FMMPAY Privacy and Security Agreement

1. Effectiveness of the Agreement

1.1 This Privacy and Security Agreement (hereinafter referred to as the “Agreement”) is formed and becomes effective as of the date on which the following parties actually use the Services, and shall be legally binding upon both parties.

(1) “FMMPAY” means the collective reference to the relevant legal entities within the FMMPAY group that are lawfully incorporated under the laws of Hong Kong, Mainland China, the United States, or other relevant jurisdictions, and that legally hold payment or related business licenses, permits, or registrations, and that provide the services under this Agreement; the specific service provider entity shall be the entity from which the User actually receives the services.
(2) “User” means any natural person, legal person, or other organisation that enters into a User Service Agreement with the FMMPAY operating entity, completes registration, and uses the Services.

1.2 Whereas the parties have established a cooperative relationship in respect of FMMPAY services, and FMMPAY is required to process the User’s personal data in the course of providing the services, in order to clarify the rules governing the entire data processing lifecycle and to clearly define the respective rights and obligations of both parties with respect to privacy protection and data security, this Agreement is entered into pursuant to the Personal Data (Privacy) Ordinance (Cap. 486) of Hong Kong (hereinafter referred to as the “PDPO”), the Payment Systems and Stored Value Facilities Ordinance (Cap. 584), the Personal Information Protection Law of Mainland China (if applicable to Mainland China service scenarios), the California Consumer Privacy Act (CCPA) of the United States (if applicable to United States service scenarios), and regulatory requirements relating to cross-border transfer of personal information in other applicable jurisdictions , through equal consultation between the parties, and shall be jointly observed.

2. Declarations and Undertakings of the Parties

2.1 Declarations and Undertakings of FMMPAY

FMMPAY hereby declares and undertakes that:

(1) It has established a data processing system that complies with the PDPO and international data security standards (ISO/IEC 27001 Information Security Management System), is equipped with dedicated data security officers and compliance teams, and possesses comprehensive technical and management capabilities to safeguard the security of User data;

(2) All data processing activities strictly adhere to the principles of “lawfulness, fairness, and necessity”, and data is processed solely within the scope agreed under this Agreement, without carrying out any processing activities beyond the authorized scope;

(3) It has completed the necessary compliance filings in respect of cross-border data transfer matters.

(4) It has formulated a Data Security Incident Emergency Response Plan, which specifies the classification criteria for incidents such as data leakage, loss, and misuse such as general incidents, major incidents, and serious incidents, response procedures including incident detection, assessment, containment, and remediation, responsible departments (led by the data security officer, in coordination with the compliance team and technical team), and internal and external notification time limits; a summary version of the emergency response plan may be provided upon reasonable request by Users.

2.2 Declarations and Undertakings of the User

The User hereby declares and undertakes that:

(1) The User has fully read all provisions of this Agreement through channels such as the FMMPAY official website and APP pop-up windows, has fully understood the purposes, scope, methods, and potential risks of FMMPAY’s processing of the User’s personal data, and voluntarily agrees that FMMPAY may process the User’s personal data in accordance with this Agreement;

(2) All personal data provided by the User to FMMPAY is true, accurate, and complete, with no false statements or material omissions;

(3) If the User is a natural person, the User confirms that he or she has reached the age of eighteen (18) and has full civil capacity; if the User is a legal person or other organisation, the User confirms that the signing representative has obtained lawful authorisation; if the User is a minor, the User’s legal guardian has fully read this Agreement and has provided

written consent for FMMPAY to process the minor's personal data, and shall assume corresponding guardianship responsibilities.

3. Core Definitions

3.1 "Personal Data" means information that can directly or indirectly identify a specific individual, including but not limited to a natural person's name, identification document number, contact details, address, bank account information, biometric information; as well as personal information of the legal representative and authorised representatives of corporate Users, and contact person information.

3.2 "Cross-Border Data Transfer" means the act by which FMMPAY transfers Users' personal data stored within the United States to other jurisdictions outside the United States through dedicated lines, cloud storage synchronisation, API interface calls, or other means, regardless of whether the recipient is a FMMPAY affiliated company, a cooperating institution, or any other third party.

