BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

MEMORANDUM NO. M-2026-017

To : **All Bangko Sentral ng Pilipinas-Supervised Institutions**

Subject : **Reiterating Guidelines on Ensuring Integrity of Payment Activities**

Under Republic Act (R.A.) No. 11127 or the National Payment Systems Act (NPSA), the Bangko Sentral ng Pilipinas (BSP) has the authority to safeguard the integrity of the Philippine financial system and promote the efficiency, safety, security, and reliability of the National Payment System. In parallel, R.A. No. 9160 or the Anti-Money Laundering Act (AMLA), as amended, enjoins the State to protect and preserve the integrity and confidentiality of bank accounts and to prevent the Philippines from being used as a conduit for money laundering and other unlawful activities.

Consistent therewith, BSP-Supervised Institutions (BSIs) are enjoined to strictly ensure that their anti-money laundering and countering terrorism and proliferation financing (AML/CTPF) controls, including account onboarding controls and ongoing account monitoring, remain effective and commensurate with risk across all payment activities.[1]

In this regard, the BSP reiterates the strict compliance of BSIs with the following regulations to adequately identify, measure, monitor, and control Money Laundering (ML)/Terrorist Financing (TF)/Proliferation Financing (PF) risks arising from payment activities:

1. Applicable AML/CTPF requirements under Part Nine of the Manual of Regulations for Banks (MORB) and relevant AML/CTPF provisions of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI)[2]; and
2. Expectations on merchant due diligence, including merchant identification, risk assessment, and monitoring, under Subsection 503.7 of the Manual of Regulations for Payment Systems (MORPS).

Based on the foregoing regulations, BSIs are reminded that integrity controls for payment activities should be underpinned by sound account opening, onboarding, and ongoing account monitoring practices. These ensure that customer and account relationships remain consistent with their stated purpose and to enable timely prevention, detection, and response to potential misuse of accounts as conduits for ML/PF/PF and related predicate offenses or other unlawful activity.

Where the payment activity involves merchant payment acceptance, BSIs are reminded that the following guidelines shall also apply:

1. Consistent with the above regulations, BSIs are expected to retain primary responsibility for AML/CTPF compliance for merchant payment activities, whether conducted as the originating financial institution (OFI) or the receiving financial institution (RFI), through payment aggregators or similar intermediaries.[3] The participation of these entities in the payment chain does not transfer, diminish, or

[1] "Payment activities" include, among others, electronic fund transfers and other payment services/use cases (e.g., person-to-person, person-to-merchant, person-to-biller, and other retail payment use cases), whether initiated through branch, online, mobile, QR-enabled, or other channels.

[2] Part IX of the Q-Regulations, Part VI of the S-Regulations, Part V of the P-Regulations, and Part VI of the N-Regulations

[3] "Payment aggregator" refers to an entity that facilitates the acceptance and processing of payment transactions for multiple merchants by enabling access to payment services, settlement, or payment rails, including situations where the aggregator onboards, manages, or transacts on behalf of merchants, whether directly or through sub-merchant arrangements.

substitute the AML/CTPF obligations of the BSI providing accounts, access to payment rails, or settlement services.

a. Payment aggregators or similar entities bear independent and commensurate AML/CTPF responsibilities arising from its role in onboarding, monitoring, and controlling sub-merchant access to payment services. These responsibilities, among others, include merchant due diligence, risk-based onboarding and monitoring, implementation of appropriate risk mitigation measures, and suspicious transaction reporting, in accordance with the above regulations.
b. While the payment aggregator or similar entity remains accountable for managing AML/CTPF risks within its functions, BSIs retain primary responsibility for AML/CTPF risks associated with settlement accounts. In this regard, BSIs remain responsible for ensuring that appropriate risk-based arrangements are in place to maintain adequate visibility over the underlying merchants and related payment activities. This responsibility shall, among others, include the following:
    - Ensuring sufficient access to sub-merchant information, transaction-level data, and merchant risk profiles;
    - Applying risk-based criteria for sub-merchant onboarding and monitoring; and
    - Conducting periodic reviews with clear triggers for restricting or terminating relationships involving high-risk or non-compliant sub-merchants.

2. BSIs are expected to ensure the appropriate opening and use of accounts consistent with the MORPS concept of a "merchant account," i.e., a transaction account where funds from merchant payment acceptance activities are received by the merchant, and to align settlement/receipt arrangements accordingly. For this purpose, BSIs are expected to maintain clear and effective differentiation between merchant accounts and personal accounts, consistent with the nature, purpose, and risk characteristics of the underlying payment activity.
3. BSIs shall ensure that ongoing merchant monitoring (including periodic review of merchant account profiles, merchant information, and merchant account usage against expected activity) remains effective and risk-based.
4. BSIs shall ensure that appropriate, risk-based measures are implemented to prevent and detect mule merchants, including the unauthorized use or misuse of QR codes by persons or entities other than the duly registered merchant.

The BSP likewise reiterates the relevant guidelines under Subsection 1201.2 of the MORPS to give utmost priority to the safety of both payers and the payees using QR-enabled payment and financial services and ensure that the threats and vulnerabilities arising from QR-enabled payment and financial services are identified, measured, monitored, and controlled accordingly. The BSP further reminds all BSIs participating in QR-enabled payment services under the national QR Code Standard (i.e., QR Ph) to adopt commensurate end user (i.e., customer or merchant) due diligence, transaction monitoring, and other risk control measures consistent with the above regulations and guidelines.

For strict compliance.

Electronically signed by
Bernadette R. Puyat
08 May 2026

BERNADETTE T. ROMULO-PUYAT
Officer-in-Charge

08 May 2026