CaaS Master Agreement

SquareFi · Last updated 2026-11-15

(together with its Exhibits and any Commercial Offer, the "Agreement")

Effective Date: the date on which the Client executes a Commercial Offer that incorporates this MSA (the "Effective Date").

This Cards-as-a-Service Master Agreement (this “MSA”) is made and entered into by and between the entity named as the Service Provider in the Commercial Offer, being either (a) BUYEASY TECHNOLOGY CO., LTD, a company having its registered office at 320 Matheson Blvd W, Suite 211, Mississauga, Ontario L5R 0H2, Canada, a Money Services Business registered with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) (registration No. M23877619) and a payment service provider registered with the Bank of Canada under the Retail Payment Activities Act (PSP entity ID RPS0014827), or (b) MOSTA PAYMENTS LTD., a company having its registered office at 320 Matheson Blvd W, Suite 211, Mississauga, Ontario L5R 0H2, Canada, a Money Services Business registered with FINTRAC (registration No. N300001741) and a payment service provider registered with the Bank of Canada under the Retail Payment Activities Act (PSP entity ID RPS0016067), in each case contracting for and on behalf of itself and its Affiliates (the “Service Provider”), and the client identified on the Commercial Offer (the “Client”). The Service Provider and the Client are referred to individually as a “Party” and collectively as the “Parties”.

The Service Provider is a card-payment distributor and program manager and a facilitator of virtual-currency exchange services that enable payment transactions to be funded from fiat currency and/or virtual currencies. The Service Provider relies on regulated financial partners that provide the underlying financial services (including card issuance and the safeguarding and settlement of funds) with which the Service Provider interfaces to provide the Services.

The Client wishes to rely on the Services provided by the Service Provider in order to offer to its customers self-branded payment cards and related payment services funded from fiat currency and/or their own virtual currencies.

In consideration of the mutual covenants set out below, and intending to be legally bound, the Parties agree as follows.

1. Definitions

For the purposes of this MSA, capitalised terms have the meanings set out below. Terms used in the singular include the plural and vice versa, depending on the context. Capitalised terms used but not defined in this MSA have the meaning given in the Commercial Offer.

- “Affiliate” any entity that controls, is controlled by, or is under common control with a Party at the effective date of an Commercial Offer, provided that such control remains effective during the Agreement Term; “control” means the direct or indirect holding of more than 50% of the voting rights of an entity.
- “Agreement” this MSA together with an Commercial Offer relating thereto agreed upon by the Parties from time to time, including all Exhibits.
- “Agreement Term” has the meaning given in Article 4.
- “All Required Information” the information and documents required of the Client as set out in the applicable Commercial Offer, which are required for the Card Program to go live.
- “AML Laws” all applicable anti-money-laundering, counter-terrorist-financing, sanctions and proceeds-of-crime laws and regulations, including, in Canada, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and FINTRAC guidance, and any equivalent laws applicable to a Party or to a Financial Partner.
- “API” any application programming interface made available by the Service Provider for access to and use of the Payment Solution.
- “Applicable Law” any law, statute, regulation, rule, regulatory guidance, order, ordinance, network operating rule, or binding decision of any judicial, legislative, regulatory or governmental authority having jurisdiction over a Party or a Financial Partner that applies to the performance, receipt or use of the Services.
- “Authorized User” an individual designated by the Client (directly or through a Business Administrator) who is permitted to be issued and to use a Card, or to access the Back-Office, in each case under the Client’s authority and responsibility.

• “Back-Office” the web-based application made available by the Service Provider to the Client to manage access to and use of the Payment Solution, including for the provision of Level 1 Support.

• “Brand” any trademark (registered or unregistered), trade name, logo or other graphical element of the Client.

• “Business Administrator” the individual designated by the Client to administer the Card Program on the Client’s behalf, including the designation of Authorized Users.

• “Card” a physical or virtual payment card issued by a Financial Partner for use by a Cardholder; delivered without the branding of the issuer or the Service Provider by default, with the Client’s Brand applied only where the White-Label custom-branding add-on is elected in the Commercial Offer, and in all cases bearing the Card-network and digital-wallet marks required by the applicable scheme rules.

• “Card Account” the prepaid ledger account associated with one or more Cards, fundable from fiat currency and/or from supported virtual currencies (Crypto Top-Up), with the funding methods available depending on the Card Program and the relevant Financial Partner.

• “Cardholder” an individual or entity that is a customer or Authorized User of the Client and that agrees to use or receive Payment Services in connection with a Card.

• “Cardholder Terms of Service” the terms and conditions governing the issuance and use of a Card by a Cardholder, as approved or required by the Service Provider and/or the relevant Financial Partner.

• “Chargeback” any reversal, refund, reclamation, dispute or other debit initiated by a Cardholder, a Cardholder’s financial institution, a payment network or a similar entity.

• “Client Data” all data or information provided, uploaded or submitted by the Client or its Users to the Payment Solution in the course of using the Services, other than KYC Elements and KYC Supplements.

• “Confidential Information” non-public technical, financial, commercial or other sensitive information of a Party (including the Platform, the API, the Back-Office, the Payment Solution and the Documentation), disclosed to the other Party before or during the performance of the Agreement.

