



# BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR | FINANCIAL SUPERVISION SECTOR

## MEMORANDUM NO. M-2024-029

To : **ALL BSP-SUPERVISED FINANCIAL INSTITUTIONS (BSFIs)**

Subject : **Reiterating the Guidelines on Risk Management Systems and Controls to Protect Financial Accounts in relation to Section 6 of Republic Act No. 12010 or the Anti-Financial Account Scamming Act (AFASA)**

Republic Act No. 12010, otherwise known as the "Anti-Financial Account Scamming Act (AFASA)," seeks to curb financial cybercrimes, protect financial consumers' interests, and maintain the integrity of the financial system. This law took effect on 13 August 2024. Section 6 of the AFASA reiterates, clarifies, and further reinforces the duty and responsibility of all *Bangko Sentral ng Pilipinas* (BSP)-Supervised Financial Institutions (BSFIs) to employ adequate risk management systems and controls to protect their clients' financial accounts. Thus:

*Sec. 6. Responsibility to Protect Access to Client's Financial Account.* - Institutions shall ensure that access to their clients' Financial Accounts is protected by adequate risk management systems and controls such as MFA, FMS and other Account Owner enrollment and verification processes: *Provided,* That such risk management systems and controls are proportionate and commensurate to the nature, size, and complexity of their operations.

Institutions that are determined by the BSP to be compliant with the requirements of adequate risk management systems and controls shall not be liable for any loss or damage arising from the offenses under Sections 4 and 5 of this Act.

Without prejudice to other liabilities under existing laws and consistent with BSP rules and regulations, Institutions shall be liable for restitution of funds to the Account Owners for failure to employ adequate risk management systems and controls, or failure to exercise the highest degree of diligence in preventing loss or damage arising from the offenses under Sections 4 and 5. Conviction shall not be a prerequisite to the restitution of funds.

Relative thereto, BSFIs are enjoined to strictly observe the BSP issuances on the adoption of adequate risk management systems and controls, particularly the following:

1. Information technology (IT) and cybersecurity risk management controls laid down under Section 148 of the Manual of Regulations for Banks (MORB), Sections 147-Q/145-S/142-P/126-N/163-T of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI), and their related appendices;
2. Amendments to the regulations on IT risk management under BSP Circular No. 1140, Series of 2022; and
3. Anti-Money Laundering (AML)/Countering Terrorist and Proliferation Financing (CTPF) controls under Sections 911 and 921 of the MORB, Sections 911-Q, 921-Q/601-S/601-N/501-P/101-T of the MORNBFI, and their subsequent amendments.

To reiterate, under the IT Risk Management Standards and Guidelines,<sup>1</sup> BSFIs are required to provide various controls specific to e-services, including application security,

---

<sup>1</sup> Appendix 79 to Section 148 of the MORB and Appendix Q-66 to Sections 147-Q, 145-S, 142-P, 126-N, and 163-T of the MORNBFI on Electronic Banking, Electronic Payment, Electronic Money and Other Electronic Products and Services.

non-repudiation of transactions, authorization controls and access privileges. In addition, BSFIs should ensure adoption of the following key controls to protect financial accounts:

1. ***Fraud Management Systems (FMS)***. BSFIs are required to implement automated and real-time fraud monitoring and detection systems to identify and block suspicious or fraudulent online transactions. The expected sophistication and capabilities of BSFIs' FMS should be commensurate to the risks associated with their digital financial and payment platforms. As fraud and cyber threats evolve, the BSFIs' FMS must be constantly calibrated to be able to process surges in transactions, collectively analyze customer profiles/behavior, and detect new fraud patterns.<sup>2</sup>

BSFIs may employ a combination of rules-based, machine-learning, and other technologies to ensure robustness of their FMS. Below are some examples of fraud rules and mechanisms which may be adopted or integrated by BSFIs in the implementation of their FMS:

- a. **Geolocation blocking** – the FMS may stop transactions outside the usual location or country or trigger enhanced due diligence procedures.
  - b. **Transaction velocity checks/thresholds** – the FMS should detect and/or block transactions with unusual velocity, such as multiple transactions which might be performed by automated bots or malware. Moreover, transactions limits may be assigned to financial accounts such as number of transfers per day, maximum transfers per account, etc.
  - c. **Changes in mobile device and account information controls** – the FMS should be able to detect and monitor changes in mobile device and account information. For example, surges in new mobile device registration of customers within a short timeframe might signal automated account takeover attacks. BSFIs may likewise automatically block transactions after change of device or account information within a certain timeframe (e.g., 24-hour cooling off period).
  - d. **Blocking of transactions from blacklisted merchants/sites** – the FMS may include rules to block transactions from known malicious sites and insecure merchants.
2. ***Infrastructure and security monitoring***. The BSFI should establish an appropriate operating environment that supports and protects systems on e-services. It should proactively monitor systems and infrastructure on an ongoing basis to detect and record any security breaches, suspected intrusions, or weaknesses. The BSFI should ensure that adequate controls are in place to detect and protect against unauthorized access to all critical e-services systems, servers, databases, and applications.<sup>3</sup>

The BSFI should put in place effective monitoring mechanisms to detect in a timely manner suspicious online transactions and unusual activities. A sound monitoring system should include audit features that can assist in the detection of fraud, money laundering, compromised passwords, or other unauthorized activities. In particular, the monitoring mechanism for personal e-services should be able to detect cases similar to the following:<sup>4</sup>

---

<sup>2</sup> BSP Circular No. 1140, Series of 2022.

<sup>3</sup> Section 4.1.7, Appendix 79 to Section 148 of the MORB and Section 4.1.7, Appendix Q-66 to Sections 147-Q, 145-S, 142-P, 126-N, and 163-T of the MORNBF.

<sup>4</sup> *Id.*

- a. False or erroneous application information, large check deposits on new e-services accounts, unusual volume or size of funds transfers, multiple new accounts with similar account information or originating from the same internet address, and unusual account activity initiated from a foreign internet address;
- b. Multiple online transfers are made to the same unregistered third-party account within a short period of time, especially if the amount transferred is close to the maximum amount allowed or the value exceeds a certain amount; and
- c. Change of a customer's correspondence address shortly followed by transactions which may indicate potential fraudulent activities, such as opening of an e-service account online, a request for important documents (e.g., cheque book, new e-banking password, credit card/ATM PIN) to be mailed to that address, increase of fund transfer limits, or a sudden increase of fund transfers made to unregistered third parties.<sup>5</sup>

3. **Multi-Factor Authentication (MFA).** The BSFI should use reliable and appropriate authentication methods to validate and verify the identity and authorization of customers. The use of single factor authentication alone is considered inadequate to address the risks inherent in sensitive communications and/or high-risk transactions. Thus, BSFIs should adopt MFA or use a minimum of two (2) factors in such instances. This requirement shall apply to online transactions where the risk of compromise is heightened. As authentication methods continue to evolve, the BSFI should monitor, evaluate, and adopt sound industry practices to address current and changing risk factors.<sup>6</sup>

4. **Account owner enrollment and verification processes, and ongoing monitoring of customer account and transactions.** BSFIs should adopt sound user enrollment and verification processes in onboarding customers to their digital financial channels and applications.<sup>7</sup> Reliable methods must be used for originating new accounts,<sup>8</sup> identifying the customer,<sup>9</sup> and verifying the true identity of the customer based on official identification documents (IDs)<sup>10</sup> presented against established data sources, including the use of facial recognition technologies.<sup>11</sup>

For instance, BSFIs may adopt sound device enrollment procedures such as enrollment of unique device ID (UDID) bound to the registered user/customer and mobile security controls which prevent the use of rooted/jailbroken mobile devices and emulators. These procedures should be complemented by appropriate AML/CTPF customer due diligence policies and controls, particularly in onboarding and updating customer information.

