BANK OF MAURITIUS

Guideline for Payment Aggregators

July 2026

(Page intentionally left blank)

TABLE OF CONTENTS

INTRODUCTION

The safety and efficiency of retail payment systems and instruments remain a key priority for the Bank of Mauritius (the "Bank") in view of their critical role in both the financial system and real economy.

The National Payment Systems Act 2018 (the "NPS Act") empowers the Bank to regulate, oversee and supervise the national payment systems and payment systems being operated in Mauritius primarily for the purpose of ensuring their safe, secure, efficient and effective operation and accessibility to the public.

The Bank is thus mandated to issue licences to entities to act as payment service providers, defined under section 2 of the NPS Act as *"an entity which provides payment services"*. Payment services for which the Bank may issue a licence are listed in the First Schedule of the NPS Act and include *"services functional to the transfer of money, including the issuance of electronic money and electronic money instruments, but excluding the provision of solely online or telecommunication services or network access"*.

Non-bank intermediaries such as payment aggregators act as a bridge between merchants and customers by enabling e-commerce platforms and merchants to accept a wide range of payment instruments from customers**.** Given that the services provided by payment aggregators are functional to the transfer of money, such entities are required to obtain a payment service provider licence in accordance with section 9 of the NPS Act.

Purpose

The objective of this Guideline is to provide a regulatory framework for the activities of **payment aggregators** with the objective of safeguarding the interests of customers and users of online and physical point-of-sale payments while also promoting the stability and integrity of the financial system.

The Guideline outlines the requirements that payment aggregators must comply with.

Authority

This Guideline is issued under the authority of section 17 of the NPS Act.

Scope of application

This Guideline applies to banks and payment service providers offering payment aggregator services. The Guideline shall also apply to banks and payment service providers engaging with payment aggregators.

This Guideline does not apply to entities, which provide exclusively technical services to merchants on behalf of a bank or payment aggregator through alternative delivery channels, as the entity does not handle funds or process payment transactions directly.

Relation to other guidelines issued by the Bank of Mauritius

Payment aggregators shall be subject to the prudential, anti-money laundering, combatting the financing of terrorism and proliferation, and regulatory requirements applicable to payment service providers licensed under the NPS Act. This includes compliance with relevant guidelines, directives and circular letters issued by the Bank of Mauritius.

Effective date

This Guideline shall come into effect on 31 August 2026.

Interpretation

Unless otherwise stated, the following definitions apply throughout this Guideline:

"acquirer" means a bank or financial institution that accepts and processes card and mobile payments on behalf of a merchant;

"NPS Act" means the National Payment Systems Act 2018;

"Bank" means the Bank of Mauritius established under section 3 of Bank of Mauritius Act 2004;

"bank" has the same meaning as in the Banking Act 2004;

"e-commerce marketplace" means a digitally enabled platform, which hosts multiple merchants and buyers;

"independent trustee" means a trustee who has no business relationship or interest in the payment aggregator or any of its subsidiaries or affiliates or another payment aggregator;

"KYC" means 'Know Your Customer';

"licence" means a payment service provider licence issued under the National Payment Systems Act;

"merchant" means any person who accepts payment instruments as a means of receiving payments in exchange for their goods and services;

"merchant payment" means a payment received from customers in exchange of goods and services delivered by the merchant;

"payment aggregator" means a payment service provider which –

(i) enables e-commerce platforms and merchants to accept various payment instruments, such as credit or debit cards, bank transfers, mobile payment and e-money, from customers; and

(ii) facilitates the processing of these transactions without the need for the merchant to set up its own payment integration system or maintain payment accounts with a bank;

"payment instrument" has the same meaning as in the National Payment Systems Act;

"payment service provider" has the same meaning as in the National Payment Systems Act;

"NPS Regulations" means the National Payment Systems (Authorisation and Licensing) Regulations 2021;

"trust" means a legal arrangement established for holding and managing funds from the payment aggregator scheme on behalf of the payment aggregator and onboarded merchants;

"trust account" means a bank account under the control of the trustees, used to hold funds on behalf of merchants participating in the payment aggregator scheme;

"trustee" means a person appointed by the payment aggregator with the approval of the Bank to manage the trust.

