



## SaaS Agreement

This SaaS Agreement ("Agreement") dated as of June 30, 2023 (the "Effective Date") is entered into by and between Spreadly, Inc., a Delaware corporation, with offices located at 300 Morris St STE 400 Durham, NC 27701 ("Provider" or "Supplier" or "Spreadly") and Mastercard International Incorporated, a Delaware corporation, with offices at 2000 Purchase Street, Purchase, New York 10577 ("Mastercard") and constitutes the entire agreement between the parties supersedes any prior and contemporaneous communications with respect to the matters described in this Agreement.

WHEREAS, Provider provides access to its software-as-a-service offerings to its customers;

WHEREAS, Mastercard desires to access certain software-as-a-service offerings described herein, and Provider desires to provide Mastercard access to such offerings, subject to the terms and conditions set forth in this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

**1. Definitions.** This Agreement incorporates and applies the terms set for in Attachment A which forms an integral part.

**2. SaaS Services.** Throughout the Term and at all times in connection with its performance under this Agreement, Provider shall, in accordance with all terms and conditions set forth in this Agreement, provide to Mastercard and its Authorized Users the following services as set forth in this Section 2 (collectively, the "SaaS Services"):

2.1 Access and Use to SaaS Application. Provider hereby grants to Mastercard, exercisable by and through its Authorized Users, a non-exclusive and non-transferable right to:

(a) access and use the software-as-a-service offering described in Exhibit A attached hereto (the "SaaS Application"), including in operation with other software, hardware, systems, networks, and services, for Mastercard's business purposes, including use in connection with Mastercard Data;

(b) generate, print, copy, upload, download, store, and otherwise use all GUI, audio, visual, digital, and other output, displays, and content as may result from any access to or use of the SaaS Application; and

(c) access and use the SaaS Application for all such non-production uses and applications as may be necessary for the effective use of the SaaS Application as permitted hereunder, including for purposes of analysis, development, configuration, integration, testing, training, maintenance, support, and repair, which access and use will be without charge and not included for any purpose in any calculation of Mastercard's use of the SaaS Application;

(d) perform, display, execute, reproduce and distribute and otherwise make available to Authorized Users, any Provider Materials set forth in Exhibit A solely to the extent necessary to access or use the SaaS Services in accordance with the terms and conditions of this Agreement.

2.2 SaaS Support. Provider shall provide the support, maintenance and other services (collectively, "SaaS Support") for the SaaS Application described in Exhibit B attached hereto.

2.3 Use Restrictions. Mastercard shall not: (i) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer, or otherwise make any Provider Materials or any features or functionality of the Provider Materials available to any third party, except as expressly permitted by this Agreement; (ii) use or authorize the use of the SaaS Services, Documentation or other Provider Materials in any manner or for any purpose that is unlawful under applicable Law; (iii) modify, adapt, translate or create derivative works or improvements of the Provider Materials or any portion thereof; (iv) reverse engineer, disassemble, decompile, decode, adapt or otherwise attempt to derive, gain access to or discover the source code of the SaaS Services or the underlying structure, ideas, know-how, algorithms or methodology relevant to the SaaS Services; (v) input, upload, transmit or otherwise provide to or through the SaaS Services



Platform any information or materials that are unlawful or injurious, or contain, transmit or activate any Harmful Code; (vi) attempt to gain unauthorized access to, damage, destroy, disrupt, disable, impair, interfere with or otherwise impede or harm in any manner the SaaS Services; (vii) access or use the SaaS Services in any way that infringes, misappropriates or otherwise violates any intellectual property right, privacy right or other right of any third party, or that violates any applicable Law; or (viii) access or use the SaaS Services for purposes of (a) benchmarking or competitive analysis, (b), developing, producing, marketing, distributing, licensing or selling any product or service that may compete with the SaaS Services or other Provider Materials, or (c) disclosing to Provider's competitors, for any purpose, otherwise non-public information about the Provider Materials. Mastercard shall ensure its Authorized Users' compliance with the terms of this Agreement.

