occurred or the PIN and security credentials may have been compromised;
(d) Notify the issuer immediately upon receiving a transaction alert if the transaction was unauthorised;
(e) Notify the issuer immediately of any change in the cardholder's contact number;
(f) Use the debit card product responsibly, including not using the card for unlawful activity; and
(g) Check the account statement periodically and report any discrepancy without undue delay.

During the term of contract

S 11.8 Statement

(a) For accounts without a passbook, issuer 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, issuer shall facilitate the requests without any fee, unless otherwise approved by the Bank.

S 11.9 Closure of account

(a) Issuer shall allow cardholders to close their accounts at any time without being subjected to a cumbersome account closure procedure.
(b) Issuer shall disclose any penalty charge applicable to early closure of the account within a specified time frame.

S 11.10 Change to the terms and conditions

(a) Should there be any change in the terms and conditions, issuer shall provide at least twenty-one (21) calendar days' notice to cardholders before the new terms and conditions take effect.
(b) Any change in fees and charges applicable to the accounts shall be communicated by the issuer to cardholders at least twenty-one (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.

12 Usage of debit card product for unlawful activities

S 12.1 Issuer shall ensure that the terms and conditions include a clause specifying that the debit card product must not to be used for any unlawful activities[5]. Issuer shall immediately terminate the debit card product if cardholders are found to have used the debit card product for any unlawful activity.

13 Disclosure on fraud prevention and cardholder awareness

S 13.1 Issuer shall ensure that cardholders are provided with safety guides to prevent the cardholders from becoming victims of debit card products fraud. These safety guides shall be current, simple to understand and easily accessible by the cardholders across various platforms. At minimum, issuer shall ensure that cardholders are constantly reminded on the following:

(a) To check transaction alerts in a timely manner, as well as account balances or statements on a regular basis and to report to the issuer as soon as any unauthorised transaction, error or discrepancy is detected;

(b) To verify the authenticity of messages sent by the issuer and appropriate action to be taken upon detecting that such message is fraudulent; and

(c) To read the security guide or warnings posted on the issuer's website or mobile application, including the issuer's privacy policy statement, prior to providing confidential information to the issuer or third parties.

S 13.2 Issuer shall ensure periodic reminders are issued to cardholders, at least once in every calendar year after card issuance, on the following:

(a) The responsibilities of cardholders under paragraph 11.7, failing which cardholder may be liable for the fraudulent transaction;

(b) That cardholders would not be liable for unauthorised transactions except in situations outlined under paragraph 16.2; and

(c) Guidance on actions to be taken by cardholders in the event of suspected fraud as per paragraph 17.

S 13.3 Information provided as per paragraph 13.1 and 13.2 shall be made easily accessible and clearly noticeable by cardholders such as by prominently displaying the information on the issuer's website or mobile application as well as via email notification, taking into account the cardholders' preferences and profile.

S 13.4 Issuer shall ensure that customer service representatives are kept up to date on current fraud risks and are well-versed on the end-to-end fraud investigation process such that the issuer is able to advise cardholders effectively upon receiving reports of debit card product fraud cases.

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

14 Disclosure for advertisement

S 14.1 Issuer shall ensure compliance with the requirements on disclosure for advertisements as specified under the Policy Document on Product Transparency and Disclosure[6]. Where information is disclosed through digital channels, issuer shall comply with requirements on digital disclosure outlined in paragraph 11 of the said policy document.

S 14.2 Issuer shall ensure that advertisements and promotional materials on debit card products are clear, fair and not misleading.

S 14.3 Issuer shall establish processes for an independent review of advertisements and promotional materials on debit card products, for instance by the Compliance Unit or Legal Unit, to ensure that they are clear and not misleading.

S 14.4 For print media advertisements, the advertisement shall clearly and conspicuously disclose material information about any debit card 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 14.5 Promotional materials shall provide adequate information on the key terms and conditions of the debit card 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 14.6 Issuer shall state prominently important terms and conditions associated with offers of free gifts, prizes, discounts or vouchers for the promotion of debit cards in print advertisements, or in the marketing materials for new cardholders, or together with the account statements for existing cardholders.