PART I - LICENSING AND CAPITAL REQUIREMENTS

1.1 Licensing process

1.1.1 No person shall carry out the business of payment aggregator in Mauritius without a licence or a written approval, as applicable, from the Bank.

1.1.2 A body corporate, other than a bank or a payment service provider, that intends to engage in payment aggregator business shall apply for a payment service provider licence from the Bank under the NPS Act and shall comply with the licensing requirements set out in the NPS Regulations.

1.1.3 A payment service provider or a bank that intends to offer payment aggregator services, shall seek the written approval of the Bank before offering the payment aggregator services.

1.1.4 The application for a licence or an approval shall be processed in accordance with the provisions of the NPS Regulations.

1.2 Transitional arrangements for existing entities

1.2.1 Existing non-bank entities currently offering payment aggregator services shall apply for a licence on or before 31 August 2026. These entities may continue their operations until the Bank determines their application. Any entity which fails to meet the licensing requirements shall cease its payment aggregator business on such date and in such manner as determined by the Bank.

1.2.2 E-commerce marketplaces which also provide payment aggregator services shall not continue the payment aggregator activity beyond the deadline specified at clause 1.2.1 above if they have not applied for a licence. E-commerce marketplaces intending to pursue the payment aggregator business should separate this activity from their marketplace operations and apply for a licence accordingly on or before 31 August 2026.

1.3 Minimum capital and ongoing capital requirements

1.3.1 A payment aggregator shall hold a minimum initial capital of Rs 5 million.

1.3.2 Notwithstanding clause 1.3.1 of this Guideline, a payment aggregator shall, after deducting its accumulated losses, maintain at all times in Mauritius a minimum

paid-up capital of Rs 5 million or 10 per cent of the average balance of the trust account over the preceding six months, whichever is higher. The capital requirement shall be reviewed and will be adjusted on a half-yearly basis or on an *ad hoc* basis as determined by the Bank, based on the transaction volume and risk profile of the payment aggregator's operations.

1.4 Effect of suspension or revocation of payment aggregator licence

1.4.1 Where a payment aggregator licence is suspended or revoked by the Bank in terms of Regulation 10 of the NPS Regulations, the payment aggregator shall immediately cease all payment aggregator activities from the effective date of suspension or revocation.

1.4.2 Upon suspension or revocation of a licence, the Bank shall notify any bank holding a trust account related to the business of the affected payment aggregator to immediately cease all transactions involving the funds held in the trust account. The bank shall await further directives from the Bank regarding the funds held in the trust account.

1.4.3 Subject to clause 1.4.2, the Bank may require the payment aggregator and its trustee to –

(a) cease immediately from carrying out the payment aggregator services;

(b) distribute the funds held in the trust account to the rightful beneficiaries within a prescribed timeframe and submit detailed reports of the distribution to the Bank as directed by the Bank;

(c) ensure that all relevant records and accounts identifying the beneficiaries of the trust account funds are made available to the trustees to facilitate accurate and timely distribution;

(d) cover any shortfall in the trust account; and

(e) provide the Bank with access to, or hand over, the complete database, electronic records in a readable format and other relevant information required for examination.

1.4.4 Regulation 10 of the NPS Regulations shall apply where the Bank decides to suspend or revoke a payment aggregator's licence.

1.4.5 The Bank shall notify the public of the suspension or revocation of a payment aggregator's licence in accordance with Regulation 10(6)(a) of the NPS Regulations.

1.5 Transitional arrangements

1.5.1 Payment aggregators operating as of the effective date of this Guideline shall be given a transition period of 6 months from the application date to meet the minimum paid-up capital requirement of Rs 5 million and maintain this minimum capital or any other capital amount prescribed by the Bank at all times thereafter.

1.5.2 A new applicant for a payment aggregator licence shall hold a minimum capital of Rs 5 million at the time of application.

1.5.3 Notwithstanding the above, the Bank reserves the right to review and revise the minimum paid-up capital requirement that a payment aggregator would be required to hold in light of the transaction volume and risk associated with its business activities.

