SINGAPORE FINTECH ASSOCIATION (SFA)

PAYMENTS INDUSTRY CODE OF CONDUCT

TABLE OF CONTENTS

A. INTRODUCTION

1. Scope and Applicability

1.1 This Code aims to set out consistent professional standards and standards of transparency which may be adopted by holders of a major payment institution licence, standard payment institution licence, money-changing licence, or exempt payment service providers under the Payment Services Act 2019 ("**PS Act**"), as they may relate to any one or more regulated "payment services" that is **not** a "digital payment token service" (for the purposes of this Code, "**PSPs**"). Where a PSP operates a hybrid business model or provides a combination of multiple regulated activities, or is an exempt payment service provider that carries on other regulated activities outside the scope of the PS Act, this Code shall apply strictly to its non-digital payment token services that constitute "payment services" under the PS Act. In the context of exempt payment service providers in particular, this Code shall cover only the conduct of "relevant payment services" as such term is defined in section 13(13) of the PS Act. For the avoidance of doubt, the Code does not extend to, nor govern, any digital payment token or crypto-related payment services conducted by the PSP.

1.2 PSPs are already subject to requirements under the PS Act, and the regulations, notices and guidelines promulgated thereunder ("**Applicable Regulations**") as administered by the Monetary Authority of Singapore ("**the Authority**" or "**MAS**"). This Code is **not** intended to overlap with or override any such requirements. To the extent that any provisions of this Code conflict with Applicable Regulations, the latter will prevail. In addition, where the Code sets out a general principle but Applicable Regulations are prescriptive, PSPs (whether or not Code Adherents, as defined below) would be required to comply with the prescriptions of the Applicable Regulations.

1.3 To be clear, this Code sets out general standards of professional conduct which PSPs may choose to adhere to, as well as general principles which PSPs adhering to the Code agree to abide by in their dealings with customers and other members of the industry, in addition to what is required under Applicable Regulations. The objective of this Code is to provide for consistent standards of professional conduct and to contribute to a stronger, more transparent payments industry in Singapore.

1.4 **To avoid doubt, this Code does not automatically apply to all PSPs and PSPs may choose to adhere to the Code or not to adhere to the Code**. Please see Section A.2. below for more information.

2. Adherence to the Code

2.1 Voluntary Adherence via Self-Assessment: adherence to this Code is voluntary. PSPs may choose to adhere to the Code by conducting a self-assessment of their internal policies, processes, and systems against the principles and standards set out herein. A PSP that has successfully completed this self-assessment and determined that it meets the requirements of this Code shall be referred to as a "Code Adherent." For the avoidance of doubt, adherence is based entirely on the PSP's own self-assessment and does not constitute independent verification, regulatory approval, or third-party certification by the SFA, nor does it subject the PSP to any supervisory obligations or oversight by the SFA.

2.2 Public declaration: upon satisfying themselves of their compliance through self-assessment, Code Adherents may make a public statement indicating that the firm adheres to the best practices outlined in the SFA Payments Industry Code of Conduct. Such a public declaration must clearly state the year in which the self-assessment was conducted. To maintain the "Code

Adherent" status, the self-assessment and accompanying public declaration shall have a validity duration of one (1) year, after which the “Code Adherent” status expires unless a renewed self-assessment is completed.

2.3 Accuracy of representation: Code Adherents acknowledge that public declarations of adherence must be accurate and substantiated by their internal policies and practices. Code Adherents are responsible for ensuring their ongoing compliance to maintain the validity of their public declaration and to avoid making any false or misleading claims to customers and the public. Where a Code Adherent does not complete a renewed self-assessment upon expiry of the validity period referred to in Clause 2.2, it should cease making any public-facing statement or representation that it adheres to this Code, and should remove or update any public-facing materials referring to such adherence until a renewed self-assessment has been completed.

3. Core Principles

3.1 **Fair Treatment:** Code Adherents are committed to the general principle of ensuring fair dealing and fair treatment across all customer segments, including small-and-medium-sized enterprises (“**SMEs**”), large enterprises, sole proprietors, and individual consumers. To establish a common standard, Code Adherents agree to be guided by the applicable principles set out in the MAS Guidelines on Fair Dealing, particularly the outcomes ensuring that (a) customers are provided with clear, relevant, and timely information to make informed decisions; and (b) customer complaints and disputes are handled in an independent, effective, and prompt manner.

3.2 **Proportionality:** The extent to which a Code Adherent adheres to this Code shall be proportionate to the size and risk profile of the Code Adherent, considering its business model, customer base, transaction types, and risk exposure.