S 14.7 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 cards. Issuer shall not merely indicate in a footnote that "terms and conditions apply".

S 14.8 Advertisements or other promotional materials shall not describe any debit card feature as "free" or at "no cost" if there are conditions attached or other forms of charges will be imposed on cardholders.

[6] Issued on 3 December 2024, including any amendments and reissuances thereafter.

Issuers' other obligations

S 14.9 Issuer shall ensure that sales and customer service representatives (including call centres) are adequately trained and knowledgeable about the key features, benefits and risks of the debit card products.

S 14.10 Issuer 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 product or services being offered.

S 14.11 Issuer 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 14.12 Issuer shall put in place adequate verification procedures to confirm the identity of a debit card product applicant to prevent the use of stolen information (e.g., identity theft) for debit card product applications.

15 Disclosure of cardholder information

S 15.1 Issuer shall ensure compliance with the requirements on disclosure of cardholder information as specified under paragraph 12 of the Policy Document on Product Transparency and Disclosure[7].

Investigation and assessment of fraud cases

16 Liability of unauthorised transaction

S 16.1 Issuer shall not hold cardholders responsible for losses incurred from an unauthorised transaction[8] if the cause of the losses is due to any of the following:

(a) Failure of the issuer to take reasonable steps to inform cardholders of their obligations as stated in paragraph 11.7;
(b) Failure of the issuer to provide adequate means for the cardholders to promptly notify the issuer of any lost, stolen or unauthorised use of the debit card products;
(c) A breakdown or other deficiencies in relevant systems of the issuer;
(d) Weaknesses or vulnerabilities in the system, process and controls adopted by the issuer. This includes failure to take reasonable

[7] Issued on 3 December 2024, including any amendments and reissuances thereafter.

[8] For the avoidance of doubt, issuer shall not solely rely on whether the cardholder has authenticated the transaction in determining whether the transaction has been authorised.

measures to detect and block suspicious transactions[9] in and enhance fraud detection rules upon learning of new fraud techniques;

(e) Transactions that involve the use of a forged, faulty or cancelled debit card products;
(f) Transactions that occur before the cardholder receives the passcode or a similar security credential; or the security device for the debit card products;
(g) Fraudulent or negligent conduct of employees or agents of the issuer, acquirers or merchants;
(h) Transactions that occur after the cardholder has notified the issuer of a lost, stolen or unauthorised use of the debit card products;
(i) Transactions that occur after the cardholder has notified the issuer of a compromised security credential (e.g., PIN); or
(j) Failure of the issuer, debit card products network operator and acquirer to resolve any contradictory evidence on the fraud case during the investigation.

S 16.2 Issuer shall not hold cardholders responsible for losses incurred from an unauthorised transaction, unless the issuer can prove that the cardholder has:

(a) Acted fraudulently;
(b) Refused to cooperate[10] with the issuer in the investigation; or
(c) Failed to carry out the obligations informed by the issuer as stated in paragraph 11.7.

S 16.3 Where issuer or acquirer decides not to authenticate[11] the cardholder using a strong authentication method for card-not-present transactions, the cardholder shall not be held liable for any financial losses arising from such unauthenticated transactions, subject to the cardholder not acting fraudulently.

17 Investigation and assessment of dispute cases

S 17.1 When a cardholder lodges a report on a disputed transaction, the issuer shall acknowledge receipt of the dispute as soon as practicable and inform the cardholder of the information needed for investigation purposes within three (3) working days from the date the report is lodged. The information, at minimum shall include the following:

(a) Cardholder's name;
(b) Affected debit card product number;
(c) Date of the disputed transaction;
(d) Amount of the disputed transaction; and
(e) Reason why the cardholder believes that it is a disputed transaction.

[9] Examples of failure to detect and block suspicious transactions include failure of issuer to block a series of transactions occurring within a short time frame which is not consistent with the normal transaction behaviour of the customer.

[10] This may include expectation to surrender mobile or security device to the authority for forensic investigation.

[11] Under the Policy Document on Risk-based Authentication for Online Transactions issued on 4 November 2020, an issuer and acquirer may decide not to authenticate the cardholder for low-risk online payment card transactions.

