BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Managing Risks of Electronic Banking, Direct Debit and Risks Associated with Payment Instruments

Circular

Issued on: 24 December 2014

1. INTRODUCTION

Electronic Banking

1.1 As provided in the Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions (FIs) issued on 30 March 2010, the board of directors and senior management of FIs are responsible to address the risks associated with the security, integrity and availability of the FIs' e-banking products and services. In this regard, FIs amongst others, should continuously assess the effectiveness of their risk mitigation measures and take proactive measures on a timely basis in addressing new security threats that may result in financial losses to the FIs and their customers, and would undermine customer confidence and the FIs' reputation.

1.2 The recent cases of malware attacks on internet banking customers' accounts where fraudsters have been able to steal confidential banking information such as the victim's login credentials, password and transaction authentication code is a concern. As new malware virus variants are introduced, anti-virus software are likely to lag behind, thus undermining the effectiveness of using mobile devices for the purpose of second factor authentication of internet banking transactions. Consequently, there is a need for FIs and issuers of designated payment instruments to review the adequacy of their second factor authentication method.

Direct Debit

1.3 The exposure of customers' account details (i.e. bank account details or designated payment instrument account details) may increase the risk of such information being misused to create unauthorised direct debit transactions. With the increasing use of electronic payments, it is important to further strengthen the risk mitigation measures to counter any misuse of customers' account details.

Card-not-present and overseas transactions for designated payment instruments

1.4 With the growth of debit and prepaid cards that allow consumers to conduct face-to-face (card present) transactions both locally and abroad, as well as, non-face-to-face (card-not-present) transactions, there is a need to implement adequate risk management measures and controls, and to educate customers of the safe practices in order to mitigate the risks of unauthorised transactions, in particular for card-not-present and overseas transactions.

Customer Confidence

1.5 Following the recent cases of malware attacks, it is important to enhance the protection of consumers and strengthen consumer confidence by clearly stating the circumstances in which customers can be held liable for unauthorised transactions and facilitating the efficient resolution of disputed transactions. In addition, with the anticipated growth in electronic payment transactions and increase in the usage of payment cards, particularly the debit card, FIs and issuers should take proactive measures to ensure that their risk mitigation mechanisms remain effective to safeguard their customers' account balances.

1.6 The requirements in this Circular are in addition to the consumer protection measures provided in the Guidelines on the Provision of E-Banking Services by Financial Institutions, Guidelines on Complaints Handling and the policy documents on credit card/credit card-i, charge card/charge card-i and debit card/debit card-i.

2. APPLICABILITY

2.1. This Circular is applicable to all FIs and issuers of designated payment instruments.

2.2 Except for paragraphs 5.6 to 5.10, the requirements in this Circular shall apply to transactions performed by individuals, micro and small enterprises.

2.3 The requirements under paragraphs 5.1 to 5.8 are applicable to e-banking transactions, direct debit transactions and card-not-present transactions using designated payment instruments, as the case may be. The requirements under paragraphs 5.9 to 5.10 are applicable to card-not-present and overseas transactions using debit card, debit card-i and prepaid card. The requirements under paragraphs 5.11 to 5.16 are applicable to financial products and services where funds are drawn from customers' savings, current or prepaid account balances.

3. ISSUANCE AND EFFECTIVE DATE

3.1. Unless otherwise stated, the requirements in this Circular come into effect on:

(a) 2 February 2015 with respect to all the requirements except the requirements set out in paragraphs 5.9 and 5.10 below; and

(b) 1 June 2015 with respect to the requirements set out in paragraphs 5.9 and 5.10 below.

4. INTERPRETATION

4.1. For the purpose of this Circular:

"e-banking" means the provision of banking products and services through electronic channels, including via the internet, mobile devices, telephone, automated teller machines (ATM), and any other electronic channel.

"financial institution" or **FI** means any person licensed under the Financial Services Act 2013 (FSA) or the Islamic Financial Services Act

2013 (IFSA) or prescribed under the Development Financial Institutions Act 2002 (DFIA).

"issuer of designated payment instrument" or **"issuer"** means any person who has obtained approval from Bank Negara Malaysia (BNM) under the FSA or the IFSA to issue a designated payment instrument.

"direct debit" means a payment service for debiting a payer's account (i.e. savings account, current account or designated payment instrument account) whereby a payment transaction is initiated by the payee on the basis of consent given by the payer to:

(a) the payee;
(b) the payee's FI or issuer of designated payment instrument; or
(c) the payer's own FI or issuer of designated payment instrument.

