Legal Watch

BSP MEMORANDUM NO. M-2026-017

Photo Credit:
Jire Carreon / Rappler

Agency Name

Bangko Sentral ng Pilipinas (BSP)

Issuance Title

Reiterating Guidelines on Ensuring Integrity of Payment Activities

Issuance Date

8 May 2026

Link

https://www.bsp.gov.ph/Regulations/Issuances/2026/M-2026-017.pdf

SUMMARY

The BSP-Supervised Institutions (BSIs) are expected to prevent the Philippines from being used as a conduit for money laundering and other unlawful activities. Accordingly, BSIs are enjoined to strictly ensure that their Anti-Money Laundering/Countering Terrorism and Proliferation Financing (AML/CTPF) remain effective and commensurate with risk across all payment activities.

In relation thereto, the BSIs shall strictly comply with the applicable regulations, specifically:

1. Requirements under the Manual Regulations for Banks (MORB) and relevant AML/CTPF provisions of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI)
2. Expectations on merchant due diligence, including merchant identification, risk assessment, and monitoring of the Manual of Regulations for Payments Systems (MORPS)

BSIs are reminded that integrity controls for payment activities should be underpinned by sound account opening, onboarding, and ongoing account monitoring practices.

Additionally, if the payment activity involves merchant payment acceptance, BSIs shall observe the following additional guidelines:

1. BSIs are expected to retain primary responsibility for AML/CTPF compliance for merchant payment activities through payment aggregators or similar intermediaries, including*: (a) Merchant due diligence, risk-based onboarding and monitoring, implementation of appropriate risk mitigation measures, and suspicious transaction reporting; and (b)Ascertaining that appropriate risk-based arrangements are in place to maintain adequate visibility over the underlying merchants and related payment activities.

* Payment aggregator is an entity facilitating the acceptance and processing of payment transactions for multiple merchants by enabling access to payment services, settlement, or payment rails, including situations where aggregator onboards, manages, or transacts on behalf of merchants, whether directly or through sub-merchant arrangements.

Legal Watch

BSP MEMORANDUM NO. M-2026-017

Photo Credit:
Jire Carreon / Rappler

Agency Name

Bangko Sentral ng Pilipinas (BSP)

Issuance Title

Reiterating Guidelines on Ensuring Integrity of Payment Activities

Issuance Date

8 May 2026

Link

https://www.bsp.gov.ph/Regulations/Issuances/2026/M-2026-017.pdf

SUMMARY

2. BSIs are expected to ensure the appropriate opening and use of accounts consistent with the MORPS concept of a “merchant account” by maintaining a 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 and 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.

Lastly, the BSP requires BSIs participating in QR-enabled payment services to prioritize the adoption of the national QR code standard and implement appropriate measures to identify, monitor, and mitigate risks associated with QR-based transactions. They must likewise conduct end-user due diligence, transaction monitoring, and other risk control measures in accordance with applicable regulations and guidelines.

ACTIONABLE ADVICE

All BSIs shall strictly ensure that their AML/CTPF remain effective and commensurate with risk across all payment activities by:

1. Observing AML/CTPF requirements under the MORB and MORNBFI
2. Meeting the expectations on merchant due diligence, merchant identification, risk assessment, and monitoring under the MORPS
3. Implementing appropriate, effective, and risk-based mitigation measures
4. Reporting any suspicious transactions
5. Adopting commensurate end user due diligence, transaction monitoring, and other risk control measures for those using QR-enabled payments.