S 17.2 Issuer shall prominently disclose on the issuer's website and mobile application the information required for investigation purposes from the cardholder as per paragraph 17.3.

S 17.3 Issuer shall ensure fraud cases are subject to a robust investigation and assessment process that appropriately considers the respective obligations of the issuer, debit card product networks, acquirers, merchants and cardholders.

S 17.4 In conducting the investigation, issuer shall first consider the obligations of the issuer, debit card product networks, acquirers and merchants[12], including the effectiveness of fraud detection and prevention controls in averting an unauthorised transaction.

S 17.5 Where the issuer has determined that the fraud losses arising from the unauthorised transactions shall be borne by the cardholder, the issuer shall ensure that there is adequate evidence to substantiate that the cardholder has breached obligations specified in paragraph 11.7.

S 17.6 In the event that the issuer and acquirer have conclusively established that neither the cardholders nor themselves are at fault, the issuer shall make an assessment to identify other factors that could have contributed to the disputed transaction and undertake mitigating measures, where appropriate.

18 Communication of decision

S 18.1 Issuer shall regularly update the cardholders on the status of the investigation and upon completion of the investigation, communicate their decision in writing to the cardholder as soon as practicable, by clearly providing –

(a) A brief assessment of the case and the outcome; and
(b) The basis on the allocation of any fraud losses passed to cardholders, where applicable.

S 18.2 In addition to paragraph 18.1, issuer shall inform the cardholders of their rights and available channels to request for further information on the investigation. Such information shall also be made clearly visible on the issuer's banking website and mobile banking application.

S 18.3 Issuer shall refer cardholders to the Financial Markets Ombudsman Service (FMOS) as an avenue to seek redress in the following circumstances –

[12] Acquirers shall furnish the necessary information or evidence to issuer to facilitate in the investigation of merchants' compliance with their obligations.

(a) The cardholder is an eligible complainant as defined under the FSA, IFSA or DFIA, as the case may be, and the complaint falls within the FMOS' jurisdiction[13]; and
(b) The complaint does not fall within FMOS' jurisdiction but the issuer, as the case may be, and the cardholder agree for the complaint to be referred to FMOS.

S 18.4 In cases where the complaint does not fall within FMOS' jurisdiction and the issuer, as the case may be, or the cardholder disagrees to refer the complaint to FMOS, the issuer must refer the cardholder to the Bank's Laman Informasi Nasihat dan Khidmat (BNMLINK).

19 Provisional credit

S 19.1 In the event an issuer extends the investigation beyond fourteen (14) working days from the date of receipt of the dispute, the issuer shall –
(a) Immediately offer the cardholder credit on a provisional basis (provisional credit) up to the full amount of the disputed case or RM5,000 per disputed case, whichever is lower. The issuer shall clearly disclose the full terms and conditions of the provisional credit provided to the cardholder and shall not at any time charge any interest, fees or charges on the provisional credit;
(b) Disburse the provisional credit into the cardholder's account upon the cardholder –
  (i) Agreeing to the terms and conditions of the provisional credit covering terms of repayment in the event the cardholder is found to be at fault; and
  (ii) Being informed by the issuer of the impact of non-repayment of the provisional credit in such an event as stated in paragraphs 19.2 to 19.4;
(c) Allow the cardholder the full use of the provisional credit; and
(d) Credit the remaining amount of the disputed case (including any interest or profit where applicable) no later than thirty (30) working days from the date of receipt of the dispute if the investigation has not been concluded by that time.

In implementing this, issuer shall provide adequate warning to cardholders of the actions that can be taken by the issuer against cardholders for any attempt to make false claims on the disputed transactions.

S 19.2 Upon completion of the investigation and where the issuer has concluded that the cardholder shall be held liable for the losses, the issuer retains the right to request the cardholder to repay the provisional credit. In doing so, issuer shall provide the cardholder with a reasonable timeline to repay the outstanding provisional credit.

