



BANGKO SENTRAL NG PILIPINAS

Cover Note

Republic Act No. 12010, or the Anti-Financial Account Scamming Act (AFASA), establishes a sector-wide framework to combat financial account-related scams and emerging cyber fraud schemes. It aims to strengthen consumer protection, enhance accountability across the financial ecosystem, and preserve public confidence in the digital financial system.

To implement Section 6 of AFASA, the BSP issued Circular No. 1213 requiring BSFIs engaged in complex electronic services and high-value online transactions to adopt robust fraud management systems and strong customer authentication mechanisms. In line with this, server-side biometric authentication is recognized as an acceptable control for high-risk transactions and critical account changes, subject to appropriate safeguards. The BSP will consider the adoption of such controls in assessing risk management adequacy and potential liability under AFASA.

BSFIs are also expected to transition away from interceptable authentication methods, such as SMS- or email-based OTPs, for financial transactions and other high-risk activities. Institutions remain responsible for ensuring that their authentication frameworks are commensurate with their risk profile and aligned with existing security standards to effectively mitigate digital financial fraud.

BSFIs remain responsible for ensuring that their authentication frameworks are commensurate with their risk profile and are not precluded from implementing stronger or equivalent authentication mechanisms and complying with the security standard under existing regulations to protect customers against scams and digital financial fraud.



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR | FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. _____

To : **ALL BSP SUPERVISED FINANCIAL INSTITUTIONS (BSFIS)**

Subject : **Adoption of Server-Side Biometric Authentication and Other Key Controls for High-Risk Transactions and Critical Account Changes in Financial Applications**

Republic Act No. 12010, otherwise known as the Anti-Financial Account Scamming Act (AFASA), establishes a sector-wide approach to combat financial account-related scams and emerging cyber fraud schemes. The Act seeks to safeguard financial consumers, strengthen accountability across the financial ecosystem, and preserve public confidence in the digital financial system.

To implement Section 6 of AFASA¹, the Bangko Sentral ng Pilipinas (BSP) issued BSP Circular No. 1213 which requires BSFIs engaged in complex electronic products and services and handling high aggregate values of online transactions² to adopt a robust FMS capable of rapidly detecting, preventing, and blocking disputed, suspicious, or other fraudulent transactions, including new and evolving fraud schemes. Likewise, It prescribes the implementation of strong customer authentication mechanisms, **including biometrics authentication**, to identify users and to help ensure the authenticity and integrity of customer-initiated transactions.

Consistent with Circular No. 1213, **Server-Side Biometric Authentication** is considered a strong and acceptable authentication mechanism for high-risk transactions and critical account changes in electronic financial applications, provided that the risks associated with its implementation are adequately addressed and sound practices or minimum control requirements are adopted. The adoption of server-side biometrics authentication and other key controls will inform the evaluation of whether a BSFI has maintained adequate risk management systems and control measures, and will be taken into account in determining the potential liability for loss or damage arising from offenses under Sections 4 and 5 of the AFASA. Additional guidelines on server-sider biometric authentication are in Annex A.

Moreover, in line with Circular No. 1213, BSFIs are expected to transition away from the use of interceptable authentication mechanism, such as One-Time Pins (OTPs) via SMS and email, as an authentication mechanism for financial transactions or other high-risk activities, given the elevated risks of SIM swap fraud, phishing, and related attacks. OTPs may, however, be used for verifying the existence or ownership of a registered mobile number.

¹ Section 6 of AFASA requires institutions to implement adequate risk management systems and controls, such as multi-factor authentication, fraud management system (FMS), and other enrollment and verification processes, that are proportionate and commensurate to the nature, size, and complexity of their operations. It further provides that 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 the AFASA. Conversely, 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.

² Complex electronic products and services refer to advanced electronic payment and financial services (EPFS) as defined under Sections 701/701-Q/401-S/114-P/401-N/404-T of the Manual of Regulations for Banks/Manual of Regulations for Non-Bank Financial Institutions and high aggregate values of online transactions refer to average monthly network value of transactions of at least Php 75 million for the last six (6) months.

Finally, BSFIs remain responsible for ensuring that their authentication frameworks are commensurate with their risk profile and are not precluded from implementing stronger or equivalent authentication mechanisms and complying with the security standard under existing regulations to protect customers against scams and digital financial fraud.

For information, guidance and implementation.

LYN I. JAVIER
Deputy Governor

__ February 2026

Att: a/s

DRAFT

Server-Side Biometric Authentication

Server-side biometric authentication is an authentication mechanism whereby a customer's biometric credential is validated and verified within the secure backend system of a BSP Supervised Financial Institution (BSFI) or its authorized third-party provider, using centrally-stored reference templates. This enables the BSFI's system to authenticate the customer's identity against the records it maintains, regardless of changes on the device used, thereby reducing the risk of account takeover, device compromise, spoofing, and unauthorized credential changes, among other threats.