2.4 Mastercard acknowledges and agrees that Provider is not a payment gateway or merchant account provider and Provider does not assume any direct or indirect liability or responsibility for Mastercard's agreements with payment gateways or merchant account providers supported on the SaaS Services. If and only if Provider is required by applicable law, government agency or court order, Mastercard hereby grants Provider authorization to share information with law enforcement about Mastercard, Mastercard's transactions and Mastercard's Provider account, in each case if Provider reasonably suspects that Mastercard's use of the SaaS Services has been for an unauthorized, illegal, or criminal purpose. Further, Provider reserves the right to not store or submit any transaction Mastercard submits if and only if Provider has been advised by a law enforcement agency that such transaction is (i) in violation of applicable Law or (ii) otherwise exposes Provider or other Provider users to harm, including but not limited to, fraud, illegal, and other criminal acts. Except where prohibited by applicable law or court order, Provider agrees to provide prompt notice of any law enforcement request or decision to not store or not submit any transaction under this Section.

2.5 Changes to the SaaS Services. Provider may make any changes to the SaaS Services (including, without limitation, the design, look and feel, functionality, content, material, information and/or services provided via the SaaS Services) that Provider deems necessary or useful to improve the SaaS Services or for any other reason, from time-to-time in Provider's sole discretion, and with such adequate notice to Mastercard as Provider deems necessary; provided, however, that Provider will not make any such changes that will materially adversely affect its features or functionality available to Mastercard during the Term. Such changes may include upgrades, bug fixes, patches and other error corrections and/or new features (collectively, including related Documentation changes, "Updates"). All Updates will be deemed a part of the SaaS Services governed by all the provisions of this Agreement pertaining thereto.

2.6 Provider acknowledges and agrees that the SaaS Services must, on an ongoing basis, comply with certain Mastercard vendor requirements, including but not limited to the areas of information security, operational resiliency, and risk management. Upon Mastercard's request, Provider hereby agrees to meet with Mastercard to mutually agree upon the scope, timing, and duration of a review of the SaaS Services by certain Mastercard divisions in connection with Mastercard's requirements. The obligations set forth in this Section 2.6 are independent of any other obligations in this Agreement.

2.7 Notwithstanding anything to the contrary in this Agreement, nothing in this Agreement shall restrict, limit, or impair the rights or ability of Mastercard from, now or in the future, independently creating, developing, engineering, providing or to otherwise make available a SaaS Application as described in Exhibit A.



**3. SaaS Service Availability.** Provider shall make the SaaS Services available, as described in Exhibit C ("Service Level").

**4. Initial Testing and Acceptance.**

**4.1 Pre-Test Period.** The Parties acknowledge and agree that the SaaS Application requires certain modifications to enable the SaaS Services to perform to Mastercard's standards. Prior to the test period set forth in Section 4.2, the Parties hereby agree that the SaaS Application shall be modified by (and at the expense of) Provider in such ways as may be required by Mastercard, including, but not limited to the areas of information security, operational readiness, and risk management. The Parties agree that Provider shall seek and obtain Mastercard's approval of any such modifications prior to then notifying Mastercard that the SaaS Application is ready for use in a production environment.

**4.2 Test Period.** When Provider notifies Mastercard that the SaaS Application is ready for use in a production environment, Mastercard shall have thirty (30) days from receipt of the notice to test the SaaS Application to determine whether it complies in all material respects with the requirements the Specifications and this Agreement.

**4.3 Acceptance.** Upon completion of Mastercard's testing, Mastercard shall notify Provider of its acceptance ("Acceptance") or, if it has identified any noncompliance with the Specifications or this Agreement, rejection ("Rejection") of the SaaS Application. If Mastercard Rejects the SaaS Application, Mastercard shall provide a written list of items that must be corrected. On receipt of Mastercard's notice, Provider shall promptly commence, at no additional cost or charge to Mastercard, all reasonable efforts to complete, as quickly as possible and in any event within twenty (20) days from receipt of Mastercard's notice (or such other period as may be agreed upon by the parties in writing), such necessary corrections, repairs, and modifications to the SaaS Application to bring them into full compliance with the Specifications or this Agreement.

**4.4 Corrections.** If any corrective measures are required under Section 4.3, upon its completion of all such measures, Provider shall notify Mastercard in writing and the process set forth in Section 4.2 and Section 4.3 shall be repeated; provided that if Mastercard determines that the SaaS Application, as revised, still does not comply in all material respects with the Specifications or this Agreement, Mastercard may, in its sole discretion commencing with the third submission of corrective measures: (i) require the Provider to repeat the correction, repair, and modification process set forth in Section 4.3 at no additional cost or charge to Mastercard; or (ii) immediately terminate this Agreement with no liability, obligation, or penalty to Mastercard by reason of such termination.