3.3 "Sensitive Personal Data" means personal data which, once leaked, illegally provided, or misused, may result in damage to the User's personal dignity or significant harm to property interests, including but not limited to biometric information such as facial information, fingerprint information, bank account passwords, credit card CVV codes, precise location information, health information, personal information of minors, religious belief information, racial information, etc.

3.4 "Anonymised Data" means data processed by FMMPAY through irreversible technical means such as deletion of personal identification fields, data desensitisation, or aggregation, such that specific Users can no longer be directly or indirectly identified and the data cannot be restored by any technical means.

3.5 "Data Recipient" means the entity that receives Users' personal data in scenarios of cross-border data transfer or data sharing, including overseas affiliated companies within the FMMPAY group, overseas cooperating banks, clearing institutions, compliance screening service providers, and others. FMMPAY shall require all Data Recipients to execute data processing agreements that specify their data protection obligations, including compliance with applicable data laws, implementation of security safeguard measures, and prohibition of data processing beyond the authorised scope, and shall supervise their processing activities.

4. Data Collection

4.1 FMMPAY adheres to the principle of “minimum necessity” and collects only the personal data necessary to achieve service purposes, which is specifically divided into two categories: basic necessary data and scenario-based supplementary data, and does not collect any irrelevant data.

4.2 Basic Necessary Data:

Such data constitutes a prerequisite for FMMPAY to provide core services and must be provided by the User; failure to provide such data will result in the inability to activate the services.

Among them, natural person Users are required to provide: name, scanned copy of valid identification documents, real-name registered domestic and overseas mobile phone numbers, and bank account information under the User’s own name;

corporate Users are required to provide: copy of business license, unified social credit code, scanned copy of identification documents of the legal representative, scanned copy of identification documents of authorised representatives and power of attorney, and corporate bank account information.

4.3 Scenario-Based Supplementary Data:

Such data is collected only when the User applies for specific value-added services; FMMPAY shall clearly inform the User of the collection purpose in advance, and the User may independently choose whether to provide such data; failure to provide such data shall only affect the use of the specific value-added service and shall not affect the normal provision of core services.

4.4 Technical Data:

For the purposes of ensuring service security and preventing transaction risks, FMMPAY shall automatically collect certain technical data during the User’s use of the services, specifically including device model, operating system version, browser type, IP address (used only for geographical location and risk screening, not linked to personal identity), login time, operation logs (such as click paths, transaction confirmation actions). Such data is used solely for security verification and risk prevention and does not involve any personal privacy information.

4.5 FMMPAY collects Users’ personal data through lawful and transparent means, including the following three methods, and all collection activities are recorded in a traceable manner.

(1) Personal data uploaded or filled in by the User through official channels such as the FMMPAY official website, mobile APP, and WeChat Mini Program, including scanned identification documents, business supporting materials, and bank account information;
(2) Technical data automatically recorded by the FMMPAY system during the User's login, operation, and transaction processes, which is collected in real time, strictly limited to the scope set out in Section 4.4, and does not include any technical data unrelated to service security;
(3) Personal data obtained by FMMPAY from cooperating third parties in order to complete identity verification, transaction confirmation, and other service requirements, in respect of which FMMPAY shall strictly review the legality of third-party data provision, ensure that the third party has obtained the User's explicit authorisation, and ensure that the scope of data provision does not exceed the authorised scope. If the data provided by a third party is false, illegal, or exceeds the authorised scope, FMMPAY has the right to terminate cooperation with such third party and require it to assume corresponding responsibility; if this causes losses to Users, the third party shall bear compensation liability (except where FMMPAY is at fault).

5. Rights and Obligations

5.1 Rights and Obligations of FMMPAY

5.1.1 Before collecting data, FMMPAY shall clearly inform the User, through prominent means such as service interface pop-ups, registration agreement appendices, and policy disclosures on the official website, of the purpose, scope, subsequent processing methods of data collection, and the rights enjoyed by the User, to ensure that the User is fully informed; with respect to the collection of scenario-based supplementary data, FMMPAY shall separately obtain the User's explicit consent through pop-ups or written forms, and shall not collect such data if the User does not consent.

