BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Ensuring Fair Treatment for Victims of Unauthorised e-Banking Transactions

Applicable to:

1. Licensed Banks
2. Licensed Islamic Banks
3. Prescribed Development Financial Institutions

Issued on: 28 June 2024 BNM/RH/PD 028-139

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 Bank Negara Malaysia (BNM) recognises the ongoing efforts by the industry in implementing fraud prevention measures and awareness initiatives which have gone a long way in combating financial fraud in Malaysia. Nevertheless, continued incidences in fraud cases involving unauthorised transactions performed without customers' consent and the perceived unfair treatment by customers after falling victim to fraud could undermine public confidence in e-banking services. Given that financial institutions (FIs) play a critical role in ensuring the security, integrity and reliability of e-banking services, it is crucial that enforcement and recovery mechanisms when fraud occurs also continue to be enhanced.

1.2 In this regard, BNM expects the industry to strengthen their practices in fraud case management to ensure victims are treated fairly. This policy document sets out BNM's regulatory requirements that are aimed at ensuring fair treatment of fraud victims arising from unauthorised e-banking transactions through the following:

(a) Greater clarity on the obligations of the FIs and customers with respect to preventing an unauthorised transaction; and

(b) Enhanced transparency and disclosure obligations for the benefit of customers with respect to the investigation process and outcomes.

2 Applicability

2.1 This policy document is applicable to FIs as defined in paragraph 5.2.

3 Legal provisions

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

(a) sections 47(1), 123(1) and 143(2) of the Financial Services Act 2013 (FSA);

(b) sections 57(1), 135(1) and 155(2) of the Islamic Financial Services Act 2013 (IFSA); and

(c) sections 41(1), 42C(1) or 116(1) of the Development Financial Institutions Act 2002 (DFIA).

3.2 The guidance in this policy document is issued 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 on 1 October 2024.

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 advice or recommendations that are encouraged to be adopted;

"BNM" refers to Bank Negara Malaysia;

"CCRIS" refers to Central Credit Reference Information System;

"**customer**" refers to all segments of customers, except for paragraphs 9.7 to 9.10 and 11 that are only applicable to individuals, micro and small enterprises[1];

"e-banking" refers to the provision of banking products and services through electronic channels, including via the internet, mobile devices, telephone, automated teller machines and any other electronic channels;

"**financial institution**" or **"FI"** refers to:

(a) a licensed bank under the FSA;

(b) a licensed Islamic bank under the IFSA;

(c) a prescribed institution under the DFIA; and

"**unauthorised transaction**" refers to a payment transaction that is not consented, initiated or authorised by the customer but excludes transactions where the victim has willingly performed and approved the payment at the point of the transaction (e.g. love scam, investment scam, parcel scam and inaccurate payment transaction). For the avoidance of doubt, FIs shall not solely rely on whether the customer has authenticated the transaction in determining whether the transaction has been authorised.

[1] As per Guideline for New SME Definition issued by SME Corporation Malaysia.

6 Related legal instruments and policy documents

6.1 This policy document must be read together with other relevant legal instruments, policy documents and guidelines issued by the Bank, as amended from time to time, in particular:

(a) Policy Document on Central Credit Reference Information System (CCRIS): Requirements on the Submission, Usage and Protection of Credit Information.

7 Policy documents superseded

7.1 This policy document supersedes the following:

(a) Managing Risks of Electronic Banking, Direct Debit and Risks Associated with Payment Instruments Circular (issued on 24 December 2014); and

(b) Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions (issued on 30 March 2010).

PART B REQUIREMENTS

8 Customer awareness

S 8.1 FIs shall ensure that customers are provided with safety tips that are current and effective across various platforms that are easily accessible by the customer to prevent the customers from becoming victims of e-banking fraud. At minimum, FIs shall ensure that customers are regularly 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 FI as soon as any unauthorised transaction, error or discrepancy is detected;

(b) To verify the authenticity of messages sent by FIs and the appropriate action to be taken upon detecting that such message is fraudulent[2];

(c) To read security tips or warnings posted on the FI's banking website or mobile banking application, including the FI's privacy policy statement, prior to providing confidential information to the FI or third parties; and

(d) To comply with the customer's obligations stipulated in paragraph 9.6 (c) below.

S 8.2 FIs shall ensure that customers are provided with access to a hotline number[3] or similar services to report to the FI if they become victims of e-banking fraud. This information must be clearly accessible on the FI's banking website and mobile banking application.

S 8.3 FIs shall ensure that their customer service personnel are well-aware of current fraud risks and the FI's end-to-end fraud investigation process such that they are able to advise their customers effectively about frauds, scams or identity theft cases.