[13] For this purpose, cases which fall within FMOS' jurisdiction include cases within the monetary limit specified in the relevant regulations pertaining to the financial ombudsman scheme under the FSA, IFSA and DFIA

S 19.3 In the event the cardholder fails to repay the provisional credit within the reasonable timeline set by the issuer, the issuer may report the outstanding provisional credit into the Central Credit Reference Information System (CCRIS) as unreturned provisional credit after six (6) months from the date of the final decision made by the issuer.

S 19.4 Notwithstanding paragraph 19.3, in the event the cardholder decides to pursue the disputed case with the FMOS within six (6) months from the date of the final decision made by the issuer, the issuer shall only report the outstanding provisional credit into CCRIS as unreturned provisional credit upon a final decision by the FMOS.

Other requirements

20 Complaints management

S 20.1 Issuer shall ensure compliance with requirements on complaints management as specified in the Policy Document on Complaints Handling[14].

S 20.2 Issuer shall provide cardholders with information on how complaints may be made and the contact details of the issuer's complaints unit.

[14] Issued on 28 March 2025, including any amendments and reissuances thereafter.

PART D RISK MANAGEMENT

21 Effective Board and senior management oversight

S 21.1 The Board of Directors and senior management of the issuer and acquirer shall establish effective internal oversight arrangements and risk management frameworks to mitigate risks associated with their debit card products 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 products operations;

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

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

(d) Periodic audits by an independent party[15] with reasonable frequency to ascertain and detect weaknesses in business operations and risk management for prompt corrective measures to be taken in a timely manner; and

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

S 21.2 The Board of Directors and senior management of the issuer and acquirer shall ensure that a robust management information system (MIS) is in place to support business decision making and risk management.

22 Comprehensive security policies, procedures and controls

S 22.1 Issuer and acquirer 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 22.2 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[16] to detect vulnerabilities for timely corrective measures to be taken to address security weaknesses.

S 22.3 Procedural and administrative controls on critical processes shall be put in place. Critical processes include, but are not limited to, the following:

[15] Internal or external auditor.

[16] Issuers shall be guided by requirements on vulnerability assessment and penetration testing outlined in the Policy Document on Risk Management in Technology (RMiT).

(a) PIN generation 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) An 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[17] process
   (i) Personalisation process shall be performed in a secure environment.
   (ii) Access to the personalisation machine, reader and data shall be strictly restricted and controlled.
   (iii) Data used for personalisation shall be classified as confidential information and the issuer shall ensure confidentiality and safety of the data that has been sent, stored and processed. This data shall be deleted upon completion of the process.
   (iv) 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.
   (v) Periodic card inventory reconciliation and audit shall be performed on blank cards.
   (vi) Card personalisation centre shall ensure that the following controls are in place -
      - Adequate physical and logical security controls.
      - Segregation of duties and dual controls.
      - Network security controls.

S 22.4 In addition to para 22.3(b), for outsourced card personalisation process, controls shall be in place to ensure that data sent for personalisation to outsourced vendors are secured. The issuer must monitor the outsourced vendor to ensure that the above requirements are met.

S 22.5 Effective segregation of functions on handling of debit card 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; and

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

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

S 22.6 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; and
(d) Handling of returned and undelivered debit card products.

S 22.7 Necessary measures shall be taken to ensure the confidentiality of debit card products 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 such 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 products and create fraudulent transactions.
(e) Confidential data and sensitive information shall only be accessible and managed by authorised parties.

S 22.8 Proper identification and authentication method (e.g., PINs) shall be adopted to avoid unauthorised usage of debit card products. For more robust security, the following shall be adopted at the minimum:
(a) The use of strong PIN shall be adopted;
(b) Maximum PIN tries shall be limited to three (3) on an accumulated basis;
(c) PIN shall not be stored permanently in any format or media;
(d) If the PIN is computer-generated and is not chosen by the cardholder, mandatory PIN change shall be adopted before the first transaction is permitted;
(e) Cardholders shall be allowed to change the PIN at any time; and
(f) Cardholders shall be advised that they shall not use a PIN selected from their birth date, identity card, passport, driving licence or contact numbers to mitigate unauthorised use of their debit card in the event their cards are lost or stolen.