• “Crypto Top-Up” the funding of a Card Account using supported virtual currencies (including USDT and USDC on supported networks such as Polygon, Ethereum/ERC-20, Tron/TRC-20 and Solana), converted into the settlement currency, with blockchain settlement (gas) sponsored by the Service Provider unless otherwise stated in the Commercial Offer.

• “Designated Account” the account designated by the Service Provider and held with a Financial Partner on a for-benefit-of (FBO) basis into which the Client funds amounts used to fund Card Accounts and to settle amounts due under the Agreement.

• “Documentation” user information, feature descriptions of the API, and any other document relating to the use of the Payment Solution generally made available by the Service Provider under the Agreement.

• “Fees” the fees and charges set out in the applicable Commercial Offer.

• “Financial Partner” any third-party partner of the Service Provider or of an Affiliate of the Service Provider that provides Financial Services, including any issuing bank, BIN sponsor, processor, custodian or safeguarding institution.

• “Financial Services” any regulated services relating to the issuance of Cards, the safeguarding and settlement of funds, and the provision of Payment Services.

• “Fraud Recall” a request, instruction, return, reclamation, Chargeback, or other debit received from a payment network, card scheme, financial institution, or other counterparty in respect of a transaction posted to or attempted on a Card Account, where that request is identified, coded, or described as fraud, unauthorized use, or a comparable fraud reason. A notice given by the Cardholder that a transaction on the Cardholder’s own Card Account was unauthorized or fraudulent is not a Fraud Recall. A later message that only continues, updates, or responds to the same Fraud Recall (including a representment, pre-arbitration, or status update) is not a separate Fraud Recall.

• “Fraud Recall Fee” USD 500 per Fraud Recall, unless the Commercial Offer states a different amount.

• “GDPR” Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), where applicable to processing under the Agreement.

• “Go-Live Date” the date of the Go-Live Notice.

• “Go-Live Notice” a document signed by the Parties confirming that (i) all approvals required by the Service Provider (from its Financial Partners or otherwise) for the Card Program are in place, and (ii) the Platform and the Client’s integration of the Payment Solution have been tested and are ready for commercial use.

• “Infrastructure Partner” SquareFi Inc., the company that develops and licenses to the Service Provider the software used for the Platform.

• “Key” an individual API key (or any replacement) delivered by the Service Provider to the Client for use of the API under the Agreement.

• “KYC Elements” documents and information relating to a prospective Cardholder or Authorized User that the Client must transmit to the Service Provider to allow the Service Provider and its Financial Partners to comply with Applicable Law and AML Laws.

• “KYC Supplements” additional documents and information relating to a prospective or existing Cardholder or Authorized User that the Client must transmit to the Service Provider to allow the Service Provider and its Financial Partners to comply with Applicable Law and AML Laws.

• “Level 1 Support” the assistance and support services to be provided by the Client to Cardholders with respect to Cards and Payment Services, as set out in the Commercial Offer.

• “Commercial Offer” the document(s) issued by the Service Provider and executed by the Parties specifying the Services subscribed by the Client, the duration of the subscription, the Price, and any other specific terms mutually agreed upon by the Parties.

• “Payment Services” the payment services available to a Cardholder in respect of a Card, subject to the Cardholder Terms of Service, provided by the Service Provider and/or its Financial Partners.

• “Payment Solution” the proprietary software application of the Service Provider in object-code form described in the Commercial Offer, accessible through the API and from the Back-Office for the delivery of Payment Services, including any related Documentation and any updates, revisions, modifications, fixes, additions and enhancements provided through Support.

• “Personal Data” has the meaning given in Article 11.

• “Platform” the platform used to host and deliver the Payment Solution to the Client.

• “Price” the Fees payable by the Client to the Service Provider under an Agreement.

• “Prohibited Activities” the businesses, activities, merchant categories and jurisdictions set out in Exhibit 2, which the Client and the Cardholders may not engage in through the Services.

• “Reserve” an amount that the Service Provider may, acting reasonably, require the Client to maintain or that the Service Provider may hold back to secure Chargebacks, fraud losses, fees, indemnity obligations, network fines or other amounts that may become due under the Agreement.

• “Service Level Agreement” the service levels and support policy set out in Exhibit 1.

• “Services” the services provided by the Service Provider relating to the Card Program, the Payment Solution and the supply of Cards, as set forth in an Commercial Offer, including any of the service components described in Article 6.

• “Support” the standard support services in relation to the Payment Solution provided by the Service Provider to the Client in accordance with the Service Level Agreement.

• “Territory” the country or region specified in the Commercial Offer in which the Client is authorised to offer Cards and to access and use the Payment Solution.

• “Third-Party Approvals” the approvals of the third parties listed in the Commercial Offer that are required for the Card Program to go live, as evidenced by the Go-Live Notice.

• “User” (i) any employee, agent or contractor of the Client authorised to embed the API into the Client’s systems or to access the Back-Office for the provision of Level 1 Support, and (ii) any Cardholder or Authorized User accessing the Payment Solution through use of a Card.

• “White-Label” card issuing and program management delivered without the issuer’s or the Service Provider’s branding on the Card or in the associated interface by default; custom branding may be provided as a paid add-on as set out in the Commercial Offer.

• “xPays” third-party services used to host and tokenize Cards (for example, Apple Pay and Google Pay), into which the Client may elect to make its Cards eligible, on the conditions set out in an Commercial Offer.