9 Investigation and assessment of fraud cases

S 9.1 FIs are required to ensure fraud cases are subject to a robust investigation and assessment process that appropriately considers the obligations of both FIs and customers according to paragraphs 8.1, 9.5 and 9.6 (c).

S 9.2 When a customer lodges a report on a disputed transaction, the FI shall acknowledge receipt of the dispute as soon as practicable[4] and inform the customer within 3 working days of the information required for investigation purposes. The minimum information shall include the following:

[2] For example, "don't click, don't tell, don't pay and don't download anything from any unknown or unverified sources".

[3] As required in BNM's letter on Specifications on Measures to Combat Electronic Banking Fraud dated 23 August 2022.

[4] Industry practice is generally within 24 hours.

(a) customer's name;

(b) customer's NRIC or passport number;

(c) affected account number;

(d) date of the disputed transaction;

(e) amount of the disputed transaction; and

(f) reason why the customer believes that it is a disputed transaction.

FIs shall also clearly disclose the minimum information above on the FI's banking website and mobile banking application. FIs may also request additional information from the customer to facilitate the investigation process.

S 9.3 Once a report is lodged, FIs shall immediately advise the customer to lodge a police report and inform the customer in writing of what to expect in connection with the investigation and assessment process of fraud cases. At minimum, this shall include the different stages of the investigation process, expected timelines and a customer's entitlement to provisional credit in the event of prolonged investigations. Relevant guidance to customers in the event of suspected fraud should also be disclosed on the FI's banking website and mobile banking application.

S 9.4 In conducting the investigation, FIs shall first consider their obligations in relation to paragraphs 8.1 and 9.5, including the effectiveness of their fraud detection and prevention controls in averting an unauthorised transaction especially in cases where the payment is not within the normal payment transaction behaviour or pattern of the customer[5].

S 9.5 FIs shall not hold customers responsible for fraud losses incurred from an unauthorised transaction if the cause of the losses is due to any of the following:

(a) the FI has failed to take reasonable steps to adequately remind customers of the obligations that the customer should undertake as stated in paragraph 9.6 (c) below;

(b) the FI has failed to provide adequate means for the customer to promptly notify the FI of an unauthorised transaction;

(c) a breakdown or some other deficiency in relevant systems of the FI;

(d) weaknesses or vulnerabilities in the security features and controls adopted by the FI. This includes the failure to take reasonable measures to prevent account takeovers using stolen banking credentials, detect and block suspicious transactions[6] and enhance fraud detection rules upon learning of new fraud techniques;

[5] For example, multiple transactions that do not correspond with the customer's normal behaviour, either during normal working hours or odd hours.

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

(e) passcodes or similar security credentials or security devices supplied by the FI to the customer which are forged, faulty or cancelled;

(f) transactions that occur before the customer receives the passcode or a similar security credential or the security device;

(g) fraudulent or negligent conduct of employees or agents of the FI;

(h) transactions that occur after the customer has notified the FI of an unauthorised transaction, compromised security device or breached passcode; or

(i) the FI has failed to resolve any contradictory evidence observed during the investigation.

S 9.6 FIs shall also not hold customers responsible for fraud losses incurred from an unauthorised transaction, unless the FI can prove that:

(a) the customer has acted fraudulently[7];

(b) the customer has refused to cooperate[8] with the FI in the investigation; or

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

i. customer shall not disclose their banking credentials such as access identity (ID) and passcode[9] to a third-party;

ii. customer shall take reasonable steps to keep their security device[10] secure at all times[11]; or

iii. customer shall report any security breach of their banking credentials or the loss of a security device to the FI as soon as the customer becomes aware of the breach or loss.

S 9.7 While customers are subject to obligations in paragraph 9.6 (c), a customer shall not be made to fully bear the fraud losses, where the FI has the capacity and failed to act and prevent further unauthorised transactions. In such cases, FIs shall properly consider the element of joint culpability in their investigation.

---

7 FIs shall provide adequate warning to their customers of the actions that can be taken by the FI against their customers for any attempt to make false claims on disputed transactions.

8 Cooperation required from the customer beyond the minimum information as stated in paragraph 8, such as a requirement for customers to surrender their mobile device for forensic investigation must be supported by appropriate justification. Under such scenario, the FI shall ensure to only retain the device for investigation purposes and to return the device to the customer in a timely manner. Where appropriate, the FI may consider to extend a temporary mobile device to the customer during the investigation period to alleviate the customer's burden.

9 "Passcode" means a password or code that is used to authenticate the identity of a customer and to authorise a transaction. Examples include transaction authorization code (TAC), personal identification number (PIN) and a code generated by a security device.

10 "Security device" means a token or other devices that generate a passcode.