**4.5 Right to Terminate.** The parties shall repeat the foregoing procedure until Mastercard Accepts the SaaS Application or elects to terminate this Agreement, as provided in Section 4.4 above. If, exercising its rights under Section 4.4, Mastercard elects to terminate, Provider shall refund to Mastercard all sums previously paid to Provider under this Agreement. All refunds payable under this Section 4.5 shall be paid within ten Business Days of Mastercard's written notice of termination under Section 4.4.

**5. Professional Services.**

**5.1 Professional Services.** Mastercard and Provider may execute a Statement of Work for additional professional services including, but not limited to, training, consulting, advisory, implementation, configuration, customization and/or other technical services (the "Professional Services") that are mutually agreed upon and described in one or more Statements of Work. For the avoidance of doubt, the Professional Services provided to Mastercard in this Section 5 shall



be entirely separate from and in addition to any work performed by Provider in order to obtain and/or maintain Acceptance of the SaaS Application under Section 4.

**5.2 Personnel.** Provider reserves the right to determine which of Provider's personnel or subcontractors will be assigned to perform Professional Services, and to replace or reassign such personnel during the Term.

**5.3 Mastercard Responsibilities.** In connection with Provider's provision of the Professional Services, Mastercard will: (i) reasonably cooperate with Provider in all matters relating to the performance of the Professional Services; (ii) respond promptly to Provider's requests to provide direction, information, approvals, authorizations or decisions that are reasonably necessary for Provider to perform the Professional Services in accordance with the Statement of Work; (iii) provide the content, data and materials that Mastercard is required to provide as described in the Statement of Work; and (iv) perform those additional tasks and assume those additional responsibilities specified in the applicable Statement of Work. Mastercard understands and agrees that Provider's performance is dependent on Mastercard's timely and effective satisfaction of the responsibilities in this Section.

**5.4 Securing Rights.** Mastercard will be solely responsible for securing all rights, consents, licenses or approvals to grant Provider access to or use of any third-party data, materials, software or technology necessary for Provider's performance of the Professional Services, other than with respect to any third-party materials included as part of the Platform or that Provider has otherwise agreed to provide as described in the Statement of Work. Provider will abide by the terms and conditions of such permissions, licenses or approvals, provided that Mastercard has provided to Provider written copies of such permissions, licenses or approvals prior to the commencement of the applicable Professional Services.

**5.5 Ownership of Work Product.** Unless Mastercard and Provider have otherwise expressly provided in a Statement of Work (including by making a specific reference to this Section 5.5), all Deliverables (as defined below) will be deemed to be a part of the Platform hereunder and therefore owned by Provider (pursuant to Section 14.3.1 below) and provided to Mastercard (pursuant to Section 2.1 above) under the terms of this Agreement. "Deliverables" means all results and proceeds of the Professional Services provided by Provider.

**5.6 Acceptance of Deliverables.** If Mastercard reasonably believes that any final Deliverable provided by Provider as part of Professional Services fails to conform in some material respect to the specifications set forth in the applicable Statement of Work, then Mastercard will provide Provider with a detailed written description of each alleged non-conformance within ten (10) business days after receipt of such Deliverable. In such an event, Provider will either confirm the non-conformance and commence work on making corrections to such Deliverable or inform Mastercard that Provider does not agree that a non-conformance exists and provide Mastercard with a written explanation for Provider's conclusion. If Provider does not agree that a non-conformance exists, Mastercard and Provider agree to work together in good faith to try to resolve the matter. If Provider does not receive a non-conformance notice from Mastercard within ten (10) business days after receipt of such Deliverable, such Deliverable will be deemed to be accepted under this Agreement. Each Party will provide reasonable assistance and information to one another to assist in resolving any Deliverable non-conformance issues.

## **6. Term.**

**6.1 Term.** The term of this Agreement commences as of the Effective Date and, unless terminated earlier pursuant any of the Agreement's express provisions, will continue in effect until for the period identified in Exhibit A (the "Term").



## 7. Fees, Invoicing and Payment.

7.1 Fees. Subject to the terms and conditions of this Agreement, Mastercard shall pay the fees set forth in Exhibit A ("Fees").