2. Purpose

The purpose of this MSA is to define the conditions that govern any Commercial Offer placed by the Client for the purchase of Services. The Services are distributed by the Service Provider as a technology and program-management provider; the underlying Financial Services are provided by the relevant Financial Partners. The Service Provider does not itself act as the issuer of the Cards and, except to the extent of its own MSB and PSP authorisations, does not act as a bank or deposit-taking institution.

3. Ordering

This MSA does not constitute a commitment to order. Any subscription to the Services requires the prior execution of an Commercial Offer by the Client, which is governed by and incorporates this MSA to form the Agreement. Each Commercial Offer is separate and independent from any other Commercial Offer.

As the Client enters into this MSA in its own name and on behalf of its Affiliates, each Affiliate of the Client is authorised to place an order under this MSA through an Commercial Offer. The Client is responsible for communicating this MSA to its Affiliates. By executing an Commercial Offer, the Client's Affiliate agrees to be bound by this MSA, which applies mutatis mutandis to the Affiliate as if it were the Client. The Client and the Affiliate executing the Commercial Offer are jointly and severally liable to the Service Provider for compliance with the Agreement.

Each Commercial Offer, and the commencement of the Services thereunder, is subject to the Third-Party Approvals and to the satisfactory completion of the Service Provider's and the relevant Financial Partner's onboarding, due-diligence and compliance requirements in respect of the Client.

Infrastructure Partner. The Service Provider issues and signs each Commercial Offer and administers onboarding, KYC/KYB and the regulated financial services. SquareFi Inc. develops and licenses the software used for the Platform. It is not a party to this Agreement or to any Commercial Offer. The Service Provider remains the Client's counterparty under the Agreement and the party responsible for the regulated financial services. The Service Provider may engage Financial Partners and other third parties to provide the Services and is not required to disclose them, save as required by Applicable Law.

4. Term

This MSA is not signed separately. It becomes effective on the Effective Date — the date on which the Client executes a Commercial Offer that incorporates this MSA — and expires one (1) year after the expiry or termination of the last Commercial Offer in force (the "MSA Term"), unless terminated earlier in accordance with Article 18.

Subject to the Third-Party Approvals, each Commercial Offer enters into force and remains in force for the duration specified in it (the "Initial Subscription Term"). Unless the Commercial Offer provides otherwise, upon expiry of the Initial Subscription Term the Commercial Offer renews automatically for successive periods of one (1) year each (each an "Additional Subscription Term") unless either Party gives at least sixty (60) days' prior written notice of

non-renewal. The Initial Subscription Term together with any Additional Subscription Term constitute the "Agreement Term". Termination of one Commercial Offer does not automatically terminate this MSA or any other Commercial Offer.

5. Financial Conditions

5.1 Price and funding

The Price due by the Client to the Service Provider, including its breakdown, is set out in the Commercial Offer, and is exclusive of any applicable tax. Unless otherwise stated in the Commercial Offer, the Price is structured as the greater of (i) the applicable platform minimum and (ii) the usage-based fees for the relevant month, plus any setup fee and any pass-through costs. Unless otherwise agreed in writing, all amounts are payable in United States dollars (USD). The Service Provider issues the invoices, as set out in Article 5.2.

The Client shall at all times maintain sufficient cleared funds in the Designated Account to fund Card Accounts and to meet amounts due under the Agreement. The Card Program operates on a pre-funded basis: the aggregate daily purchase limit available across the Card Program shall not exceed the cleared cash balance in the Designated Account (excluding any Reserve). If purchases would exceed the available balance on any day, the Service Provider may freeze Cards or decline or reverse transactions at its reasonable discretion.

The Service Provider may pass through, without margin, network, scheme, blockchain-settlement, Financial Partner and other third-party costs. The Service Provider will give thirty (30) days' notice of changes to its own rates; fluctuations in pass-through third-party costs may be applied without prior notice. Except as otherwise agreed, the Price is non-refundable and is not subject to deduction or set-off by the Client.

Subject to Applicable Law, the Client (and the Client alone, not the Service Provider, any Financial Partner or any KYC service provider) is free to set the fees and charges payable by its Cardholders.

5.2 Payment terms

The Services are supplied on a post-payment basis. The Service Provider issues all invoices. The Service Provider shall issue an invoice for any setup fee within five (5) business days after the Client executes the Commercial Offer. Recurring and usage-based Fees are invoiced monthly in arrears for amounts accrued during the preceding month.

Unless otherwise stated in the Commercial Offer, invoices are payable within thirty (30) days of the invoice date, and the Service Provider may debit amounts due (including Fees, Chargebacks, fraud losses and network fines) from the Designated Account or any Reserve, with reasonable re-attempts, set-offs and nettings. Commencement of and access to the Services are not conditional on payment in advance.

Overdue amounts accrue interest, from the day following the due date until payment in full, at a rate of 1.5% per month (or the highest rate permitted by Applicable Law). If the Client fails to pay undisputed amounts more than thirty (30) calendar days after the due date, the Service Provider may, after written notice, suspend the Services and, if the default continues for a further fifteen (15) days, terminate the Agreement, without prejudice to any other remedy. The Client must notify the Service Provider in writing of any good-faith dispute over an invoice within ten (10) business days of the invoice date; undisputed amounts remain payable.

