



Amendment No. 1

Effective date: 30 September 2026

NOTICE TO BANKS

NOTICE NO. BU/N-3/2022/74 - AMENDMENT NO. 1

NOTICE ON REPORTING OF FRAUD INCIDENTS

1. INTRODUCTION

- 1.1. This Notice sets out the requirement for banks to report incidents of fraud to the Authority.
- 1.2. This Notice is issued pursuant to section 66 of the Banking Act, Chapter 95 (BA) and applies to all banks in Brunei Darussalam licensed under the aforesaid Act.
- 1.3. This Notice shall take immediate effect.

2. DEFINITIONS

- 2.1. For this Notice-

“authorised communication channel” refers to email, mobile phone, letter or other channels that have been agreed between the Authority and the bank;

“ATM skimming” refers to incidents in which Automated Teller Machines in Brunei Darussalam are compromised through the installation of unauthorised devices designed to capture payment card data and/or a cardholders' Personal Identification Number (PIN) for the purpose of conducting unauthorised transactions;

[Amendment No. 1 dated 30 September 2026]

“Authority” means Brunei Darussalam Central Bank as defined by the Brunei Darussalam Central Bank Order, 2010 [“BDCB Order”];

“Financial Intelligence Unit” means the agency responsible for receiving, requesting, analysing and disseminating information concerning money-laundering, suspected proceeds of crime and terrorist financing under the Criminal Asset Recovery Order [2012];



“**fraud**” can be defined as an act or omission intended to gain dishonest or unlawful advantage for the party committing the fraud or for other related parties; and

“**Key Responsible Persons**” refers to senior persons that are accountable or responsible for the management and oversight of the banks of which they may hold controlled functions in executive positions.

- 2.2. Any expression used in this Notice shall, except where expressly defined in this Notice or where the context requires, have the same meaning as in the BA.

3. FRAUD POLICY

- 3.1. A bank shall establish a **fraud policy** approved by its board of directors (for banks incorporated in Brunei Darussalam) or by its group/regional office or equivalent oversight function for the operations in Brunei Darussalam (for banks registered in Brunei Darussalam) which includes defining the classification of fraud incidents (material or non-material).

4. REPORTING REQUIREMENTS

- 4.1. A bank shall report to the Authority in the form, manner and within such time as specified in paragraph 4.2 below, upon discovery of suspected or confirmed fraud incidents where such incidents¹ are **material to the safety, soundness or reputation of the bank**.

- 4.1A Notwithstanding paragraph 4.1 above, a bank shall report to the Authority all suspected or confirmed fraud incidents involving impersonation of the Authority, government or law enforcement authorities and/or bank staff as well as all incidents of ATM skimming.

[Amendment No. 1 dated 30 September 2026]

- 4.2. For the purpose of paragraphs 4.1 and 4.1A, a bank shall report fraud incidents to the Authority in the following manner via an authorised communication channel²:

[Amendment No. 1 dated 30 September 2026]

- 4.2.1. Notify the Authority upon detection of a suspected fraud incident **no later than 1 working day**;

- 4.2.2. Submit a report using the reporting form in Appendix 1, **no later than 5 working days** or such longer period as the Authority may allow, upon detection of a suspected fraud incident. Any reference to the reporting form shall be construed as reference to the current version of Appendix 1 which is displayed on the Authority’s website at www.bdcdb.gov.bn; and

¹ For fraud incident categorisation, see Schedule 1

² For guidance on authorised communication channel under paragraph 4.2 of the Notice, see Schedule 2



- 4.2.3. Submit a brief summary detailing the necessary actions³ and duration taken to resolve the case **no later than 10 working days** upon resolution of such case.
- 4.3. The reporting form and brief summary as per paragraphs 4.2.2 and 4.2.3 respectively shall be certified by a relevant Key Responsible Person.
- 4.4. Where a fraud incident is suspected or confirmed and a bank has not reported it to the Authority, it shall document the reasons for its decision and store the associated documents and supporting information.
- [Amendment No. 1 dated 30 September 2026]
- 4.5. A bank shall furnish to the Authority such other information relating to the reporting of fraud incidents, as may be requested by the Authority.
- 4.6. For the avoidance of doubt, banks shall continue to comply with the provisions of the Criminal Asset Recovery Order, 2012. In relation to banks, this means that in addition to the requirements of paragraph 4.1 and 4.1A above, a Suspicious Transactions report shall be filed to the Financial Intelligence Unit of the Authority as required after a suspicion has been established⁴.
- [Amendment No. 1 dated 30 September 2026]

5. PROVISIONS REPEALED

- 5.1. The provisions of any other notices, directives and policy documents issued by the Authority prior to this Notice and which are inconsistent with it are hereby repealed.