In addition, BSFIs must adopt an AML/CFT monitoring system proportionate to their respective risk profile and business complexity, and strengthen risk and

<sup>5</sup> *Id.*

<sup>6</sup> Section 4.1.2 of Appendix 79 to Section 148 of the MORB and Section 4.1.2 of Appendix Q-66 to Sections 147-Q, 145-S, 142-P, 126-N, and 163-T of the MORNBFI.

<sup>7</sup> See Section 4.1.1 in relation to Section 4.1.2 of Appendix 79 to Section 148 of the MORB and Section 4.1.1 in relation to Section 4.1.2 of Appendix Q-66 to Sections 147-Q, 145-S, 142-P, 126-N, and 163-T of the MORNBFI.

<sup>8</sup> *Id.*

<sup>9</sup> See "Customer identification," Section 921 of the MORB and Sections 921-Q, 601-S, 601-N, and 501-P of the MORNBFI.

<sup>10</sup> *Id.*

<sup>11</sup> See "Face-to-Face contact," Section 921 of the MORB and Sections 921-Q, 601-S, 601-N, and 501-P of the MORNBFI.

materiality based on ongoing monitoring of customers' accounts and transactions, including periodic sanctions screening.<sup>12</sup>

Lastly, BSFIs should cooperate with the BSP and law enforcement agencies for the prosecution of cyber-criminals (including money mules) to the extent permitted by relevant laws and regulations.<sup>13</sup>

5. **Audit trail.** The BSFI should ensure that comprehensive logs are maintained to record all critical e-services transactions to help establish a clear audit trail and promote employee and user accountability.<sup>14</sup>


The various layers of the transaction execution that must have an audit trail may include the application, server, and network layer, among others. The comprehensive logs also facilitate the conduct of detailed investigation and attribution of unauthorized transactions and/or access to accounts.

6. **Cybersecurity tests and evaluations.** BSFIs offering digital/ electronic financial services are required to undergo an annual Vulnerability Assessment and Penetration Testing (VAPT) performed by an independent external party.<sup>15</sup> BSFIs should also employ effective testing methodologies and practices to validate the effectiveness of its information and cybersecurity program.<sup>16</sup>

It should be emphasized that under Section 6 of the AFASA, BSFIs which are determined by the BSP to be compliant with the requirements of adequate risk management systems and controls shall not be liable for any loss or damage arising from the offenses under Sections 4 and 5 of the AFASA. However, BSFIs shall be liable for the restitution of funds to Account Owners for the failure to employ adequate risk management systems and controls or the failure to exercise the highest degree of diligence in preventing loss or damage arising from the said offenses.

Subject to the promulgation of the implementing rules and regulations of the AFASA, all BSFIs are expected to ensure compliance with the guidelines on risk management systems and controls to protect financial accounts under existing BSP regulations.

For guidance and implementation.

 Digitally signed by  
Chuchi G. Fonacier  
Date: 2024.09.19  
13:59:40 +08'00'  
**CHUCHI G. FONACIER**  
Deputy Governor

19 September 2024

<sup>12</sup> See "On-going monitoring of customers, accounts, and transactions," Section 921 of the MORB and Sections 921-Q, 601-S, 601-N, 501-P, and 101-T of the MORNBFi in relation to Section 911 of the MORB and Section 911-Q of the MORNBFi.

<sup>13</sup> See Section 4.2 of Appendix 75 to Section 148 of the MORB and Sections 147-Q, 145-S, 142-P, and 126-N of the MORNBFi.

<sup>14</sup> Section 4.1.8 of Appendix 79 to Section 148 of the MORB and Appendix Q-66 to Sections 147-Q, 145-S, 142-P, 126-N, and 163-T of the MORNBFi.

<sup>15</sup> Section 3.7.2(d) of Appendix 75 to Section 148 of the MORB. See Section 4.1 of Appendix Q-62 to Sections 147-Q, 145-S, 142-P, 126-N, and 163-T of the MORNBFi.

<sup>16</sup> See Section 3.7.2 of Appendix 75 to Section 148 of the MORB. See Section 4.1 of Appendix Q-62 to Sections 147-Q, 145-S, 142-P, 126-N, and 163-T of the MORNBFi.