5.1.2 FMMPAY shall establish registers for all data collection activities, recording the collection time, collection method, data type, collection purpose, and User authorisation status, and shall retain such registers for a period of not less than three (3) years.

5.1.3 FMMPAY has the right to conduct authenticity and completeness reviews of paper-based or electronic data submitted by the User, and where data is incomplete or questionable, shall promptly notify the User to supplement or verify such data, and shall not arbitrarily use questionable data.

5.1.4 FMMPAY shall strictly process Users' personal data in accordance with this Agreement and relevant laws and regulations, and shall not collect, use, or transfer data beyond the authorised scope.

5.1.5 FMMPAY shall fully perform the security safeguard obligations stipulated in this Agreement, and in the event of a data security incident, shall immediately activate emergency response plans, take remedial measures such as suspending data transmission, repairing vulnerabilities, freezing involved accounts, and notify according to the following time limits: for general incidents such as temporary inaccessibility of non-sensitive data of a single user, notify the User within 24 hours; for major incidents such as suspected leakage of sensitive data of 10-100 users, notify the User within 12 hours and report to PCPD within 24 hours; for serious incidents such as leakage of sensitive data of more than 100 users, notify the User within 4 hours and report to PCPD within 12 hours.

5.1.6 FMMPAY shall establish convenient channels for the exercise of rights, (Customer service hotline, email) timely respond to Users' applications for inquiry, correction, deletion, and withdrawal of consent. Inquiry and withdrawal of consent applications shall be processed and responded to within 5 working days; correction and deletion applications shall be processed and responded to within 10 working days, which may be extended to 15 working days if third-party assistance is required for verification, and the User shall be notified in advance of the reason for the extension, and shall not unreasonably delay or refuse legitimate requests for the exercise of Users' rights.

5.1.7 FMMPAY shall establish complete records of all data processing activities for regulatory inspection and User inquiry purposes.

5.2 Rights and Obligations of the User

5.2.1 The User shall ensure that all personal data provided to FMMPAY is true, accurate, and complete, without falsification, tampering, or impersonation of others; where third-party data is provided, the User shall ensure that lawful authorisation has been obtained from such third party.

5.2.2 Where personal data already provided has changed, the User shall submit an update application and relevant supporting materials to FMMPAY within thirty (30) calendar days after completion of the change; where failure to update in a timely manner results in service abnormalities or losses, the User shall bear the responsibility.

5.2.3 The User shall cooperate with FMMPAY's information verification requests within fifteen (15) calendar days and provide supplementary supporting materials; where failure to cooperate results in service suspension, the consequences shall be borne by the User.

5.2.4 If the User discovers that personal data stored by FMMPAY is inaccurate, incomplete, or outdated, the User has the right to request correction.

5.2.5 The User has the right to withdraw consent to FMMPAY's data processing at any time; withdrawal of consent may result in certain services being unavailable, and FMMPAY shall clearly inform the User of the relevant impacts before the User performs such operation.

5.2.6 If the User believes that FMMPAY's data processing activities infringe upon the User's privacy rights as defined under the California Consumer Privacy Act (CCPA) or other applicable U.S. privacy laws, the User has the right to submit a complaint to FMMPAY. FMMPAY shall investigate all such complaints and respond within thirty (30) business days of receipt. If FMMPAY denies the User's request or the User is dissatisfied with the handling outcome, the User may have the right to appeal the decision internally. Following the exhaustion of FMMPAY's internal appeals process (or where applicable), the User may have the right to lodge a complaint with the California Privacy Protection Agency (CPPA) or seek other remedies as provided by law.

5.2.7 The User shall ensure that all personal data provided to FMMPAY is true, accurate, and complete, and shall not provide false data or impersonate others; where losses are caused to FMMPAY or third parties due to the provision of false data, the User shall bear compensation liability.

5.2.8 The User shall timely update changed personal data and notify FMMPAY within the agreed time limits and provide supporting materials; losses caused by failure to update in a timely manner shall be borne by the User.