S 22.9 Disposal of debit card products related materials/assets, such as damaged or returned cards, reports and embossing machines shall be performed in a controlled environment.

23 Robust operational reliability and business continuity

S 23.1 Issuer shall ensure compliance with the requirements on essential services as specified in the Policy Document on Business Continuity Management[18].

S 23.2 Acquirers shall ensure compliance with the requirements on business continuity management as specified in the Policy Document on Merchant Acquiring Service[19].

Fraud risk management

24 Fraud monitoring and detection

S 24.1 Issuer and acquirer shall deploy effective and efficient fraud detection[20] and monitoring mechanisms that:

(a) Enable fraud detection and monitoring of transactions.

(b) Enable detection of high-risk transactions and trigger any unusual transactions. To ensure this –

(i) Issuer shall establish internal criteria to determine high risk transactions and merchants to facilitate early detection of fraud.

(ii) Issuer shall put in place procedures to facilitate early detection of unusual transaction patterns or trends that could be indicative of fraud and take necessary actions to block/delay these transactions for further investigation[21].

S 24.2 Issuer shall establish comprehensive fraud case investigation, analysis and reporting procedures by -

(a) Conducting regular analysis to understand fraud trends and modus operandi.

(b) Putting in place adequate risk management processes, systems and controls to mitigate fraud risk. This shall take into account developments in fraud trends and material changes in business strategy which may increase exposure to fraud risk.

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

[18] Issued on 19 December 2022, including any amendments or reissuances thereafter.

[19] Issued on 15 September 2021, including any amendments or reissuances thereafter.

[20] Issuer shall be guided by expectations outlined in the Specifications Letter on Fraud Detection Standards to Combat Electronic Banking Fraud issued on 27 March 2024.

[21] Issuer must investigate suspicious transactions and conduct the necessary verification (such as callbacks or other effective methods) with the cardholder prior allowing the flagged transactions to proceed. To ensure acceptable cardholder experience, issuer should notify the affected cardholder immediately upon the blocking of each suspicious transaction.

S 24.3 Fraud risk management measures shall be reviewed periodically for proactive actions to be taken to address any inadequacies in such measures.

25 Opt-in requirements for card-not-present and overseas transactions

S 25.1 Issuer shall by default block debit card products cardholders from making:

(a) Card-not-present transaction which is not authenticated with strong authentication; and

(b) Any overseas transaction,

unless to facilitate specific transactions as stipulated in paragraph 25.3.

S 25.2 Notwithstanding paragraph 25.1, issuer shall permanently enable the card-not-present transactions for debit card products solely for domestic toll-related transactions[22].

S 25.3 Issuer shall only allow cardholders to make a card-not-present transaction or an overseas transaction using a debit card product, provided that the cardholders have expressly opted-in to conduct such transactions. For cardholders who wish to opt-in card-not-present or overseas transactions, the issuer is required to inform the cardholders of the risks of such transactions.

S 25.4 For the purpose of paragraph 25.2, issuer shall provide cardholders with a convenient mechanism to manage the activation and de-activation of card-not-present and overseas transactions including via enabling a self-service toggle and providing a hotline.

S 25.5 Issuer shall clearly communicate to cardholders that the activation of card not present transactions and overseas transactions is based on the opt-in requirement.

S 25.6 For debit card products which have been enabled for card-not-present or overseas transaction by cardholders, issuer shall block card-not-present transactions or overseas transactions on the debit card products if no such transactions were conducted within the last twelve (12) months. Issuer shall ensure that affected cardholders are notified prior to the blocking.

S 25.7 Issuer who has provided a self-service mechanism to manage activation and de-activation of card-not-present and overseas transactions via a self-service toggle are not subject to requirements outlined in paragraph 25.6.

[22] For avoidance of doubt, this requirement also applies to existing cardholders who have requested to disable the card-not-present transaction on their cards. Automatic enablement shall only apply to domestic toll-related transactions.