While server-side biometric authentication enhances user verification, it also introduces heightened security, operational, and privacy risks. As such, BSFIs should address the following concerns to ensure effective implementation of this control:

1. The centralized storage and validation of biometric templates³ and data may create a high-value target for threat actors. A compromise of the biometric database, authentication engine, or associated cryptographic keys could result in large-scale unauthorized access, systemic account takeover, and irreversible exposure of sensitive identity data;
2. Improper collection, storage, or processing of biometric data and inadequate consent mechanisms may lead to regulatory non-compliance, legal liability, and reputational damage. The use of biometric data should adhere to principles of transparency, necessity, and proportionality while ensuring that biometric data is not used, disclosed, or repurposed beyond the specific purpose for which it was collected;
3. Biometric authentication mechanisms may be vulnerable to spoofing, replay attacks, synthetic identity manipulation, or deepfake technologies in the absence of robust liveness detection and anti-spoofing controls;
4. Weak identity verification during biometric enrollment or re-enrollment may enable fraudulent credential registration and increase account takeover risk;
5. Outsourcing biometric authentication services to third-party providers may introduce supply chain and concentration risks;
6. Over-reliance on biometrics without layered security controls may weaken overall fraud detection and prevention; and
7. False acceptance, false rejection, or algorithmic bias may result in unauthorized access, customer disruption, or reputational damage.

Minimum Control Requirements

To ensure that server-side biometric authentication is implemented in a secure, reliable, and risk-based manner, BSFIs are advised adopt the following minimum control requirements:

1. Collection, Storage, and Processing of Biometric Data
 - a. Store biometric data in the form of encrypted biometric templates and avoid retention of raw biometric images;
 - b. Encrypt both data at rest and in transit;

³ A biometric template is a mathematical representation of features or characteristics from the source data, whether a fingerprint scan, facial image, or voice recording.

- c. Adopt architectural or operational approaches to reduce reliance on centralized biometric storage and mitigate risks arising from single points of compromise;
 - d. Limit biometric data access to authorized personnel and enforce logging, monitoring, and periodic review to promote accountability and oversight.
 - e. Establish clear processes for the enrollment, retention, and secure disposal of biometric data, including timely de-identification or secure destruction of biometric templates that are no longer required or upon revocation of biometric enrollment; and
 - f. Design biometric authentication solutions to support inclusivity and accessibility, taking into account vulnerable users⁴ and ensuring compatibility across devices and platforms without materially weakening security controls.
2. Multi-Layered Security and Step-Up Authentication Controls
- a. Restrict high-risk transactions to recognized or appropriately bound devices and revalidate sessions for sensitive actions, particularly following device changes or credential resets;
 - b. Complement automated biometric and risk-scoring systems with human review for flagged or anomalous events to ensure effective oversight and audit. Treat biometric resets and re-enrollment as high-risk activities subject to enhanced verification and monitoring;
 - c. Implement liveness and deepfake detection mechanisms to distinguish genuine users from physical or digital spoofs;
 - d. Adopt multimodal checks⁵ to detect deviations from expected activity and increase the difficulty of successful fraud through simultaneous spoofing of multiple factors;
 - e. Harden authentication Application Programming Interface (API), apply rate limiting and anti-automation controls, and conduct regular penetration testing and code reviews; and
 - f. Implement fallback or alternative secure authentication mechanisms that maintain equivalent assurance levels in cases where server-side biometric authentication fails.
3. Governance, Data Protection, and Third-Party Oversight
- a. Implement governance frameworks to monitor the use of biometric data and ensure compliance with internal policies and applicable data protection laws and regulations;
 - b. Provide clear and accessible notices to users outlining the purpose of biometric data collection, the implications of refusal to provide biometric data, and any potential disclosures to third parties. Biometric data should only be collected for clearly defined, legitimate purposes, and must not be repurposed for unrelated activities without the user's explicit consent;
 - c. Enforce rigorous due diligence and continuous security monitoring when engaging third parties or availing "biometrics-as-a-service" for server-side biometrics authentication. Vendor or service provider contracts must incorporate explicit data protection clauses and mandate regular independent audits to verify compliance;
 - d. Organizations should perform enhanced third-party risk assessments covering security architecture, data protection, resilience, and breach response capabilities;
 - e. Monitor false acceptance rate (FAR), false rejection rate (FRR), and demographic performance, tune thresholds based on transaction risk, and regularly review for algorithmic bias; and

⁴ This includes consideration for users with specific needs, such as elderly individuals with worn or damaged fingerprint characteristics, persons with disabilities who may lack suitable biometric templates, or marginalized populations without access to high-end devices required for certain authentication methods.

⁵ Multimodal checks refers to the combined use of independent verification factors, which may include physiological biometrics (e.g., facial characteristics, fingerprint, etc.) and behavioral or contextual indicators (e.g., device attributes, geolocation, or usage patterns) to increase assurance and reduce the risk of successful fraud through simultaneous compromise of multiple controls.

- f. Continuously test liveness controls against new spoofing techniques and adjust thresholds to balance security (FAR) and usability (FRR).

These controls are intended to safeguard biometric data, mitigate fraud and account takeover risks, preserve customer trust, and ensure alignment with applicable authentication, cybersecurity, and data protection standards. These requirements establish the BSP's baseline expectations. BSFIs, however, should implement additional controls, as warranted, to effectively address the risks and concerns identified above, commensurate with the complexity and risk profile of their digital financial services.

DRAFT