5.3 Fraud Recall Fee

The Client shall pay the Fraud Recall Fee for each Fraud Recall received on a Card Account in the Client's program. The Fraud Recall Fee is incurred when the Service Provider or a Financial Partner receives the Fraud Recall, and is payable whether the Fraud Recall is later accepted, rejected, withdrawn, reversed, represented, or otherwise resolved. The Fraud Recall Fee is not refunded, credited, or reduced by reason of that outcome.

The Fraud Recall Fee is in addition to, and not in substitution for, the principal amount of the underlying transaction. If that principal is debited, refunded, or otherwise passed through, the Client remains liable for it as well as for the Fraud Recall Fee. The Service Provider may debit the Fraud Recall Fee from the Designated Account or any Reserve in accordance with Article 5.2.

Unless the Commercial Offer states a different Fraud Recall Fee, the amount is USD 500 per Fraud Recall. A Commercial Offer may vary the amount. It may not provide that the fee is conditional on the outcome of the Fraud Recall.

6. Scope of the Services

6.1 Services

The scope of Services is defined in the Commercial Offer. Unless an Commercial Offer provides otherwise, the Service Provider does not at any time take possession of virtual currency stored in a Cardholder wallet or transacted through Cards, other than in the course of Crypto Top-Up conversion performed under the Service Provider's MSB authorisation. The Payment Solution comprises software-related services and an end-to-end solution for facilitating the communication, processing and settlement of payment transactions and related Financial Services.

Depending on the Commercial Offer, the Services may include any of the following components:

- Virtual card issuance, including instant issuance;
- Physical card issuance, including design customisation and shipping;
- Fiat Top-Up of Card Accounts using supported fiat-currency funding methods (such as bank transfer or card funding), with the availability and supported methods depending on the Card Program and the relevant Financial Partner;
- Crypto Top-Up of Card Accounts using supported virtual currencies (such as USDT and USDC on supported networks), with conversion into the settlement currency and sponsored blockchain settlement;
- Corporate Spend programs, under which Cards are issued for corporate purchases by the Client's designated Authorized Users (and not consumer-facing cards) unless otherwise agreed;
- Tokenization and mobile-wallet provisioning through xPays (such as Apple Pay and Google Pay);
- 3D Secure authentication, available in a generic mode (included with standard Cards) or a fully custom mode (paid add-on);
- ATM services (balance inquiry and, subject to the Service Provider's approval, cash withdrawal);
- Dispute and Chargeback processing (per-case fee), and the Fraud Recall Fee under Article 5.3;
- KYC and KYB services, managed by the Service Provider (per-customer fee), it being understood that the Client may perform KYC itself provided it meets the standards required under AML Laws;
- White-Label program delivery, with optional custom branding as a paid add-on.

Card Accounts may be funded (topped up) in fiat currency and/or in supported virtual currencies. The funding methods available for a given Card Program, including whether fiat funding, Crypto Top-Up, or both are enabled, depend on the Commercial Offer and on the capabilities and approval of the relevant Financial Partner.

The Service Provider undertakes to provide the Services, directly and/or indirectly through its Financial Partners where applicable, in accordance with the Service Level Agreement. The Client shall provide all information reasonably requested by the Service Provider to enable the Service Provider to provide the Services in accordance with Applicable Law and the Cardholder Terms of Service.

The Service Provider reserves the right, at any time, to add, remove or replace any Financial Partner or other service provider, provided that the Service Provider gives the Client reasonable notice where the change is material and ensures continuity of the Services to the extent commercially practicable. Such a change does not require the Client's consent.

6.2 Remote provision of the Services

Unless the Commercial Offer states otherwise, the Services are supplied remotely. The Client shall integrate with the Service Provider's API as necessary for the performance of the Services and is responsible for taking appropriate safeguards for its IT systems and data. The Service Provider disclaims liability for loss or destruction of the Client's data during performance of the Services, except to the extent caused by the Service Provider's wilful misconduct or gross negligence.

6.3 Service Provider staff

The Service Provider undertakes to perform the Services diligently and professionally and to assign qualified personnel. The Service Provider retains the sole and exclusive right to control the manner, means and methods by which the Services are performed, including the personnel assigned. The Service Provider's personnel remain under the Service Provider's sole authority as their exclusive employer.

7. Card Ordering and Delivery of Payment Services to Users

7.1 Card ordering and Cardholder relationship

The Client is responsible to the Service Provider for any ordering of Cards under the Agreement on behalf of Cardholders and Authorized Users. Unless the Commercial Offer provides otherwise, the Service Provider will arrange, on behalf of the Client and through its Financial Partners, the delivery of Cards to the Cardholder addresses provided by the Client. The Client shall:

- collect and/or provide to the Service Provider the KYC Elements relating to prospective Cardholders and Authorized Users, and any KYC Supplements relating to existing Cardholders and Authorized Users;
- have prospective Cardholders agree to the Cardholder Terms of Service, having informed them that such acceptance is a necessary condition for the provision of the Card and the related Payment Services;
- inform the Service Provider, no later than seven (7) business days after receipt, of any request by a Cardholder to exercise a right of withdrawal under the Cardholder Terms of Service;
- send Cardholders any updates to the Cardholder Terms of Service in accordance with the conditions and deadlines set by the Service Provider;
- provide regular reports to the Service Provider on Card Accounts and Cards that have been closed or de-linked;
- provide Level 1 Support to Cardholders.