26 Fraud mitigation measures for card application, delivery and activation

S 26.1 The following shall be observed at the point of issuer receiving debit card products applications:

(a) Issuer 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 are not misused by persons authorised by the issuer to receive the application(s); and

(b) Issuer or any persons acting on behalf of the issuer to receive debit card products applications are prohibited from photocopying the applicants' other debit card products.

S 26.2 The following controls shall be taken into consideration when processing debit card product 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; and

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

S 26.3 Issuer is prohibited from activating debit card products prior to such action by its cardholders. Issuer shall also put in place stringent activation procedures, which shall include a robust verification process that cannot be easily bypassed by fraudsters and by the issuer's own employees.

27 Requirements when changing cardholder's contact details

S 27.1 To mitigate the risk of account takeover, issuer shall put in place effective measures to verify any request it receives for change of mailing address, contact numbers or security credentials including PIN as well as for the shipment of new or replacement cards.

G 27.2 The following are some practices that issuer may consider 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 a secure electronic mode (e.g., electronic banking) but subject to further verification before updating the contact details; and

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

28 Transaction authentication

S 28.1 Issuer and acquirers shall enable chip and PIN verification for debit card products transactions at point-of-sale (POS) terminals and cash withdrawals at ATMs.

S 28.2 Issuer that authenticates via Consumer Device Cardholder Verification Method (CDCVM) shall comply with the following conditions:

(a) Ensure the implementation of CDCVM is robust[23],

(b) Ensure that each transaction is individually authenticated on the CDCVM device; and

(c) Require debit card products cardholders to set a transaction limit as part of the card provisioning process.

S 28.3 Issuer and acquirers shall authenticate all card-not-present transactions using more secure authentication methods[24] to mitigate the risk of unauthorised use of debit card products.

S 28.4 Issuer that continues to adopt Short Message Service (SMS) One Time Password (OTP) as a form of authentication for card-not-present transactions shall ensure that such transactions do not exceed RM250. Transactions above such threshold must be authenticated using more secure authentication methods.

29 Use of secure device to authenticate card transaction

S 29.1 Where authentication via a secure device is implemented, issuer shall restrict the authentication of debit card products transactions by default to one mobile device or secure device per cardholder (or to designated devices in the case of joint accounts).

30 Contactless transaction

S 30.1 Issuer shall set an appropriate limit for each contactless transaction as well as an appropriate daily cumulative limit for contactless transactions which do not require any cardholder verification. In implementing this requirement, issuer shall undertake the following:

(a) Provide cardholders with a simple and convenient mechanism to set a lower daily cumulative transaction limit for contactless transactions;

(b) Provide cardholders with a simple and convenient mechanism to turn off the contactless functionality in contactless debit card products; and

[23] This includes requirement for issuer to provide the necessary documents pursuant to paragraph 14.5 of Policy Document on Risk Management in Technology (RMiT) for the introduction of new services or any enhancements not listed in the prescribed list and undertake vulnerability assessment and penetration testing and address all the issues prior to implementation of CDCVM.

[24] For the avoidance of doubt, more secure authentication shall align with requirements on control measures for digital services under the Policy Document on Risk Management in Technology (RMiT) and the authentication notification should not include any use of hyperlink.

(c) Raise awareness among cardholders about the mechanism set out in paragraphs (a) and (b) minimally via the issuer's website and PDS.

S 30.2 Issuer shall ensure that verification is conducted once transactions exceed the single transaction limit or the daily cumulative limit for contactless transactions, i.e., via chip and PIN.

S 30.3 Requirements under paragraph 30.1 and 30.2 are not applicable to contactless transactions which are authenticated via the use of an authentication method that combines two (2) or more factors (e.g., PIN), inherent factors (e.g., biometric characteristics) or possession factors (e.g., debit card products, mobile device).

31 Kill switch

S 31.1 Issuer shall provide convenient 24/7 access for customers to temporarily suspend their debit card products in the event of suspected fraud such as by offering a self-service kill switch or freeze function in the issuer's online banking website or mobile application.

32 Cooling off period for higher risk activity

S 32.1 Issuer shall introduce an appropriate cooling-off period for:
(i) Enrolment of a secure device;
(ii) Changes of mobile phone/personal details; and
(iii) Increases in the transaction limit for card-not-present transactions, for cardholders who continue to use SMS OTP as a method for verification.