7.2 Expenses. Provider is responsible for all expenses Provider incurs in connection with the performance of Provider's obligations under this Agreement.

7.3 Invoices. Provider will raise invoices to Mastercard as notification for the sums payable and no sum shall be due before Mastercard receives an invoice that:

(a) is itemized, including, as applicable:

- (i) a detailed description of the SaaS Services that accurately reflects their true nature and purpose;
- (ii) an itemization of applicable taxes payable by Mastercard; and
- (iii) ensuring that each invoice line item matches and references the corresponding purchase order line item;

(b) contains an invoice date and invoice number;

(c) contains Provider's complete name, address, and tax identification number (or comparable identification number under applicable Law);

(d) references the purchase order number (if applicable) provided by Mastercard and complies with the invoicing requirements specified in that purchase order;

(e) is delivered electronically to the "bill-to" address or addresses specified in the purchase order (or otherwise by Mastercard) for delivery of invoices; and

(f) is accompanied by supporting receipts, documents, and any other information that Mastercard reasonably requests to verify that invoice.

7.4 Payment. Subject to Provider's compliance with the terms of this Agreement, Mastercard shall pay Provider within forty five (45) days from Mastercard's receipt of the applicable invoice. Payments shall be made on a Mastercard branded card (e.g. purchasing card or virtual card) or through the Mastercard Payment Gateway. All payments hereunder shall be in US dollars. Provider is responsible for all of its costs related to payment acceptance. Except as otherwise expressly provided in this Agreement, all payments are non-refundable. If Mastercard fails to make any payment when due then, in addition to all other remedies that may be available to Provider, Provider may charge interest on the past due amount at the rate of 1.5% per month calculated daily and compounded monthly or, if lower, the highest rate permitted under applicable law.

7.5 Disputes. In the event Mastercard disputes the amounts specified on any invoice received from Provider, Mastercard shall give Provider notice of such dispute prior to the payment due date, pay any undisputed portions of the invoice, and Provider agrees that it shall promptly enter into good faith negotiations to resolve any discrepancy or misunderstanding associated with such amounts. Further, Provider agrees to provide reasonable supporting documentation for any such disputed amount or a corrected invoice within ten (10) days of written request of Mastercard.

7.6 SaaS Support Not to Be Withheld or Delayed. Provider shall not withhold or delay any SaaS Services or fail to perform any other SaaS Support or obligations hereunder by reason of:





(i) Mastercard's good faith withholding of any payment or amount in accordance with this Section 7; or (ii) any dispute whatsoever between the parties, including any payment or other dispute arising under or concerning this Agreement. For the avoidance of doubt, this Section 7.6 does not affect Provider's rights under Section 18.2.3 (Limited Suspension Right) or Section 18.3 (Termination for Cause).

## 8. Security.

8.1 Security Requirements. Throughout the Term and at all times in connection with its actual or required performance of the SaaS Services hereunder, Provider shall:

- (a) maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Operation of the SaaS Services and use of Mastercard's Confidential Information that meet or exceed the security requirements as set forth in Annex 1 to Exhibit D-2 and, to the extent such practices and standards are consistent with and not less protective than the foregoing requirements, are at least equal to applicable industry practices and standards;
- (b) provide technical and organizational safeguards against accidental, unlawful, or unauthorized access to or use, destruction, loss, alteration, disclosure, transfer, commingling, or Operating of such information that ensure a level of security appropriate to the risks presented by the use of Mastercard's Confidential Information and the nature of such Confidential Information, consistent with industry practice and standards;
- (c) take reasonable measures to (i) secure and defend all locations, equipment, systems, and other materials and facilities employed in connection with the SaaS Services against "hackers" and others who may seek, without authorization, to disrupt, damage, modify, access, or otherwise use Provider Systems or the information found therein; and (ii) prevent: (a) Mastercard and its Authorized Users from having unauthorized access to the data of Provider's other customers or such other customers' users of the SaaS Services; (b) and (b) unauthorized access to any of Mastercard's Confidential Information;
- (d) periodically test its systems for potential areas where security could be breached;
- (e) report to Mastercard any breach of security which leads unauthorized access to Mastercard's Confidential Information the Provider detects or becomes aware of (a "Security Breach") without undue delay and in any event within twenty-four (24) hours after Provider confirms such Security Breach; provided that unsuccessful attempts or activities that do not compromise the security of Mastercard's Confidential Information, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems, will not constitute a Security Breach;
- (f) use its best efforts to remedy any Security Breach in a timely manner and deliver to Mastercard a root cause assessment and future incident mitigation plan with regard to any Security Breach that sets out written details regarding Provider's investigation of such incident;
- (g) refrain from notifying, for or on behalf of Mastercard or any Authorized User, any regulatory authority, consumer, or other Person of any such Security Breach unless Mastercard specifically requests in writing that Provider do so, except as and when otherwise required by applicable Law; and
- (h) if such Security Breach results from any act or omission of Provider or any Provider Personnel that constitutes a material breach of this Section 8, promptly reimburse Mastercard for all reasonable costs and expenses Mastercard may incur in notifying any Person of such security breach or unauthorized access required by applicable Law.
- (i) Without limiting the generality of the foregoing, Provider and Mastercard will work together to formulate a plan to rectify all Security Breaches.



