Policy Guideline

Know Your Merchant (KYM)

4 October 2021 (B.E. 2564)

BANK OF THAILAND

Prepared by

Payment Systems Policy Department

Payment Systems Policy and Financial Technology Group

Bank of Thailand

Tel. 0 2283 5137, 0 2283 6718, 0 2356 7230

Fax. 0 2282 7717

e-mail: OversightDivisionPSD@bot.or.th

Table of Contents

Policy Guideline

Know Your Merchant (KYM)

---

1. Rationale

Currently, the payment through electronic channels for the purchase of goods or services from online merchants has been widely made with the continuously increased volume of transactions. Business providers of designated payment services (hereinafter referred to as "business providers") facilitate the merchants in receiving payment by electronic means, such as installing Electronic Data Capture (EDC) machines, providing Quick Response Code (QR Code), and other forms of receiving payment. However, the processes of getting to know and monitoring the risks of merchants of business providers are different, in terms of considering the risk of type of goods or services, the risk of merchants and the risk of methods of receiving payment. With inadequate risk assessments, these may result in the possibility of using a service of receiving electronic payment as a fraudulent channel, money laundering or non-compliance with applicable laws and regulations, which are subsequently leading to the damage to customers.

The Bank of Thailand hereby issues the Policy Guideline on Know Your Merchant (KYM) for a service of receiving electronic payment so that business providers can adopt it as a minimum standard in setting out a KYM process, and monitoring and managing merchant risks, which covers the specification of policy, risk management measures, internal control processes, risk monitoring and review based on the merchants' risk level. The key principles are as follows:

1) Categorizing merchants and setting out a KYM process which is in line with the merchants' risk level and other relevant laws and regulations.

2) Managing merchants' risk by using mechanisms, processes, systems, or tools that are appropriate to merchants' risk level, as well as having in place the ongoing monitoring and examining such risk management.

3) Setting out a KYM and risk monitoring standards between business providers, where such standards must not cause extensive burden on the business providers.

4) Ensuring that the payment system is secure for providing service.

2. Scope of Application

This Policy Guideline shall apply to business providers of designated payment services according to the Payment Systems Act B.E.2560 (2017).

3. Content

3.1 Definitions

In this Policy Guideline,

"Business provider" means a business provider of designated payment services according to the law governing payment systems.

"Receipt of electronic payment" means a transaction of receiving payment for goods or services via electronic means, electronic card or by any other means for and on behalf of a merchant, a service provider or a creditor.

"Credible source" means a source that provides or develops information with rationale, criteria or reference for people or business groups to examine or have access to various information.

"BOT" means the Bank of Thailand under the law governing the Bank of Thailand.

3.2 Policy Guideline on Know Your Merchant (KYM)

To know your merchants and monitor the risk of merchants, business providers shall do as follows:

3.2.1 Set out the policy, risk management measures, internal control processes, and risk monitoring and examining to cover the merchants categorization, KYM process, and risk monitoring that are in line with the merchants' risk level and

relevant laws and regulations e.g. regulations on customer identification and verification according to the anti-money laundering laws, regulations on Know Your Customer (KYC) for deposit-account opening, or for e-Money service opening. The policy shall be approved by the business providers' board of directors or designated committees, as well as communicated and included in a training session for the related staff and personnel to ensure the compliance with such policy, measures, and guidelines. The review and amendment of the policy, risk management measures, internal control processes, risk monitoring and examining, and compliance with the specified guidelines shall be carried out at least annually.

3.2.2 Assess and categorize merchants' risk level from data and evidence of the merchants. The merchants' risk level shall be categorized in line with nature and type of businesses. Risk factors related to fraud, money laundering and financing of terrorism according to, at least, the anti-money laundering laws, and non-compliance with relevant laws and regulations shall also be taken into consideration. Business providers may apply the risk factors specified by international card schemes to assess and determine the merchants' risk level. Merchants' risk can be categorized into the following 3 levels:

1) **General merchant:** a merchant considered by a business provider as selling general goods or services, not classified as high-risk or prohibited merchant.