5.2.9 The User shall properly safeguard account login credentials and transaction authorisation information, shall not disclose or lend the account to any third party, and upon discovering account abnormalities, shall promptly take measures such as freezing and notification, and cooperate with FMMPAY in conducting risk investigations.

5.2.10 The User shall cooperate with FMMPAY in carrying out anti-money laundering, sanctions screening, and other compliance work, provide necessary supporting materials, and during the exercise of data subject rights, provide true and valid identity credentials and

cooperate with FMMPAY in completing identity verification.

6. Data Storage

6.1 For the purposes of ensuring data security and compliance, the core storage nodes of Users' personal data are located within the United States, specifically stored on servers of third-party data centres entrusted by FMMPAY that hold certifications recognized under applicable U.S. federal and state laws and comply with ISO/IEC 27001 information security standards. Only where necessary to achieve cross-border service coordination needs shall necessary data be stored cross-border in accordance with this Agreement; except for such circumstances, FMMPAY shall, in principle, not transfer any data for storage outside the United States.

6.2 FMMPAY sets data retention periods in accordance with the principle of "statutory minimum necessity".
Users' basic necessary data and transaction records shall be continuously stored during the account existence period to ensure normal service operation; after account cancellation, such data shall be retained for at least seven (7) years or other legally required periods.
Such retention periods constitute statutory obligations and shall not be affected by the User's withdrawal of consent to data processing.

6.3 Technical data such as login logs, device information, and operation behaviour logs shall be stored for six (6) months calculated from the date of data generation; upon expiry, the system shall automatically execute cleanup procedures and permanently delete such data without backup retention.

6.4 Upon expiry of the retention period, FMMPAY shall classify and process data; data that must be deleted shall be permanently deleted to ensure irrecoverability; data that may be anonymised shall be anonymised using irreversible techniques, and anonymised data may be used for purposes such as business analysis and service optimisation without separately obtaining User consent.

7. Cross-Border Data Transfer

7.1 FMMPAY shall only carry out cross-border data transfer activities where a lawful basis exists, which the User expressly acknowledges and agrees to.

7.2 FMMPAY and its overseas affiliated companies may transfer data based on intra-group service coordination needs.

7.3 Where it is necessary to transfer Users' personal data in response to lawful requirements of regulatory authorities or judicial bodies in U.S. or overseas jurisdictions, FMMPAY shall, to the extent permitted by law, endeavour to notify the User in advance of the content and basis of the transfer, except where notification is prohibited by law.

7.4 Where the User's transactions involve overseas banks or international clearing organisations, FMMPAY shall transfer necessary transaction data to such institutions to complete cross-border fund settlement.

7.5 FMMPAY shall transfer necessary data to overseas cooperating institutions, with the scope of transfer determined according to service type; except for data disclosure or transfer obligations arising from bank, clearing institution, regulatory, or sanctions requirements.

7.6 Where security incidents such as unauthorized access, loss, or misuse occur in cross-border data transfers, FFMPAY shall immediately terminate the transmission channel with the relevant recipient and notify the affected User within a reasonable time, generally not to exceed seventy-two (72) hours, upon confirmation of the incident. Based on the severity of the incident, FMMPAY shall comply with all applicable breach notification obligations under relevant U.S. federal and state laws, including but not limited to reporting to supervisory authorities where required, cooperating with regulatory investigations, tracking incident handling progress, and timely providing affected Users with follow-up information as legally required or as necessary to mitigate harm.

7.7 Where the User believes that cross-border transfer poses risks, the User may apply to FMMPAY to terminate such transfer, and FMMPAY shall terminate the relevant transfer within three (3) working days after review.
The User expressly acknowledges and accepts that termination of such data transfer shall result in termination of all related services.

7.8 The User shall cooperate with FMMPAY in conducting pre-transfer risk assessments for cross-border transfers and provide necessary supporting materials; where compliance risks arise due to false data provided by the User, the User shall bear corresponding responsibility.