7.2 Payment Services to Cardholders

The Client is responsible for the services it provides to Cardholders, including Level 1 Support, other than the Payment Services. Subject to the Client's compliance with the Agreement, the Service Provider and its Financial Partners are responsible to the Cardholder for the Payment Services in accordance with the Cardholder Terms of Service. The Client undertakes to:

- embed the API in accordance with the Documentation, the Agreement and Applicable Law;
- not modify the API or any component of the Services;
- not circumvent or interfere with any security measures implemented in respect of the Payment Solution;
- without undue delay, implement any change requested by the Service Provider to remedy a security vulnerability or to comply with Applicable Law or network rules;

• implement and maintain appropriate administrative, physical and technical safeguards, in accordance with best industry standards, to ensure the security, confidentiality and integrity of Card Accounts, Cards and Cardholder data.

Where a Cardholder disputes or reports as fraudulent a transaction authorised through use of a Card, the Client shall be responsible for the full refund of the relevant amount to the Cardholder, and shall indemnify the Service Provider and/or the Cardholder for any resulting losses, where the dispute or fraud arises from a breach by the Client of its obligations to secure Card Accounts, Cards or Cardholder data. The Client's indemnity does not arise to the extent the loss results from the Cardholder's own fraudulent or negligent act or omission not contributed to by a breach by the Client.

7.3 Compliance, KYC/KYB and AML

Compliance with AML Laws is a fundamental condition of the Agreement. The Client shall collect and verify all identity and verification information required for each Cardholder and Authorized User, perform preliminary risk scoring and sanctions screening, and deliver the complete KYC/KYB dossier to the Service Provider as required by the Service Provider and the relevant Financial Partner. The Service Provider and its Financial Partners do not rely on the Client's KYC as a substitute for their own obligations and will perform final identity verification and onboarding; no nested reliance on a third party's KYC is permitted.

Where the Client performs KYC/KYB or transaction monitoring in respect of its Cardholders and Authorized Users, it does so as agent of the Service Provider and to the Service Provider's and the Financial Partners' standards. The Service Provider may, at any time and at the Client's cost, revoke that agency and assume those functions if it reasonably determines that the Client has failed, or is likely to fail, to perform them in accordance with Applicable Law. The Client and the Cardholders shall not engage in any Prohibited Activities. The Service Provider may suspend the Services immediately where it reasonably suspects a breach of AML Laws, sanctions, network rules or the Prohibited Activities, or where directed by a Financial Partner, regulator or payment network.

8. Payment Solution

8.1 Licence grant

In consideration of the Client's compliance with the Agreement, the Service Provider grants the Client and its Affiliates a personal, non-exclusive, non-transferable and non-sublicensable licence, for the Territory, allowing (i) the Client's Users to embed the API and to access the Payment Solution through the Back-Office to provide Level 1 Support, and (ii) the Client to provide products and services to Cardholders through the Cards. No Cardholder may access the Back-Office. All rights not expressly granted are reserved by the Service Provider.

8.2 Licence restrictions

The Client shall use the Payment Solution only as expressly permitted by the Agreement and the Documentation. The Client shall not, and shall ensure that its Users do not: (i) copy, make available or distribute the API, the Back-Office or the Payment Solution to third parties other than authorised Users; (ii) access or use the Payment Solution beyond any metric in the Commercial Offer or outside the Territory without an additional Commercial Offer and payment of the agreed Fees; (iii) assign, sell, rent, lend, sublicense, distribute, outsource or transfer the rights granted; (iv) adapt, modify or translate the API or Payment Solution; (v) disassemble, decompile, reverse engineer or attempt to reconstruct the source code, except as permitted by Applicable Law; (vi) alter or remove any proprietary notices of the Service Provider; (vii) distribute any software (other than the Client's own application) created using the API, the Back-Office or the Payment Solution; or (viii) use the Payment Solution for benchmarking or disclose performance-testing results to third parties.

Use of the API and Back-Office may be subject to the rate limits set out in the Commercial Offer. The Client shall not make grossly unreasonable or excessive use of the Payment Solution and shall promptly inform the Service Provider in writing of any usage beyond the applicable rate limit, paying the applicable excess-usage Fees.

8.3 Access and credentials

Use of the Payment Solution requires an internet connection and prior registration to obtain a Key and Back-Office credentials. The Client must keep the Key and credentials confidential and is responsible for all access to and use of the API and the Back-Office by its Users. Cardholders may access the Payment Solution only indirectly, through use of their Cards. Use of the Payment Solution requires in-depth technical knowledge of software integration, and the Client is responsible for the configuration of its systems in accordance with the Documentation.

9. Ownership

The Service Provider and its licensors retain all title and ownership (including all intellectual-property rights) in and to the Services, including the Payment Solution, the Platform, the Back-Office, the API, the Documentation, and any enhancements or derivative works. The Agreement does not transfer any ownership to the Client, and the Service Provider reserves all rights not expressly granted. The Client shall not directly or indirectly challenge the Service Provider's title to the Services. Any material, intentional or repeated misuse of the Services constitutes a serious breach entitling the Service Provider to suspend (on not less than ten (10) days' notice) or terminate (on a further ten (10) days' notice) the Agreement.

The Client is and remains the sole owner of the Client Data. The Client grants the Service Provider a worldwide, revocable licence, for the Agreement Term, to host, store and process the Client Data in order to perform the Agreement, including to analyse, optimise and improve the Services and to develop new services, but excluding any sale or lease of Client Data to third parties.