**MANAGING DIRECTOR
BRUNEI DARUSSALAM CENTRAL BANK**

Date: 18 Rabiulakhir 1448H / 30 September 2026

³ Refer to paragraph 4.5 of the Notice on Market Conduct, as may be revised from time to time

⁴ Please refer to Guidance paper to Financial Institutions for the Obligation to Submit a Suspicious Transaction Report (STR) under Section 15 of Criminal Asset Recovery Order and Section 47 of Anti-Terrorism Order (Guidelines No FIU/G-2/2022/2)



SCHEDULE 1: FRAUD INCIDENT CATEGORISATION

[Amendment No. 1 dated 30 September 2026]

This schedule provides guidance for banks for the categorisation of fraud incidents. This list is non-exhaustive.

Type of event	Definition	Examples
Internal fraud	Acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party.	Unauthorised activity: • Transactions not reported (intentional) • Transaction type unauthorised (with monetary loss) • Mismatching of position (intentional) • Misuse of privilege information • Misuse of system access • Falsifying personal details • Activity with unauthorised counterparty • Activity leading to incorrect pricing • Transaction over-reported • Unauthorised changes to programs or data or transactions Fraud and theft: • Credit fraud/worthless deposits • Theft/extortion/embezzlement/robbery • Misappropriation of assets • Malicious destruction of assets • Forgery • Disclosure of confidential information • Cheque kiting • Smuggling • ATM Skimming • Identity theft or unauthorised customer account takeover • Impersonation of the Authority, government or law enforcement authorities or bank staff • Tax non-compliance/evasion (wilful) • Bribes/kickbacks • Insider trading (not on firm's account) • Accounting irregularities



External fraud	Acts of a type intended to defraud, misappropriate property or circumvent the law, by an external threat or a third party (including service provider under outsourcing arrangements with the bank).	Fraud and theft: • Theft / Robbery • Forgery / Counterfeit (Cover Notes, Policy Certificates, Currency, Cheque, Security Documents / Identification documents) • Fraudulent billing by suppliers • Cheque kiting • Card Related Fraud (online and offline transaction) • Internet Banking fraud • Mobile Banking fraud • E-money / Prepaid card fraud • Fraudulent account opening • Fraudulent application for banking products / facilities • Hacking or data breach damage (leading to fraud incidents specified above) • ATM Skimming • Identity theft or unauthorised customer account takeover • Impersonation of the Authority, government or law enforcement authorities or bank staff
------------------------------	---	---



SCHEDULE 2

[Amendment No. 1 dated 30 September 2026]

Please refer to the table and illustration below for the guidance relating to the Paragraph 4.2 of the Notice:-

Reporting Format	Timeline for submission	Minimum Information to be included	Authorised Communication Channel
Notification to Authority	No later than 1 working day	1. Date and time of the incident was discovered 2. Type of fraud incident 3. Optional: • Possible root cause of the incident • Possible impact of the fraud incident • Possible actions to be taken	Mandatory: • Email [official Banking Supervision's email] To fulfill the requirements under this reporting, banks shall report via email. Other authorised communication channels are supplementary, and thus, will not replace the reporting via email. However, should there be exceptional circumstance such as internet connectivity outage, reporting via other authorised communication channels is considered sufficient.
Submit a reporting form	No later than 5 working days	As set out in Appendix 1 – Reporting form	Mandatory: • Email [official Banking Supervision's email]; or • Letter
Submit a brief resolution summary	No later than 10 working days upon resolution of the incident	1. Duration taken to resolve fraud incident including resolution date 2. Actions taken to resolve the fraud incident	To fulfill the requirements under this reporting, banks shall report via email or letter.

Note: Working days are from Monday to Friday, excluding official public holidays.



Illustration: Fraud reporting mechanism under paragraph of 4.2 of the Notice