"designated payment instrument" means any or all of the following payment instruments prescribed as designated payment instruments under the FSA or designated Islamic payment instruments under the IFSA:

(a) Credit card / credit card-i;
(b) Charge card / charge card-i; or
(c) Debit card / debit card-i; or
(d) Electronic money and for the purpose of this Circular, the term "electronic money" shall mean a "prepaid card" as defined below.

"micro and small enterprises" has the same meaning as defined in the Circular on New Definition of Small and Medium Enterprises (SMEs) issued by BNM.

"pass code" means a password or code that is used to authenticate the identity of a customer and to authorise a transaction. A pass code may consist of numbers, letters, a combination of both, or a phrase. Examples of passcode include:

(a) password;

(b) one-time password (OTP)

(c) personal identification number (PIN); and

(d) code generated by a security device.

"payment instrument" means any instrument, whether tangible or intangible, that enables a person to obtain money, goods or services or to make any payment.

"**prepaid card**" means electronic money stored in a host system or in a card which can be used to conduct card-present transactions both locally and abroad, as well as, card-not-present transactions.

"**security device**" means a token or other device that generates a pass code.

5. SUPERVISORY EXPECTATIONS

E-banking transactions, direct debit transactions and card-not-present transactions made using designated payment instrument

5.1 FIs and issuers must take reasonable steps to ensure that customers are adequately alerted and provided with updated safety tips that are practicable and effective, including but not limited to the obligations set out in paragraphs 5.2(b) and 5.3(b) below, in order to prevent customers from becoming victims of e-banking, direct debit and card-not-present fraud.

5.2 A FI must ensure that a customer shall not be held liable for losses arising from an **e-banking** transaction unless the FI can prove on a balance of probabilities that:

(a) The customer has acted fraudulently; or

(b) The customer has failed to carry out the following obligations as informed by the FI to the customer:

(i) Not deliberately disclosing the access identity (ID) and passcode to any other person, via unsolicited emails or on any

website other than the official website of the FI;

(ii) Taking reasonable steps to keep security device secure at all times; or

(iii) Reporting a breach of the security of a pass code or the loss of a security device to the FI as soon as reasonably practicable, upon the customer becoming aware of the breach or loss respectively.

5.3 A FI or an issuer must ensure that a customer shall not be held liable for losses incurred from a **direct debit** transaction or a **card-not-present** transaction unless the FI or the issuer, as the case may be, can prove on a balance of probabilities that:

(a) The customer has acted fraudulently; or

(b) The customer has failed to carry out the obligation to report any unauthorised transaction to the FI or the issuer as soon as reasonably practicable, upon the customer becoming aware of the unauthorised transaction.

5.4 Provided that a customer has not acted fraudulently, a FI or an issuer must ensure that the customer shall not be held liable for losses incurred from an **e-banking**, **direct debit** or **card-not-present** transaction if the cause of the losses is due to any of the following:

(a) The FI or the issuer concerned has failed to take reasonable steps to provide adequate and conspicuous reminders of the obligations that the customer should undertake as stated in paragraph 5.2(b) or paragraph 5.3(b) above;

(b) The FI or the issuer concerned has failed to provide adequate means for the customer to notify the FI or the issuer of the unauthorised transaction;

(c) A technical breakdown or some other deficiency in the systems or equipment of the FI or the issuer;

(d) Weaknesses or vulnerability in the security features and controls adopted by the FI or the issuer;

(e) Pass code or security device which is forged, faulty, expired or cancelled;

(f) Transactions that occurred before the customer received the pass code or security device;

(g) Transactions that occurred before the customer has notified the FI or the issuer of an unauthorised transaction or that a security device has been misused, lost or stolen, or the security of a passcode has been breached, provided that the notification was made in accordance with paragraphs 5.2(b)(iii) or 5.3(b) above; or

(h) Transactions that occurred after the customer has notified the FI or the issuer of an unauthorised transaction or that a security device has been misused, lost or stolen, or the security of a passcode has been breached.

5.5 For cases of unauthorised **e-banking**, **direct debit** and **card-not-present** transactions where a FI or an issuer has determined that the customer concerned should bear the losses, the FI or the issuer must ensure that:

(a) all evidence relied on by the FI or the issuer to reach the decision is made available and verified by the FI's or the issuer's internal audit function;

(b) the FI's or the issuer's internal audit function review an adequate sample of cases of unauthorised e-banking, direct debit and card-not-present transactions on a regular basis; and

(c) the records of the investigation conducted and the evidence relied on are retained for a period of not less than 7 years and made available for BNM's review, as and when required.