The Client grants the Service Provider a worldwide licence, sublicensable to the Financial Partners and other third parties responsible for the production and issuance of Cards, for the Agreement Term, to use the Brand solely for the production, design, distribution and operation of the Cards. The Service Provider will comply, and will procure that such third parties comply, with the Client's written branding guidelines. The Client warrants that it has all rights necessary to grant these licences. Each Party retains ownership of its own pre-existing intellectual property and brand. The Service Provider owns any general-purpose improvements to the Services; outputs that are unique and bespoke to the Client's Brand and paid for as custom work belong to the Client.

10. Warranties, Service Levels and IP Indemnity

The Client acknowledges that, except as expressly stated in the Agreement, the Services are provided "as is" and "as available", without warranty from the Service Provider or its Financial Partners. The Service Provider disclaims all implied warranties, including merchantability, fitness for a particular purpose, title and non-infringement, and does not warrant that the Payment Solution will be error-free or uninterrupted. Service availability is addressed in the Service Level Agreement. The Client is solely responsible for implementing appropriate measures to mitigate the consequences of any interruption or data loss.

The Client warrants that the Client Data does not (i) infringe the rights of any third party, (ii) contain unlawful or offensive content, (iii) contain malicious code, or (iv) constitute unlawful processing of Personal Data, and shall defend and indemnify the Service Provider against any third-party claim arising from the Service Provider's use of the Client Data in accordance with the Agreement, subject to the procedure below.

The Service Provider warrants, on a continuing basis during the Agreement Term, that the API, the Back-Office, the Payment Solution and the Platform do not infringe the intellectual-property rights of any third party, and shall defend and indemnify the Client against third-party claims of such infringement, subject to the following: (a) the Client gives the Service Provider prompt written notice and sole control of the defence and settlement, and provides reasonable assistance at the Service Provider's expense; (b) the Service Provider may, at its option and expense, procure the right to continue use, modify the item to make it non-infringing, or, failing that, terminate the affected rights; and (c) the Service Provider has no liability for any claim based on the Client's modification of the Services, their combination with items not supplied by the Service Provider, third-party or open-source code, or specifications provided by the Client. This Article states each Party's entire liability and exclusive remedy for intellectual-property infringement relating to the Services.

11. Personal Data

Each Party shall process personal data (the "Personal Data") of Cardholders, Authorized Users, and the representatives or employees of the other Party in accordance with applicable data-protection laws, including, in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial legislation, and, where applicable, the GDPR. In respect of its own processing operations necessary to perform the Agreement, each Party acts as an independent controller and warrants that it will comply with the obligations arising under those laws.

Where the Service Provider processes Personal Data on the Client's behalf to operate the Services, the Service Provider acts as the Client's processor; where the Service Provider processes Personal Data to discharge its own regulatory obligations (including KYC, KYB and AML record-keeping), the Service Provider acts as an independent controller. Personal Data is collected for the purpose of performing the Agreement and complying with Applicable Law, and may be shared with Affiliates, Financial Partners and other third parties to that end. Each

Party shall promptly inform the other of any data-subject request that requires the other's cooperation. Each Party shall implement appropriate technical and organisational security measures and shall comply with its obligations regarding sub-processing, international transfers, breach notification and assistance in accordance with applicable data-protection laws.

12. Confidentiality

Each Party shall keep the other Party's Confidential Information strictly confidential, shall not disclose it to third parties (other than to its representatives, agents and advisers on a need-to-know basis and under equivalent confidentiality obligations), and shall not use it for any purpose other than performing the Agreement. These obligations do not apply to information that the receiving Party can demonstrate is or becomes public without its breach, was lawfully obtained from a third party without restriction, was independently developed, or was disclosed with the disclosing Party's prior written consent.

If the receiving Party is required by law or regulatory authority to disclose Confidential Information, it shall, where legally permissible, give the disclosing Party prior notice and reasonable cooperation to seek protective measures. The confidentiality obligations remain in force during the Agreement Term and for so long thereafter as the information remains protected as a trade secret, and in any event for not less than three (3) years after termination. Upon termination, each Party shall, at the disclosing Party's request, return or destroy the other Party's Confidential Information, subject to retention required by Applicable Law or routine backup.

13. Audit

During the Agreement Term and for two (2) years thereafter, the Service Provider may verify the Client's access to and use of the Services no more than once per year, unless there are reasonable grounds or an audit is required by a regulatory authority or Financial Partner with jurisdiction over the Service Provider or its Financial Partners. The Client shall provide, within twenty-one (21) calendar days of a request (or as otherwise required by the regulatory authority), such documents and information as the Service Provider reasonably requires to verify compliance with the Agreement and Applicable Law. If an audit reveals material non-compliance, the Client shall remedy it as soon

as practicable and reimburse the reasonable third-party audit costs (on production of evidence). Where the audit is required by a regulatory authority, each Party bears its own costs.

14. Liability

The Client is responsible for ensuring that the Client Data and the equipment it uses to access the Payment Solution are suitably protected, and remains liable to the Service Provider for any breach of the Agreement by its Users. The Service Provider disclaims all liability for the inaccuracy, loss or alteration of Client Data and for any indirect or consequential damage, including loss of revenue, profits, business, goodwill or anticipated savings.