8. Liability and Compensation

8.1 Where FMMPAY fails to collect, use, or transfer data in accordance with this Agreement, resulting in data leakage, misuse, or damage to the User’s personal dignity, FMMPAY shall compensate the User for direct economic losses. Direct economic losses include but are not limited to: losses of account funds due to data leakage, reasonable expenses incurred by the User for rights protection such as legal fees, litigation fees, appraisal fees; for indirect losses such as the User's loss of goodwill, loss of expected income, FMMPAY shall not bear compensation liability, unless such indirect losses are caused by FMMPAY's intentional conduct or gross negligence.

8.2 Where FMMPAY fails to perform its security safeguard obligations, resulting in theft, tampering, or loss of User data, FMMPAY shall compensate the User for all direct losses thereby incurred and take measures to restore the data.

8.3 Where the User provides false data, impersonates others, or fails to update data in a timely manner, resulting in regulatory penalties imposed on FMMPAY such as fines, business restrictions, third-party claims such as infringement claims by the subject whose information was impersonated, or reputational damage such as user attrition due to negative media coverage, the User shall compensate FMMPAY for all losses. The scope of losses includes: the amount of regulatory fines, principal and interest of third-party claims, reasonable expenses incurred by FMMPAY for reputation repair such as public relations fees, announcement fees; the amount of compensation shall be calculated based on FMMPAY's actual expenditure vouchers such as penalty notices, compensation agreements, invoices, and FMMPAY shall provide copies of such vouchers to the User.

8.4 Where the User discloses account login credentials, lends the account, or fails to take security protection measures, resulting in account misuse or data leakage and causing losses to FMMPAY, the User shall fully compensate FMMPAY for such losses.

9. Dispute Resolution

9.1 The formation, effectiveness, interpretation, performance, and dispute resolution of this Agreement shall be governed by the laws of the jurisdiction corresponding to the service provider entity selected by the User; where the User has not expressly selected, the laws of the jurisdiction of the entity actually providing the services shall apply.

9.2 Any dispute arising from or in connection with this Agreement shall first be resolved through friendly consultation (the consultation period shall be 30 calendar days, calculated

from the date on which one party sends a consultation notice); where consultation fails, either party shall have the right to choose one of the following methods for resolution: (1) bring an action before a court of competent jurisdiction at the location of the service provider entity; (2) submit the dispute to the jurisdiction of and venue in state and federal courts located in Wilmington, Delaware for arbitration in accordance with the arbitration rules in effect at the time of application for arbitration, with the place of arbitration being United States, and the arbitral award shall be final and binding on both parties. The specific method may be specified in a supplemental agreement; if not expressly agreed, method (1) shall apply by default.

9.3 During consultation or arbitration, except for matters in dispute, both parties shall continue to perform other obligations under this Agreement and shall not suspend or terminate other obligations due to the dispute.

10. Termination of the Agreement

10.1 Where the User voluntarily cancels the account and there are no outstanding transactions, fees, or disputes, this Agreement shall terminate upon completion of account cancellation, where the User has serious breaches of this Agreement (including but not limited to: providing false data 3 or more times cumulatively, impersonating others to conduct transactions, lending accounts resulting in money laundering/sanctions compliance risks, failure to cooperate with anti-money laundering screening resulting in notification by regulatory authorities), FMMPAY shall send written notice through the User's reserved contact methods (SMS, email, written correspondence), specifying the breach circumstances and the time of agreement termination (15 calendar days after the notice is sent), and this Agreement shall terminate upon expiry of the period.

10.2 Where FMMPAY is unable to continue providing services due to business adjustments or cancellation of qualifications, FMMPAY may terminate this Agreement after providing thirty (30) days' prior notice to the User; where long-term inability to perform arises due to force majeure, this Agreement may be terminated upon mutual consultation.

10.3 After termination of this Agreement, FMMPAY shall cease collecting new personal data of the User, and personal data already collected shall be retained in accordance with the storage periods stipulated in this Agreement and shall be deleted or anonymised upon expiry.

10.4 After termination of this Agreement, provisions relating to confidentiality obligations, compensation liability, and dispute resolution shall continue to be effective until the relevant obligations have been fully performed or the statutory limitation period has expired.