11 For example, customer should not click dubious links or download Android Package Kit (APK) files from untrusted sources. Customer shall also perform security updates with the latest anti-virus and anti-malware as advised by their FIs and only download mobile banking apps from a trusted app store.

S 9.8 In cases where joint culpability has been established, having regard to obligations of the FIs and customers as specified in paragraphs 8.1, 9.5 and 9.6 (c), any assignment of losses to the customer by an FI shall be fair and proportionate with due consideration to the facts and circumstances of the fraud incident.

S 9.9 Where the FI has determined that the fraud losses arising from the unauthorised transactions shall be borne by the customers either fully or partially, the FI shall ensure that:

(a) any allocation of losses to the customer must be supported by adequate evidence of the customer's fraud or negligence, particularly to substantiate that the customer has breached conditions specified in paragraph 9.6;

(b) the decision in such cases must be subject to an independent review to verify that the FI's decision is based on an objective assessment. At minimum, the independent review:

i. must be conducted either by an independent party within the business unit or FI's control functions;

ii. must include an assessment on the effectiveness of the FI's fraud detection and prevention control measures;

iii. must determine whether the allocation of fraud losses fairly considers the expected obligations of the FIs; and

iv. must be conducted prior to communicating the FI's decision to the customer;

(c) the records of the investigation and supporting evidence are retained at minimum for 7 years and made available for review, as and when maybe requested by the Bank.

S 9.10 Where the independent review under paragraph 9.9 (b) is conducted by an independent party within the business unit, the FI's control functions shall review adequate samples of cases of unauthorised transactions as part of the FI's periodic review as specified under paragraph 12.1.

G 9.11 In the event that FIs have conclusively established that neither the customer nor the FI itself are at fault, FIs may wish to make an assessment to identify other factors that could have contributed to the disputed transaction and undertake mitigating measures, where appropriate.

10 Communication of decision

S 10.1 FIs shall regularly update the customers on the status of the investigation and upon completion of the investigation, communicate their decision in writing to the customer 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 customers, where applicable.

S 10.2 In addition to paragraph 10.1, FIs shall inform the customers of their rights and available channels to request for further information on the investigation.

S 10.3 For customers that remain aggrieved by the outcome of the investigation and wish to pursue a next course of action, FIs shall proactively engage such customers to manage potential risks from negative publicity and ensure these customers have access to clear information on available complaint channels, including for dispute resolution with the Financial Markets Ombudsman Service (FMOS). Such information shall also be made clearly visible on the FI's banking website and mobile banking application.

11 Provisional credit

S 11.1 In the event the FI extends the investigation beyond 14 working days from the date of receipt of the dispute, the FI shall:

(a) immediately offer the customer 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 FI shall clearly disclose the full terms and conditions of the provisional credit provided to the customer and shall not at any time charge any interest, fees or charges on the provisional credit[12];

(b) disburse the provisional credit into the customer's account upon the customer:

i. agreeing to the terms and conditions of the provisional credit covering terms of repayment in the event customer is found to be at fault and the impact of non-repayment of the provisional credit in such an event as stated in paragraphs 11.2 to 11.4; and

ii. furnishing a copy of the police report on the fraud case;

(c) allow the customer 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 30 working days from the date of receipt of the dispute if the investigation has not been concluded by that time.

S 11.2 Upon completion of the investigation and where the FI has concluded that the customer shall be fully or partially liable for the losses, the FI retains the right to request the customer to repay the provisional credit. In doing so, FIs shall provide the customer with a reasonable timeline to repay the outstanding provisional credit.

[12] For avoidance of doubt, this requirement shall apply throughout the life of the provisional credit including any provisional credit that has not been fully repaid to the FI.

G 11.3 In the event the customer fails to repay the provisional credit within the reasonable timeline allowed by the FI, the FI may report the outstanding provisional credit into the CCRIS as unreturned provisional credit after six (6) months from the date of the final decision made by the FI.

S 11.4 Notwithstanding paragraph 11.3, in the event the customer decides to pursue the disputed case with the FMOS within six months from the date of the final decision made by the FI, the FI shall only report the outstanding provisional credit into CCRIS as unreturned provisional credit upon a final decision by the FMOS.

12 Periodic review

S 12.1 FIs shall periodically review their customer awareness efforts and investigation processes to ensure they remain effective. The review must be conducted by a competent and independent party[13] at regular intervals and reflect the FI's track record, experience and the impact on fraud victims from fraud investigations conducted.

S 12.2 Where the findings reveal that existing measures and practices are ineffective or likely to be ineffective, FIs shall take appropriate and timely measures to address such inadequacies. Such periodic review reports should be escalated to the Board for information and deliberation where appropriate, especially if there are material issues that remain unresolved or require their intervention.

[13] The independent party refers to internal or external audit, risk management or compliance function.