To the fullest extent permitted by the governing law of the Agreement, each Party's aggregate liability under the Agreement is limited to the amounts paid and due by the Client during the twelve (12) months preceding the event giving rise to the claim. This cap does not apply to: (i) the Client's payment obligations, including amounts owing in respect of Chargebacks, fraud losses and network fines attributable to the Client's program; (ii) either Party's breach of Article 12 (Confidentiality); (iii) the Client's breach of Article 8.2 (Licence restrictions) and the second and third paragraphs of Article 9 (Ownership); (iv) a Party's indemnification obligations under the Agreement; (v) breach of data-protection obligations or a data breach caused by a Party; or (vi) a Party's fraud, gross negligence or wilful misconduct. Chargebacks, fraud losses and network fines attributable to the Client's program are economic pass-through obligations of the Client and are not subject to the liability cap.

15. Subcontracting

The Client acknowledges that the Service Provider uses Affiliates, Financial Partners and other third-party providers to provide the Services. Notwithstanding any such delegation, the Service Provider remains liable to the Client for the proper performance of the Services and for any breach of the Agreement by its Affiliates or third-party providers, except to the extent a loss is caused by the Client or arises from a Financial Partner's regulated determination that the Service Provider cannot control.

16. Force Majeure

Except for payment, security and data-protection obligations, neither Party is liable for any failure to perform resulting from an event beyond its reasonable control, including any governmental decision (such as the withdrawal

or suspension of an authorisation), strike, fire, flood, natural disaster, earthquake, act of terrorism, war, epidemic, pandemic, interruption of telecommunications or electricity networks, or act of computer hacking (a “Force Majeure” event). The affected Party shall promptly notify the other, use reasonable efforts to mitigate, and may suspend the affected obligations. If a Force Majeure event continues for more than thirty (30) consecutive days, either Party may terminate the Agreement on notice.

17. Assignment and Change of Control

Either Party may assign or transfer the MSA and any Agreement, without the other Party’s prior consent but with not less than twenty (20) days’ prior written notice, to (i) a company within its group or (ii) a third party in connection with a merger, a transfer of all or substantially all of its assets or business, or a change of control. However, no assignment, transfer or change of control to a direct competitor of the other Party may be made without that Party’s prior written consent. In the event of an assignment, transfer or change of control involving a direct competitor, the other Party may terminate the Agreement without further liability.

18. Termination

18.1 Termination of the MSA

Only the Service Provider and the Client (or their successors or permitted assignees) may terminate this MSA. No Affiliate may terminate this MSA. Either Party may terminate this MSA and/or any Agreement, on written notice, if the other Party becomes insolvent or enters liquidation proceedings, the notice period being the greater of thirty (30) calendar days and the period required under Applicable Law.

18.2 Termination of an Agreement

The Service Provider may terminate the relevant Agreement if the Client breaches a material obligation (including those in Articles 5, 7, 8, 10, 12 and 13), the breach remaining uncured for thirty (30) calendar days after written notice. The Client may terminate the relevant Agreement if the Service Provider breaches a material obligation (including those in Articles 6, 7, 11 and 12), the breach remaining uncured for thirty (30) calendar days after written notice. In addition, the Service Provider may suspend or terminate the Agreement immediately, without a cure period, in the event of the Client’s fraud, illegality, breach of AML Laws or sanctions, engagement in Prohibited

Activities, loss of a required licence, or where directed by a Financial Partner, regulator or payment network. Termination of one Agreement does not automatically terminate other ongoing Agreements.

18.3 Consequences of termination and transition

On termination, the rights granted to the Client cease, the Client shall cease (and cause its Users to cease) all use of the Services, the Client shall pay all accrued Fees and amounts due, and the Service Provider may apply or retain any Reserve and the Designated Account funds to settle outstanding obligations (including the Chargeback and dispute tail). Except where the Service Provider terminates for the Client's cause, the Service Provider will, at the Client's documented cost, provide reasonable transition assistance for up to twelve (12) months, including: orderly Card de-activation and Cardholder notification, settlement of open transactions and Chargebacks during the tail period, return of remaining Card Account balances, export of Client Data in a usable format (such as CSV or via the API), and reasonable cooperation with a successor provider. The Service Provider is not required to transfer its proprietary Platform or to build a competitor migration.

The provisions that by their nature are intended to survive termination (including Articles 5, 9 to 14, 18 and 20) remain in full force and effect.

19. Miscellaneous

Independence. The Parties are independent contractors. Nothing in the Agreement creates a partnership, joint venture, agency, fiduciary or employment relationship between them.

Entire agreement. This MSA (with its Exhibits and any Commercial Offer) constitutes the entire agreement between the Parties on its subject matter and supersedes all prior agreements or statements. No amendment is effective unless made in writing and signed by both Parties. In the event of conflict, the order of precedence is: the Commercial Offer, then this MSA, then the Exhibits, except that the Exhibits prevail on matters they specifically govern. Any terms put forward by the Client in an order document are expressly rejected.

Notices. Notices must be in writing and delivered by hand, recognised courier or email with confirmation of receipt, to the addresses on the MSA or the Commercial Offer. A Party may change its address by notice. Notices of termination or breach must also be sent by courier or registered mail.

Non-waiver. A failure to exercise a right is not a waiver of it. Any waiver must be in writing and signed by an authorised representative of the waiving Party.