The Bank reserves the right to assess the reasonableness of the cooling off period, and to specify a longer cooling off period, where necessary to ensure the effectiveness of the countermeasure.

S 32.2 Issuer shall clearly notify the cardholders of the imposition of a cooling off period at the point of its activation through all available communication channels, either in writing or verbally, such as via e-mail, SMS or telephone call.

33 Hotline

S 33.1 Issuer shall provide effective and convenient means for cardholders to notify the issuer of any lost, stolen or unauthorised use of their debit card products. This shall include having a dedicated hotline which is operational at all times.

S 33.2 Issuer shall implement procedures for acknowledging receipt and verification of the notification of a lost, stolen or unauthorised use of the debit card products. This information must be featured prominently on the issuer's website and mobile application.

S 33.3 Issuer shall ensure that its customer service centre is adequately resourced and operating effectively to provide prompt and adequate assistance to cardholders in distress.

G 33.4 Issuer should advise cardholders to use the contact number indicated at the back of their debit card products to ensure consistent communication to cardholders and easy access to debit card-related assistance.

34 Transaction alerts

S 34.1 Issuer shall provide transaction alerts[25] to their cardholders through prominent channels, such as via SMS or in-app notification.

S 34.2 Issuer shall provide transaction alerts in the case of rejected card-not-present transactions, including a brief remark on the cause of rejection.

S 34.3 Issuer shall take into consideration the following criteria, among others, to identify high-risk transactions and trigger transaction alerts:

(a) Transaction type, e.g., transaction at high-risk merchants.
(b) Transaction location, e.g., transaction in high-risk countries.
(c) Transaction amount, e.g., transaction exceeding certain amount.
(d) Transaction velocity, e.g., transaction exceeding certain number per day.
(e) Transactions detected in relation to requirements outlined in paragraph 24.1.

S 34.4 Issuer 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, issuer shall set a default threshold amount including for contactless transactions[26] to trigger a transaction alert. Issuer shall allow cardholders to set their own preferred threshold amounts for the transaction alert. If cardholders do not set the preferred threshold amount, the issuer shall send transaction alerts based on the default threshold amount set by the issuer.
(b) First time use of new card.
(c) All card-not-present (CNP) transactions, except for recurring auto-debit transactions. However, issuer shall take the necessary steps to ensure the auto-debit transaction is a genuine transaction.
(e) High-risk transactions as stipulated under paragraph 34.3.
(f) Activation of self-service toggle to enable CNP and overseas transaction.

S 34.5 By default, transaction alerts must be sent for transactions meeting the specified criteria as stated in paragraphs 34.3 and 34.4, except where the cardholders opt not to receive any transaction alerts. In this regard, issuer must ensure that the cardholders:

[25] For the avoidance of doubt, transaction alerts shall not include any use of hyperlink.
[26] Any upward revision to the agreed threshold for contactless transaction without authentication requires notification to the Bank.

(a) Understand the risks associated with their decision; and
(b) Submit such request in writing.

S 34.6 To ensure the effectiveness of the transaction alerts, issuer shall ensure that the contact numbers of their cardholders are kept up-to-date. As such, issuer must continuously remind their cardholders of the need to provide updated contact numbers on timely basis and enable notification for the issuer's mobile application. Issuer shall verify that the contact details are provided by the cardholders.

S 34.7 To mitigate against potential abuse, issuer shall not provide any contact number or hyperlink as part of the message in a transaction alert.

S 34.8 Issuer shall not transfer the cost of sending transaction alerts to their cardholders.

PART E DEBIT CARD PRODUCT CASH OUT FACILITY

35 Cash out facility

G 35.1 Financial institutions may offer cash out facilities at POS terminals to their debit card products cardholders.

G 35.2 Where an issuer and acquirer offer a cash out facility:

(a) The cash out transaction may be conducted with or without the requirement for cardholders to conduct a purchase transaction using the debit card products; and

(b) The issuer should consider implementing a daily cumulative limit for cash out transactions using the debit card products.