Periodic assessment of risk management measures and controls

5.6 FIs and issuers must conduct periodic reviews to assess the adequacy and robustness of the existing risk management measures and preventive and detective control mechanisms for fraud which are adopted for **e-banking**, **direct debit** and **card-not-present** transactions, including

the suitability of the existing authentication method to counter existing and new fraud threats faced by the FIs and the issuers. The review must:

(a) include an assessment of the likely growth of the different types of fraud threats, including emerging fraud modus operandi, and not be limited to the historical incidences of fraud encountered by the FI and the issuer;

(b) include an assessment of the implications for customers and the extent of the FI's and the issuer's financial and reputational loss in the immediate and medium term; and

(c) take into account relevant developments in and outside Malaysia and relevant research findings.

5.7 The review to be conducted by FIs and issuers under paragraph 5.6 above must be conducted by a competent and independent party (such as the Risk Management Department or the Internal Audit function of the FIs and the issuers, or a qualified security expert), minimally on an annual basis and more frequently when warranted. Where the findings of the review show that the existing risk management measures and preventive and detective control mechanisms for fraud are ineffective or are likely to be ineffective in the medium term, FIs and issuers must take appropriate and timely measures to address such inadequacies. FIs and issuers must report such reviews, measures to be taken to address any inadequacy and the implementation timeline to their respective board of directors for endorsement, and thereafter submit such reviews, measures and implementation timeline to BNM.

5.8 FIs and issuers must submit the first report as specified under paragraph 5.7 above to the Director of the Payment Systems Policy Department, BNM, no later than **1 June 2015**.

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

5.9 Subject to paragraph 5.10 below, FIs and issuers must by default block any cardholder from making any **card-not-present** transaction which is not authenticated via strong authentication method such as dynamic password or any **overseas** transaction using a debit card, a debit card-i or a prepaid card.

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

Customer education

5.11 FIs and issuers must ensure that customers are kept regularly informed on the following:

(a) the need to check all transaction alerts in a timely manner and to check account balances, statements of any bank account or designated payment instrument on a regular basis, to detect any unauthorised transaction, error or discrepancy, and to report to the FI and the issuer as soon as reasonably practicable in the event any unauthorised transaction, error or discrepancy is detected; and

(b) the need to comply with the obligations stipulated in paragraphs 5.2(b) and 5.3(b).

5.12 FIs and issuers must regularly review the effectiveness of their customer education measures, taking into account relevant factors such as the extent to which customers are aware, understand and adopt the safe practices as advised by the FIs and the issuers, changes in the profile of customers, developments in communications technology and points of

interface with consumers, and to improve such measures, where necessary. The findings of the assessments and the measures taken to improve the effectiveness of the customer education measures must be reported to the board of directors of the FIs and the issuers.

Complaints management and crediting of customers' funds for disputed transactions

5.13 FIs and issuers must comply with the mandatory requirements as provided in the Guidelines on Complaints Handling issued on 17 December 2009, which include but are not limited to:

(a) keeping customers adequately informed of the dispute resolution procedures to resolve any disputed transaction, which includes any error, omission or unauthorised transaction; and

(b) complying with the timeframe to investigate a disputed transaction, and updating and communicating a decision to the customer upon completion of an investigation on the disputed transaction.

5.14 The dispute resolution procedures referred to in paragraph 5.13(a) above must include the requirement for a customer to provide a FI or an issuer with the following information, whether orally or in writing, with respect to a disputed transaction:

(a) Customer’s name;

(b) Affected account;

(c) Date of the disputed transaction;

(d) Amount of the disputed transaction; and

(e) Reason why the customer believes that it is a disputed transaction.

5.15 In the event a FI or an issuer extends the time period for the completion of an investigation beyond 14 calendar days from the date a disputed transaction is first reported, whether orally or in writing, by a customer to the FI or the issuer, the FI or the issuer must:

(a) at a minimum, provisionally credit the full amount of the disputed transaction or RM5,000, whichever is lower (including any interest

or profit where applicable), into the customer's account no later than 14 calendar days from the date the customer provides the FI or the issuer with the information set out in paragraph 5.14 above, whether orally or in writing;

(b) credit the remaining amount of the disputed transaction (including any interest or profit where applicable) no later than 30 calendar days from the date of the first crediting where the FI or the issuer has provisionally credited an amount into the customer's account in accordance with paragraph 5.15(a) above which is lesser than the amount of the disputed transaction; and

(c) allow the customer the full use of the provisionally credited funds.

5.16 For the purpose of implementing paragraph 5.15, FIs and issuers must provide adequate warning to their customers of the actions that can be taken by the FIs and the issuers against their customers for any attempt to make false claims on the disputed transactions.

[The remainder of this page is intentionally left blank]