3.3 **Collaboration:** To foster collective defence against broad industry concerns and to strengthen the integrity of the Singapore payments industry, Code Adherents are committed to participate in structured, industry-wide high-level collaboration (e.g. regular meetings) to address systemic challenges, including but not limited to anti-money laundering (“**AML**”) and countering the financing of terrorism (“**CFT**”) risks, consumer protection risks such as those arising from fraud and scams, technology risks, and interoperability concerns.

3.4 **AML/CFT Frameworks**: To effectively manage AML and CFT risks, Code Adherents shall establish and maintain robust policies, procedures, and controls commensurate with their risk profiles. Code Adherents agree to abide by the standards set out in the relevant MAS Notices on Prevention of Money Laundering and Countering the Financing of Terrorism and their accompanying guidelines.

B. GOVERNANCE AND RISK MANAGEMENT

4. Operational Resilience and Critical Systems

4.1 All PSPs are required, by virtue of their obligations under Applicable Regulations, to identify critical systems and conduct stress testing on these systems. Beyond this, all Code Adherents specifically identify and stress-test the following types of critical systems as may be applicable to their business model; namely —

- Ledger and wallet systems;
- Payment gateway and payment switch systems;
- Customer-facing application programming interfaces ("**API**") and mobile back-end systems; and
- Authentication systems and services, including those relating to the provision of one-time passwords ("**OTP**").

The list above is not exhaustive and Code Adherents may identify and stress-test more critical systems as may be required by Applicable Regulations.

5. Adherence to API Framework

5.1 Code Adherents adopt the MAS API framework for open banking to the extent commensurate with the nature, scale, and complexity of their businesses. This includes but is not limited to transactional APIs (such as for executing funds transfers), account information APIs (such as for retrieving wallet balances or transaction history), and product service APIs (such as for publishing foreign exchange rates or fee structures).

5.2 Where relevant, Code Adherents obtain mandatory cybersecurity certifications from third-party vendors to promote interoperability and innovation while maintaining security. This includes but is not limited to internationally recognised standards such as ISO/IEC 27001 (Information Security Management) and SOC 2 Type II, as well as local standards such as the Multi-Tier Cloud Security (MTCS) SS 584 standard.

C. CORE SERVICE ATTRIBUTES

6. Pricing and Transparency

6.1 **Principle of upfront disclosure:** Applicable Regulations already require that all PSPs must ensure that all applicable fees, charges, and rates are disclosed to customers in a clear, transparent, and prominent manner, prior to the initiation of the payment transaction. Code Adherents commit to the general principle that a customer must be able to view the full cost of any given transaction before committing to the transaction.

6.2 **Total cost of transaction:** To facilitate commitment to this principle, Code Adherents ensure that disclosures to customers will include:

- **Monetary amount:** The total fees and charges levied by the Code Adherent for any given transaction are expressed as a specific monetary amount in the currency of the payer's account, prior to the receipt of the customer's instructions to initiate a payment order or execute a transaction; and
- **Exchange rates (where applicable):** Where a currency conversion service is offered, Code Adherents must clearly disclose the exchange rate applied to the transaction where practicable prior to the transaction (recognising that for certain use cases, such as card payments involving dynamic network rates, upfront display may not be technically possible).

6.3 **Prohibition of drip pricing:** Code Adherents agree they will not engage in "drip pricing," where mandatory charges are not disclosed upfront but are added during the transaction process.

All unavoidable costs known to the Code Adherent must be included in the total amount shown to the customer before the transaction is executed in accordance with clause 6.2 above.

6.4 **Clarity on mark-ups:** As a commitment to leading standards of consumer transparency, any Exchange Rate Mark-up or mark-up applied over a reference benchmark rate constitutes a cost to the customer. Therefore, Code Adherents must not represent a service as "free" or "zero fee" if the total cost to the customer includes an Exchange Rate Mark-up, unless this cost component is explicitly and prominently disclosed or otherwise made transparent alongside the claim.

6.5 **Breakdown of charges:** The final transaction summary presented to the payer prior to execution must clearly show (to the extent such information is known and within the control of the Code Adherent):

- The principal amount to be transferred;
- The transaction fees payable in accordance with clause 6.2 above;
- The applicable exchange rate, and where applicable, the existence of any Exchange Rate Mark-up or range of mark-ups; and
- The final amount to be transacted.

D. MARKETING AND ADVERTISING

7. Advertising Standards and Expectations

7.1 **Adherence to CPFTA and SCAP:** Code Adherents shall strictly adhere to the Consumer Protection (Fair Trading) Act ("**CPFTA**") and the Singapore Code of Advertising Practice ("**SCAP**") administered by the Advertising Standards Authority of Singapore ("**ASAS**"), to the extent applicable.

7.2 **Transparency in claims:** Advertisements must not give a false or misleading impression regarding the cost of the service.