2) **High-risk merchant:** a merchant considered by a business provider as selling high-risk goods or services based on the assessment using various risk factors, such as the type and selling channel of goods or services, business model, merchant location; or as it meets the criteria according to the anti-money laundering laws or any other relevant regulations. In this regard, a business provider may apply a Merchant Category Code (MCC) as specified by international card schemes to assess the merchants' risk.

3) **Prohibited merchant:** a merchant considered by a business provider as explicitly selling goods or services that are prohibited by laws or that would negatively affect public order, or good moral, such as a merchant selling goods

or services that fall under the definition of predicate offenses pursuant to the Anti-Money Laundering Act.

3.2.3 KYM Practices which cover the processes starting from merchants onboarding to ongoing monitoring and end of a relationship, to be in line with the merchants' risk level. All merchants shall comply with the minimum practices, while the high-risk merchants shall also comply with the additional practices as follows:

1) Minimum practices

1.1) Onboarding

1.1.1) Business providers must perform KYM on an owner or a person with managerial power of merchants, either a natural person or juristic person, by complying with the regulations on customer identification and identity verification pursuant to the anti-money laundering laws as well as the BOT's regulations on KYC for deposit-account opening, for e-Money service opening or for any other payment services, as the case may be.

1.1.2) Business providers must verify merchant's data and evidence, in accordance with a nature and a risk of each type of business, in order to ensure the accuracy, authenticity and up-to-date nature of such merchant's data and evidence.

1.2) Ongoing monitoring

1.2.1) Business providers shall set out measures, operational guidelines, processes, and mechanisms for monitoring and examining the risks and the movement of receiving payment transactions. They shall also regularly monitor and update the status of merchants they provide services to in order to be informed of the merchants' risk level that may have changed due to e.g. changes of the type of goods sold or income from sales of goods. In addition, they shall establish a list of merchants which need to have close monitoring (watch list).

1.2.2) Business providers shall oversee a process of monitoring and managing merchants' risk, which covers both master merchants and sub-merchants. They should also require the master merchants to comply with this

Policy Guideline in order to oversee their sub-merchants; for example, establishing a guideline to deal with the sub-merchants in case they detect any irregularities.

1.2.3) Business providers shall specify their risk indicators and frequency of monitoring and reviewing merchants' risk in accordance with their risk level to ensure that the merchant categorization still appropriately reflects the merchants' risk.

1.2.4) Business providers shall set out the procedures and timeframe to deal with any irregularities in the merchants' operations as well as set out a period and the reporting process to the management and related agencies, based on the significance of such irregularities.

1.2.5) Business providers shall set out a guideline to regularly update data of merchants, an owner or a person with managerial power of merchants as well as related information to ensure that such data are accurate and up-to-date.

2) Additional practices

2.1) Onboarding: For merchants' data and evidence verification, business providers shall verify from credible sources in order to indicate and ensure the accuracy, authenticity, and up-to-date nature of the merchants' data and evidence, e.g. verifying the merchants' company registration or electronic certificate from the Ministry of Commerce's database, conducting a site visit, and inspecting the merchants' online sales channel from the website.

2.2) Ongoing monitoring: For risk monitoring and examination, business providers must apply the more stringent approach for the high-risk merchants. In this regard, there must have systems or tools for monitoring and examining transactions of the merchants sufficiently and in a comprehensive manner or use a special approach e.g., increasing the frequency for an on-site visit or inspection of online sales channel, conducting mystery shopping. This approach shall also be applied to merchants on the watch list. In addition, there shall be an explicit guideline to deal with any irregularities found.

3) Prohibited merchant: Business providers must not provide services, give support or encouragement to any effort to violate the related laws or regulations.

4. Effective Date

This Policy Guideline shall come into effect from the 1 January 2022 (B.E. 2565) onwards.