Commercial reference. The Client authorises the Service Provider to use the Client's name, trade name, trademark and logo for the purpose of factual reference to the contractual relationship in customer lists and promotional materials, subject to the Client's reasonable branding guidelines.

Severability. If any provision is held invalid or unenforceable, it shall be reformed to the minimum extent necessary, and the remaining provisions remain in full force and effect.

Non-solicitation of personnel. During the Agreement Term and for six (6) months thereafter, the Client shall not solicit for employment any employee of the Service Provider involved in the Services, except through general advertising not specifically directed at such employees.

Evidence and electronic signature. Records collected by the Service Provider relating to access to and use of the Services may be retained as evidence during the Agreement Term and for five (5) years thereafter, and are admissible between the Parties. The Parties agree that execution by electronic signature is valid, binding and enforceable to the same extent as a handwritten signature.

Counterparts. The Agreement may be executed in counterparts, each of which is an original and all of which together constitute one instrument.

20. Governing Law and Dispute Resolution

This MSA and each Agreement, and any dispute or claim arising out of or in connection with them or their subject matter or formation (including non-contractual disputes or claims), are governed by, and construed in accordance with, the laws of the Province of Ontario and the federal laws of Canada applicable therein, without regard to conflict-of-laws rules.

The Parties shall first attempt to resolve any dispute by good-faith discussions between their senior executives within thirty (30) days of written notice of the dispute. Any dispute not so resolved shall be submitted to the exclusive jurisdiction of the courts of the Province of Ontario sitting in Toronto, and the Parties irrevocably attorn to that jurisdiction; provided that either Party may seek urgent injunctive or other equitable relief (including to protect

Confidential Information or intellectual-property rights) from any court of competent jurisdiction. The Parties may instead agree in an Commercial Offer to refer disputes to binding arbitration seated in Toronto, Ontario, conducted in English before a single arbitrator under the ADR Institute of Canada Arbitration Rules.

Acceptance and Incorporation by Reference

This Cards-as-a-Service Master Agreement is a master template made available by the Service Provider and is incorporated by reference into each Commercial Offer. This MSA is not signed separately. By executing a Commercial Offer that references this MSA, the Client (on its own behalf and, where applicable, on behalf of the executing Affiliate) agrees to and is bound by this MSA in the version identified in that Commercial Offer, and execution of the Commercial Offer constitutes execution of the resulting Agreement. The Parties agree that execution by electronic signature is valid, binding and enforceable.

Exhibit 1 — Service Level Agreement and Support Policy

This Service Level Agreement (the “SLA”) sets out the service levels and support procedures for the Services provided by the Service Provider under the Agreement.

Availability

The Service Provider will use commercially reasonable efforts to make the Payment Solution available, measured monthly with all hours weighted equally. Availability is calculated as 100% minus the average of the Error Rates over each 5-minute interval in the month, where “Error Rate” means, for each request type, the number of internal server errors divided by the total number of requests in the interval. Intervals with no Client requests are treated as 0% Error Rate.

The following are excluded from the availability calculation: scheduled maintenance notified at least ten (10) days in advance; actions taken by the Service Provider at the Client's direction; use of the Services contrary to the Agreement; the Client's failure to respond to support requests requiring its participation; failures of electrical, connectivity, network or telecommunications equipment outside the Service Provider's control; the Client's or a third party's equipment or software; modifications not authorised by the Service Provider; suspension or termination of the Client's rights; and Force Majeure events.

If the availability target is missed in a given month, the Client's sole and exclusive remedy is a service credit against a subsequent invoice, calculated on the scale set out in the Commercial Offer. To receive a credit, the Client must notify the Service Provider within one (1) month of the downtime. Service credits are non-refundable and are not payable for any period during which the Client has not paid Fees due. Service credits are the sole remedy for missed availability targets short of a material, sustained breach giving rise to a termination right.

Incident management and response times

Each Party shall report to the other any incident it identifies in the Payment Services as soon as reasonably possible, in particular incidents affecting KYC, AML monitoring and screening, card authorisations, card issuing, or Cardholder support. The Client shall report incidents through the channels indicated in the Commercial Offer. The Service Provider will adapt its response according to incident severity and will provide a root-cause analysis for material incidents. Target response and resolution times by severity are set out in the table below.

Severity	Description	Target response	Target resolution
Critical	Service or card authorisations unavailable; no workaround.	1 hour	4 hours / workaround
High	Major function impaired; partial workaround available.	4 hours	24 hours
Medium	Minor function impaired; limited impact.	1 business day	3 business days
Low	Cosmetic issue or query; no service impact.	2 business days	5 business days

Routine maintenance is performed during off-peak windows with at least forty-eight (48) hours' notice; emergency maintenance may be performed without notice.

Exhibit 2 — Prohibited Businesses and Restricted Activities

The Prohibited Businesses and Restricted Activities are published by the Service Provider in the Prohibited Jurisdictions and Activities Policy, as updated from time to time. The Client and the Cardholders shall not use the Services in connection with any such prohibited activity.

Exhibit 3 — Commercial Offer

The Commercial Offer applicable to the Client is attached as an Appendix to, and forms part of, this Agreement. It is issued and signed by the Service Provider and executed by the Parties, incorporates this MSA by reference, and sets out the Services, Fees and other client-specific particulars. In case of conflict, the order of precedence set out in this MSA applies.