PART II – GOVERNANCE ARRANGEMENTS

In addition to complying with the licensing requirements laid down in the NPS Regulations and the application form for a payment service provider licence, payment aggregators shall also adhere to the following governance standards:

2.1 Stakeholder agreements

2.1.1 Agreements entered into with merchants, acquiring banks and any other relevant stakeholders shall clearly define the roles and contractual responsibilities of each party. These agreements must specifically address:

(a) protection of customers' interest;

(b) handling and redressal of complaints;

(c) timely reversal of failed transactions;

(d) dispute resolution and chargebacks; and

(e) proper maintenance and protection of customer data.

2.1.2 The agreements shall include provisions for the suspension or termination of a merchant in cases where the merchant fails to comply with its contractual obligations.

2.2 Transparency and disclosure

2.2.1 Payment aggregators shall ensure that they publicly disclose in a clear manner information on their policies including:

(a) customer grievance redressal mechanisms;

(b) privacy policy;

(c) terms and conditions applicable to merchants onboarded by the aggregator; and

(d) any other relevant policies affecting users and merchants.

2.2.2 Payment aggregators shall ensure that their infrastructure complies with the rules and regulations issued by card schemes, Payment Card Industry Data Security Standard and any other applicable standards issued by recognised payment schemes.

2.3 Safeguards against money laundering and financing of terrorism and proliferation

2.3.1 AML/CFTP policy

Payment aggregators shall establish and maintain a board-approved Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation (AML/CFTP) policy which should be reviewed at least annually or upon any change in applicable laws or regulations or as otherwise required by the Bank.

2.3.2 Legal and regulatory compliance

Payment aggregators shall comply with the Financial Intelligence and Anti-Money Laundering (FIAML) Act, the FIAML Regulations, the Guideline on Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation issued by the Bank, other relevant laws, guidelines and directives issued by the Bank.

2.3.3 Internal controls

Payment aggregators shall implement adequate policies, procedures and internal controls to ensure that their institutions are not used, intentionally or unintentionally, by criminals for illicit activities.

2.3.4 Monitoring and reporting

Payment aggregators shall maintain appropriate systems and controls to:

(a) monitor transactions and detect suspicious transactions; and

(b) report suspicious transactions in accordance with applicable laws, regulations and regulatory requirements.

2.4 Merchant onboarding

2.4.1 Onboarding policy

2.4.1.1 Payment aggregators shall establish a board-approved merchant onboarding policy which shall be periodically reviewed to ensure its relevance in a rapidly evolving technology and payment landscape.

2.4.1.2 Payment aggregators shall not onboard any donation-collecting organization.

2.4.1.3 Merchant onboarding must be conducted in full compliance with:

(a) the Financial Intelligence and Anti-Money Laundering (FIAML) Act;

(b) the FIAML Regulations;

(c) the Guideline on Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation issued by the Bank; and

(d) other relevant laws, guidelines and directives issued by the Bank.

2.4.2 Due diligence and monitoring

2.4.2.1 Comprehensive due diligence shall be carried out on all merchants in accordance with the payment aggregator's onboarding policy. This process must be fully documented and include technical assessments such as internet traffic, information disclosure policy and privacy policy.

2.4.2.2 Payment aggregators shall maintain ongoing monitoring of onboarded merchants and take appropriate action, if adverse information is uncovered on any of its merchants.

2.4.2.3 All due diligence and assessment reports shall be made available to the Bank upon request.

2.4.2.4 The payment aggregator shall conduct appropriate due diligence on merchants which shall include background checks to identify any involvement in counterfeit or prohibited products, fraudulent practices or customer deception. Payment aggregators shall ensure that blacklisted merchants are not onboarded.

2.4.3 Transparency and customer protection

2.4.3.1 Payment aggregators shall ensure that merchants publicly disclose in a clear manner:

(a) terms and conditions of service;

(b) dispute resolution mechanisms; and

(c) processing timelines for returns and refunds.

Complaint facilities, where available through websites/mobile, should be easily accessible and user-friendly.

2.4.3.2 Agreements between the payment aggregators and merchants shall include provisions for the security and privacy of customer data. Payment aggregators shall comply with the Data Protection Act 2017 and shall also ensure that their onboarded merchants comply with the Data Protection Act 2017.

