BANGKO SENTRAL NG PILIPINAS

MEMORANDUM NO. M-2022-016

OFFICE OF THE DEPUTY GOVERNOR
FINANCIAL SUPERVISION SECTOR

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

Subject : **Application Programming Interface (API) Security Control Recommendations**

The use of application programming interfaces (API) by BSFIs, online merchants, payment gateways and technology service providers is fast becoming the new norm with the accelerated digitalization in the financial industry. APIs refer to a set of rules and specifications for software programs to communicate with each other, forming an interface between different programs to facilitate interaction. While this has traditionally been utilized by BSFIs internally for the ease of connecting systems and applications, APIs are now exposed to a wider range of interconnected external parties in the digital ecosystem.

These developments introduce new risk vectors for BSFIs that must be addressed through adequate IT and cybersecurity risk management practices. Provisions related to API security standards have been laid down in BSP Circular No. 1122 / Section 154 of the Manual of Regulations (MORB) and Sections 152-Q/149-S/146-P/130-N/129-T/123-CC of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI). Likewise, control provisions in Appendix 75 and 79 of Section 148 of the MORB and Appendix Q-62 and Q-66 of Sections 147-Q/145-S/142-P/126-N of the MORNBFI on Information Security and Electronic Banking, Electronic Payment, Electronic Money and Other Electronic Products and Services remain applicable.

To aid in strengthening controls on API and interconnections, BSFIs are strongly advised to implement the following good practices for API management:

1. Ensure strong authentication and authorization mechanisms through in-depth evaluation of API architecture and security standards.
2. Encrypt sensitive API payload data using industry-accepted encryption standards and versions.
3. Ensure that only necessary data/information are contained in API responses.
4. Perform validation, filtering, and sanitization of all client-provided data and other data originating from integrated and partner systems.
5. Ensure that system and audit logs capture failed attempts, denied access, input validation failures, or any failures in security policy checks.
6. Regularly update API inventory, purpose, and documentation to appropriately manage deprecated API versions and unintentional endpoint exposure.
7. Conduct regular assessments, hardening, and patching of all API servers.
8. Conduct regular security tests using API and business logic exploits such as but not limited to SQL injection, replay attacks, and logic bypass.
9. Enforce thresholds and rate-limiting API calls to prevent distributed denial-of-service (DDoS) attacks.

Likewise, BSFIs should consider the following controls and processes supporting the operation, connectivity, and endpoint security of APIs:

1. IP Address filtering for third-party partner integrations.
2. Compliance audits with BSFI APIs security standards.
3. Implementation of a Web Application Firewall (WAF) in front of API resources by validating and monitoring API traffic to protect core applications.
4. Strengthening endpoint protection, particulary on mobile applications connecting through APIs, to prevent unauthorized API connections and static/dynamic code analysis. This can be achieved through the implementation of the following for mobile applications:
    a. Source code obfuscation;
    b. Restriction on the installation on unsecure mobile devices/instance (e.g. obsolete operating systems, rooted/jailbroken, emulators);
    c. Periodic changes on the mobile application's unique identifiers such as public key, globally unique identifier (GUID), and universally unique identifier (UUID); and
    d. Ensuring that potential reconnaissance/footprinting of previous mobile application versions are addressed upon implementation of additional security controls.
5. Clearly define and delineate roles and responsibilities on information security and cybersecurity for API interconnectivity between BSFIs and partners.

The controls specified in this memorandum are not exhaustive. BSFIs may likewise adopt any other generally accepted good practices for API applicable to the use cases that may not be captured in this memorandum.

BSFIs are expected to promptly report to the BSP any breaches or cyber incidents/crimes involving APIs pursuant to the event-driven report and notification (EDRN) and report on crimes and losses (RCL) requirements provided under Section

148 and 173 of the MORB and Sections 147-Q/145-S/142-P/126-N of the MORNBFI as amended by Circular No. 1104 dated 27 November 2020. As necessary, BSFIs may need to seek assistance and cooperate with appropriate law enforcement authorities for prompt resolution of cybercrime cases, especially if cases involve public safety and security, pursuant to the Cybercrime Prevention Act of 2012 and other relevant laws and regulations.

For information and guidance.

Digitally signed by Chuchi G. Fonacier
Date: 2022.03.22
16:39:28 +08'00'

CHUCHI G. FONACIER
Deputy Governor

22 March 2022