Bangkok Global Law
540, Unit 1705, 17th Floor, Mercury Tower,Ploenchit Road,
Lumpini, Pathumwan, Bangkok 10330 Thailand
Tel: +(66) 2 2525895-6 Fax: +(66) 2 2525897
Website: www.bgloballaw.com
E-mail: info@bgloballaw.com

The Merchant Fraud Management (MFM) Regulatory in Thailand's Electronic Payment Ecosystem

Electronic payments for goods and services in Thailand have grown rapidly, with transaction volumes increasing continuously. In this ecosystem, regulated payment service providers—particularly those enabling merchants to accept electronic payments—play a central operational role (e.g., card acquiring via EDC terminals, QR Code acceptance, and online direct debit).

The Bank of Thailand (BOT) identifies that insufficient "Know Your Merchant" (KYM) practices and weak merchant risk governance can generate systemic harm, especially as digital fraud techniques diversify. The risks include:

1. Unauthorized payment fraud (fraudsters transact by impersonating the customer), and
2. Authorized payment fraud (victims are deceived into initiating payment themselves), as well as merchant-side abuses such as fake merchants (no real goods/services), and sales of copyright-infringing goods.

The BOT issues the MFM requirements relying on its supervisory authority over regulated payment services.

The announcement applies to regulated providers offering electronic payment acceptance and related services, including: Electronic payment acceptance service providers, covering:

1. Acquirers,
2. Payment facilitators, and
3. Payee/collection service providers, and
4. e-Money service providers.

The framework is designed to cover both: (1) merchants with direct contractual relationships with the provider, and (2) merchants participating through connectivity structures, including master merchant / sub-merchant arrangements.

The framework is structured around (i) governance and policy design, (ii) implementation actions, and (iii) response and ecosystem coordination.

1. Policy and risk management framework
2. Actions: risk assessment, KYM onboarding, and ongoing monitoring
3. Response: incident reporting, fairness, and remediation
4. Information exchange and ecosystem coordination
5. Awareness raising
6. Reporting to the BOT and disclosure of sanctions
7. Data protection and recordkeeping

After the announcement takes effect, if a provider cannot fully comply with the policy-and-framework requirements under the governance section, it must complete implementation within 180 days from the effective date, without applying for a waiver, and promptly notify the BOT once compliant (in writing or electronically). For existing merchants onboarded before the effective date, providers must review and implement required actions within an appropriate timeframe based on each merchant's risk level.

Should you have any question, please do not hesitate to contact us via info@bgloballaw.com