- **"Zero-fee" claims:** In setting a leading standard for marketing transparency, Code Adherents shall not state or imply that a service is "free" or "low cost" if other fees and charges, including revenue derived from Exchange Rate Mark-ups, are involved.

- **Material information:** The existence of any such differential or mark-up is considered material information and must be disclosed to prevent misleading omissions under the CPFTA.

7.3 **Comparability:** Where an advertisement makes a comparison with competitors, the comparison must be fair, accurate, and capable of substantiation.

- Comparisons must compare like with like (e.g. total cost of transaction vs. total cost of transaction).
- Code Adherents must not selectively exclude their own costs while highlighting competitors' fees, to create a false impression of cost-savings in choosing one PSP over another.

7.4 **Free trials:** In the case of free trials, providers should notify consumers before the end of the trial period and provide clear information on any subsequent chargeable fees and the cancellation process.

8. Terms and Conditions

8.1 **Plain Language Summaries:** Without prejudice to the general requirement in Applicable Regulations for disclosures to customers to be written in plain language that avoids the use of technical jargon, Code Adherents shall specifically provide plain-language summaries of terms and conditions that are concise and written in simple, non-technical language. These summaries are non-binding, non-exhaustive, for convenience only, and do not replace full terms and conditions (T&Cs).

8.2 **Accessibility:** Material terms regarding pricing, fees, and liability must be clearly disclosed in the transaction flow and advertisements, not solely within a separate legal document. For space-constrained media such as short-form advertisements, abbreviated signposting (e.g. prominently stating "fees apply" or "T&Cs apply") alongside a direct link or clear pathway to the full material terms is acceptable.

E. CONSUMER PROTECTION MEASURES

9. Fraud Prevention Frameworks

9.1 Code Adherents shall implement a documented fraud prevention framework within their internal controls to enhance consumer protection. A sufficiently robust framework must include, at a minimum, regular fraud risk assessments, real-time transaction monitoring, clear incident response and escalation procedures, and ongoing user education regarding prevalent scam typologies.

9.2 **Industry collaboration:** Code Adherents shall participate in, support, or contribute to SFA-led, MAS-led, or other structured industry-wide collaboration initiatives, where relevant and proportionate to their business model, size, and risk profile, including any Fraud and Risk Committee or equivalent forum established by SFA, MAS, or the industry. Such initiatives may comprise representatives from Code Adherents, financial institutions, AML compliance professionals, and other relevant industry participants, including persons to whom this Code may not apply - to facilitate coordinated alerts and proactive engagement on fraud and scam activities, sharing high-level, non-sensitive information such as trends and typologies.

10. Card Dispute Liability

10.1 Code Adherents offering card-based payment services, in their capacity as issuers, to their customers—whether for debit cards or other types of payment accounts, and whether such cards may be used for local or overseas purchases, online and/or offline—shall establish clear terms and conditions governing the customer's liability in transaction disputes, specifically regarding fraudulent, lost, or stolen card transactions. Such terms and conditions should be included in the primary agreement entered into between the Code Adherent and its customer (being the cardholder) setting out the principal terms of the card issuance and usage.

10.2 **Liability standards:** Code Adherents shall adopt standards commensurate with those applicable to banks under the Association of Banks in Singapore (ABS) Code of Practice for Banks - Credit Cards.

10.3 These standards shall include:

- Defining liability caps for customers (e.g. capping liability for unauthorised transactions prior to reporting the loss at S$100, provided the customer has not acted fraudulently or with gross negligence, or has failed to inform the card issuers as soon as reasonably practicable after becoming aware that his or her card has been lost or stolen), with the issuer retaining the discretion to waive such liability for unauthorised transactions on a case-by-case basis;

- Defining prescribed instances in which customers will not be liable for unauthorised transactions provided the customer did not act fraudulently or with gross negligence, including (a) where the card was not stolen but card details were used for unauthorised transactions to make purchases over the telephone or Internet; (b) unauthorised PIN-activated transactions;

- Where applicable, the prompt waiver or refund of any interest and late fees levied during the period when investigations on unauthorised transactions are being carried out;

- Clear rights for issuers to terminate services to the customer and pursue legal action to recover outstanding amounts arising from unauthorised transactions, in the event a customer is found grossly negligent but refuses to settle the outstanding amount;

- Obligations for customers to provide necessary information and documentation to assist issuers in investigations to determine responsibility and liability;

- Clear procedures for stopping the use of the card as well as procedures for reporting loss or theft of the card;

- Provision of a dedicated hotline for cardholders to report loss; and

- Establishing clear dispute resolution protocols that align with the aforementioned Fair Dealing principles.

F. DATA PRIVACY AND SECURITY

11. Protection of Data Internally

11.1 Code Adherents shall implement robust internal controls to protect customer and transaction data and protect the integrity of their business activities. In establishing these controls, Code Adherents should refer to common industry standards, including the MAS Guidelines on Risk Management Practices - Internal Controls, where appropriate.