2.4.3.3 Customer complaints including those from merchants, shall be resolved within such time and in such manner as provided for in the payment aggregator's board-approved policy, and no later than 7 working days from the date of receipt of the complaint.

2.4.4 Sub-merchant oversight

2.4.4.1 Payment aggregators shall carry out appropriate KYC checks and due diligence on sub-merchants in cases where onboarded merchants engage with sub-merchants for delivery of goods and services.

2.4.5 Technical and security standards

2.4.5.1 Payment aggregators shall ensure that the infrastructure of the merchants engaged in online e-commerce are compliant with:

(a) Payment Card Industry Data Security Standard (PCI DSS); and

(b) standards issued by the PCI Security Standards Council, as applicable.

2.4.5.2 Merchant agreements shall include:

(a) security and privacy requirements for customer data;

(b) compliance to standards issued by the PCI Security Standards Council; and

(c) incident reporting obligations.

2.4.5.3 Merchants shall not retain any payment card data or credentials utilized by customers for making payments beyond the completion of the transaction. They shall keep records of transaction data only.

2.4.5.4 Payment aggregators shall obtain periodic security assessment reports either based on the risk assessment and/or at the time of renewal of contracts.

2.4.6 Suspension and termination

2.4.6.1 The agreements between payment aggregators and merchants shall include provisions for the immediate suspension or termination of any merchant found to be in breach of contractual obligations.

2.4.6.2 Payment aggregators shall immediately notify the bank holding the trust account upon the merchant's suspension or termination. Payment aggregators shall cease all transactions with the affected merchant.

2.4.7 Responsibilities of acquiring banks

2.4.7.1 Acquiring banks shall establish a clear policy governing the processing of payments for merchants onboarded through a payment aggregator.

2.4.7.2 While the acquiring bank is not required to conduct customer due diligence on each merchant directly, it must ensure that all relevant merchant information can be obtained promptly whenever required.

2.4.7.3 Furthermore, the acquiring bank of a payment aggregator shall ensure that the merchants onboarded by the payment aggregator comply fully with the bank's merchant acquiring policies and standards.

2.5 Trust account management

2.5.1 Payment aggregators shall hold funds collected as merchant payments in a trust account with one or more commercial banks. These funds must be segregated from the payment aggregator's own accounts and any other accounts related to its non-payment aggregator activities.

2.5.2 A non-bank payment aggregator is required to set up a trust, solely for the purpose of managing and overseeing the trust account.

2.5.3 A payment aggregator shall obtain the approval of the Bank prior to opening or operating a trust account.

2.5.4 The request for approval regarding section 2.5.3 shall include the following:

(a) a list of individuals or entities responsible for managing the trust account, including the names of the proposed trustees; and

(b) a copy of the trust deed.

2.5.5 Trustees must be independent and meet the requirements of section 27A of the NPS Act. They must also meet the fit and proper person criteria, as defined in the Guideline on Fit and Proper Person Criteria. This requirement applies to all individuals involved in managing the trust account.

2.5.6 Settlement process

2.5.6.1 All merchant payments received shall be automatically pooled into the trust account on the day on which the funds are received by the payment aggregator or on the next day, depending on the payment instrument.

2.5.6.2 Final settlement with the merchant by the payment aggregator shall be effected as follows:

(a) where the payment aggregator is responsible for delivery of goods or services, the payment to the merchant shall be no later than the day after the date on which the payment aggregator is informed about the shipment/delivery of goods by the merchant;

(b) where the merchant is responsible for delivery, the payment to the merchant shall be made no later than one day after the delivery date, subject to terms and conditions applicable;

(c) where the agreement with the merchant provides for holding funds by the payment aggregator till expiry of refund period, the payment to the merchant shall be made no later than one day after the expiry of the refund period;

(d) refunds, other than those managed directly by the merchants in accordance with the agreement with the payment aggregator and customer's knowledge, and credits for reversed transactions, where funds are received by the payment aggregator, shall be routed through the trust account. The payment aggregator will refund the customer by debit of the trust account no later than one day after receipt of funds.