APPENDIX

Appendix I - Product Disclosure Sheet (Debit Card and Debit Card-i)

PRODUCT DISCLOSURE SHEET

Issuer Logo and Name

Date: _____

Dear Customer,
This Product Disclosure Sheet (PDS) provides you with key information on your debit card/*debit card-i*.

Other customers have read this PDS and found it helpful; **you should read it too**.

1 What is [Product Name]?

[*Product Name*] allows you to withdraw cash at an ATM facility and pay for goods and services. You must maintain a deposit account with us, to be linked to your card. All payments and cash withdrawal will be deducted from your account. You must have sufficient funds in your account to complete any payment or cash withdrawal. If your account is closed, your debit card/*debit card-i* will be automatically cancelled.

2 Know Your Obligations

N1

Fees and charges:

- Annual fee: ***RM x***
- ATM withdrawal fee (if any): ***RM x***
- Overseas transaction conversion fee: ***RM x***
- Card replacement fee: ***RM x***
- Sales draft retrieval fee: ***RM x***

Issuers to indicate other relevant fees for this product.

It is your responsibility to:

Read and understand the **key terms** in the contract before you sign it.

Keep your **PIN and security credentials secure** at **all times**. **Do not** disclose your **credentials** to any person.

Contact us immediately, after having discovered the loss or unauthorised use of your card.

3 Know Your Risks

You may be **liable** for unauthorised transactions or cash withdrawal if you have:

- acted fraudulently;
- refused to cooperate with the issuer in investigation; **or**
- failed to carry out obligations informed by the issuer.

Page 1/2

4 Key Terms

a. This debit card/*debit card-i* is blocked from using for overseas transactions and card-not-present (CNP) transactions such as online purchases or telephone orders. You must opt-in before you can use your card for overseas and CNP transactions.

b. When you use your card at a self-service petrol dispenser, a pre-authorisation amount of ***RM x*** may be charged to your deposit account. This amount will be released and the actual transaction amount will be debited to your account within 3 working days from the transaction date.

c. You must notify us immediately:
   - upon receiving transaction alert if the transaction was not authorised by you; and
   - when there is any change in your contact number.

d. You have the option to turn off the contactless function of your card during account opening, card application, or any time thereafter.

e. If you fail to abide by the terms and conditions of your debit card/*debit card-i*, we have the right to terminate your card.

Issuers to indicate other key terms for this product.

If you have any question or require assistance on your debit card/*debit card-i*, you can:

Call us at	Visit us at:	Email us at:	QR
xxx-xxx-xxxx	https://[product webpage].com	xxx@Xmail.com	Scan the QR code above

N2

N3

Customer's Acknowledgment*

Ensure you are filling this section yourself and are aware of what you are placing your signature for.

☐ I acknowledge that [Issuer name] has provided me with a copy of the PDS.

☐ I have read and understood the key information contained in this PDS.

**A customer's acknowledgement of this PDS shall not prejudice his/her rights to seek redress in the event of subsequent dispute over the product terms and conditions.*

Name:
Date:

Notes on PDS requirements

An issuer must refer to the following table when preparing PDS for a debit card/*debit card-i*. The red annotations with an "N" numbering are for the issuer's reference only. They must be removed from the PDS to be provided to financial consumers.

An issuer has the flexibility to use appropriate infographics, illustration or colour to draw the attention of financial consumers to important information in the PDS.

Item	Notes on PDS requirements
N1	An issuer must disclose all applicable fees and charges relating to the use of the debit card/*debit card-i*.
N2	An issuer must indicate the available avenues for financial consumers to contact the Issuer should they have any questions or require assistance. QR code is only an example of the available avenues. If an issuer includes QR code to direct financial consumers to further information about the product, the issuer is reminded to adhere to the disclosure principles under paragraph 9.1 of Policy Document on Product Transparency and Disclosure.
N3	It is optional for an issuer to include this section for financial consumers to acknowledge that they have read and understood the PDS. A financial consumer's acknowledgement of this PDS shall not prejudice his/her rights to seek redress in the event of subsequent dispute over the product terms and conditions disclosed in this PDS.