11.2 These controls must include, where applicable:

- Role-based access restrictions;
- Segregation of duties;
- A documented compliance policy; and
- Audit trails or equivalent controls to ensure sensitive data (e.g. transaction volumes, client patterns) is not unnecessarily circulated or misused.
- Regular internal audits and vulnerability assessments to evaluate the effectiveness of the control environment.

12. Data Minimisation and Compliance

12.1 Compliance with PDPA: Code Adherents agree to abide by the principles and obligations set out in the Personal Data Protection Act 2012 (“PDPA”), including its subsidiary legislation and the Advisory Guidelines issued by the Personal Data Protection Commission (“PDPC”), to the extent applicable to their operations.

12.2 Code Adherents commit to the principle of data minimisation, which means collecting and processing only essential customer information that is reasonably necessary for legitimate business or legal purposes.

13. Data Breach Protocols

13.1 In the event of a data breach that is likely to result in significant harm to affected individuals or is of a significant scale, Code Adherents must notify affected users and the PDPC as soon as practicable, and in any event within 3 calendar days after assessing the breach to be notifiable.

13.2 Code Adherents undertake to adhere to this timeline for notification as a commitment to industry transparency and trust.

G. DEFINITIONS

14. Definitions

14.1 In this Code, unless the context otherwise requires:

"Critical Systems" means system, the failure of which would cause significant disruption to the operations of the Code Adherent or materially impact the Code Adherent's services to customers, including systems which process transactions that are time critical or are essential to the continuous provision of payment services.

"Drip Pricing" means the practice of advertising a price that is lower than the actual final price by adding fees or charges during the transaction process that were not disclosed upfront.

"Exchange Rate Mark-up" means the difference between the exchange rate offered to the customer and the Mid-Market Rate or benchmark rate obtained by the Code Adherent, representing a cost to the customer and/or revenue to the Code Adherent.

"Mid-Market Rate" means the midpoint between the buy and sell prices of two currencies in the open market, or an aggregated mid-market benchmark rate for the relevant currency pair, derived from multiple observable market sources and administered or published by a neutral and reputable benchmark administrator in accordance with a transparent methodology and appropriate governance arrangements, which complies with the IOSCO Principles for Financial Benchmarks. Such rate should accurately reflect prevailing market conditions and, where reasonably available, be updated or made available with a delay of no more than 10 minutes. For currencies where such an aggregated mid-market benchmark rate is not reasonably available, the Mid-Market Rate may reflect the latest available traded or observable market price from a neutral and reputable source.

APPENDIX

Template for Public Declaration of Adherence

[Full legal name of firm] declares that it has conducted a self-assessment of its internal policies, processes, systems, and controls against the principles and standards set out in the Payments Industry Code of Conduct (the "**Code**") as reviewed by members of the Singapore Fintech Association ("**SFA**").

As at the date of this self-assessment, [firm name] considers itself to be a **Code Adherent** as defined in the Code, in respect of its provision of the following payment services:

- [List specific regulated payment services / products / business lines]

For the avoidance of doubt, this declaration applies only to the non-digital payment token related payment services identified above. It does not apply to any digital payment token, crypto-related, or other regulated activities that [firm name] may conduct. Such activities are outside the scope of the Code.

[Firm name] acknowledges that adherence to the Code is voluntary and based on its own self-assessment. This declaration does not constitute independent verification, regulatory approval, third-party certification, or supervisory oversight by SFA, the Monetary Authority of Singapore, the views of its auditors or third-party advisors, or any other party. The Code has been published as reviewed by members of the SFA, but the SFA does not purport to exercise any ongoing oversight, whether of a supervisory or self-regulatory nature or otherwise, of the veracity of this self-assessment or the consistency of the conduct of Code Adherents with this self-assessment.

[Firm name] further acknowledges that this declaration must be accurate and substantiated by its internal policies and practices. [Firm name] is responsible for maintaining ongoing adherence to the Code during the validity period of this declaration, including in relation to fair treatment of customers, pricing and transparency, advertising standards, fraud prevention, operational resilience, internal controls, and data privacy and security, and ensuring it does not make any false or misleading claims to customers and the public. [Firm name] understands that this self-assessment may amount to a representation on its part as to any relevant fact or state of affairs that may be suggested by adherence with the Code, and is responsible for any inaccuracy, whether by way of negligence or fraud or otherwise, in that representation.

This declaration is valid for one year from [date] to [date], unless withdrawn, superseded, or renewed following a further self-assessment.

Signed for and on behalf of [firm name]

Name: [authorised signatory]

Designation: [title]

Date of self-assessment: [date]

Date of declaration: [date]

Contact: [email / website / compliance contact