2.5.7 Record-keeping and reconciliation

In addition to the requirements of Section 23 of the NPS Act, payment aggregators shall also comply with the following requirements:

2.5.7.1 The payment aggregator shall ensure accurate recording, management and monitoring of all merchant accounts, at all times.

2.5.7.2 Traceability of funds collected, and deposited in the trust account held in accordance with sub-section 2.5.1 pertaining to each merchant, shall be ensured.

2.5.7.3 All settlement records shall be retained for a minimum period of seven years.

2.5.7.4 The payment aggregator shall have board-approved policies and procedures which should describe the reconciliation process to ensure consistency between the balance on the trust account with merchant transactions.

2.5.8 Additional provisions

2.5.8.1 The payment aggregator shall be allowed to pre-fund the trust account with its own or merchants' funds for specific purposes.

2.5.8.2 Cash transactions are strictly prohibited in the trust account. Payments permitted to and from the trust account shall be as detailed below:

2.5.8.2.1 Credits

(a) payments received from customers for purchase of goods/services;

(b) transfer related to refunds for failed, disputed, returned and cancelled transactions;

(c) funds received for onward transfer to merchants under promotional activities, incentives, cashbacks, etc.; and

(d) any other transfers as specified in the merchant agreement.

2.5.8.2.2 Debits

(a) payments to merchants;

(b) payment to any other account on specific instructions from merchants;

(c) transfers representing refunds for failed/disputed transactions;

(d) payment of commissions to the payment aggregator. This amount shall be at pre-determined rates and frequencies; and

(e) disbursement of funds received under promotional activities, incentives, cashbacks, etc.

2.5.8.3 A trustee maintaining the trust account shall:

(a) ensure that adequate risk management procedures are implemented to mitigate the risks associated with the operation of the trust account; and

(b) submit to the Bank a copy of the annual audited accounts not later than three months after closure of the financial year.

2.5.8.4 The payment aggregator shall submit an auditor's certificate to the Bank at the end of each financial year certifying that the payment aggregator has been maintaining the trust account/s in compliance with this Guideline. In case the payment aggregator maintains more than one trust account, the certificate should explicitly cover each trust account.

2.5.8.5 The payment aggregator shall provide the bank holding the trust account with a list of merchants acquired by them and shall ensure that the list is up to date at all times. The trustee shall ensure that payments are made only to eligible merchants and for eligible purposes. The agreement signed between the payment aggregator and the bank holding the trust account shall contain a provision to restrict usage of the balance in the trust account only for purposes mentioned at section 2.5.8.2 above.

2.5.8.6 No interest shall be payable by the bank on balances in the trust account.

2.6 Complaint handling and dispute resolution

2.6.1 The payment aggregator shall maintain a comprehensive customer complaint management policy, which should include grievance redressal procedures, dispute resolution mechanisms and an escalation matrix.

2.6.2 The payment aggregator must appoint dedicated officer/s responsible for handling customers' complaints. These officers should be adequately trained to ensure prompt and effective resolution of complaints.

2.6.3 The customer grievance and dispute resolution framework shall be publicly disclosed. The complaint facility, if made available on website/mobile, shall be clearly visible, easily accessible and user-friendly.

2.6.4 The dispute resolution mechanism shall be transparent and include, *inter alia*, conditions for reversals and refunds, transaction life cycle overview, detailed categorization and documentation of dispute types, dispute management process, stakeholder responsibilities and defined timelines for dispute resolution.

2.7 Security, fraud prevention and risk management policy

The payment aggregator shall comply with the Guideline on Cyber and Technology Risk Management and the following requirements:

2.7.1 The payment aggregator shall have board-approved information security and risk management policies to safeguard customers from fraud and other risks. Both merchants and payment aggregators shall put in place robust information and data security infrastructure and systems for the prevention and detection of fraud.

2.7.2 The payment aggregator shall establish a formal mechanism for monitoring, managing and following up cybersecurity incidents and breaches.

2.7.3 Payment aggregators shall ensure that:

a) all relevant risks associated to the use of merchant's payment acceptance device are mitigated; and

b) digital payment services involving sensitive customer and counterparty information offered via mobile devices are adequately secured.

Bank of Mauritius
10 July 2026