**8.2 Provider Systems.** Subject to Mastercard's obligations under this Agreement, Provider shall be responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems), and networks used by or for Provider in connection with the SaaS Services ("Provider Systems") and shall take industry standard steps to prevent unauthorized access to the Mastercard Systems through the Provider Systems. Except as is strictly necessary to fulfill its obligations hereunder, Provider shall not access, and shall not permit any access to, the Mastercard Systems, in whole or in part, whether through Provider's Systems or otherwise, without Mastercard's express prior written authorization. Such authorization may be revoked by Mastercard in writing at any time in its sole discretion; provided that in the event Provider requires such access to perform its obligations hereunder, such non-performance will be excused without penalty or refund.

**8.3 Security Records.** During the Term, Provider shall (i) maintain complete and accurate records relating to its data protection practices and the security of Mastercard's Confidential Information, including any backup, disaster recovery, or other policies, practices, or procedures relating to Mastercard's Confidential Information and any other information relevant to its compliance with this Section 8.3; and (ii) upon Mastercard's request, make all such records, appropriate personnel, and relevant materials available during normal business hours for inspection and audit by Mastercard or an independent data security expert that is reasonably acceptable to Provider, provided that Mastercard shall: (a) give Provider reasonable prior notice of any such audit; (b) undertake such audit no more than once per calendar year, except for good cause shown; and (c) conduct or cause to be conducted such audit in a manner designed to minimize disruption of Provider's normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security, and restricted use provisions of this Agreement.

**8.4 Regulatory and Compliance Authorities.** Any authorized representative of any regulatory agency, taxing authority, or private entity that functions in a quasi-regulatory manner that has jurisdiction over Mastercard in connection with its regulatory functions (each, a "Regulator") shall, upon request, have the same rights as those set forth in Section 8.3, provided that no condition or restriction stated in Section 8.3 shall apply to any Regulator to the extent it is contrary to applicable Law. Provider shall cooperate with all individuals conducting such audits and timely comply with all legal and regulatory directives and reasonable recommendations that result from such inspections, tests, and audits.

**8.5 Non-Exclusive Remedy for Security Breach.** Any failure of the SaaS Services to meet the requirements of this Agreement with respect to the security of any Mastercard Data or other Confidential Information of Mastercard, including any related backup, disaster recovery, or other policies, practices, or procedures to the extent so required under this Agreement, is a material breach of this Agreement for which Mastercard, at its option, may terminate this Agreement on written notice to Provider without any a cure period, and Provider shall promptly reimburse to Mastercard any Fees prepaid by Mastercard prorated to the date of such termination.

**8.6 Provider Security Contact.** Provider shall appoint a Provider employee to respond to Mastercard's inquiries regarding the security of the Provider Systems, who has sufficient knowledge of the security of the Provider Systems and the authority to act on behalf of Provider in matters pertaining thereto ("Provider Security Contact").

**9. Redundancy, Data Backup, and Disaster Recovery.** Provider shall, in accordance with the provisions of this Section 9, maintain or cause to be maintained disaster avoidance procedures designed to safeguard the Mastercard Data and Mastercard's other Confidential Information, Provider's Operating capability, and the availability of the SaaS Services, in each case throughout the Term and at all times in connection with its actual or required performance of the SaaS Services hereunder. The force majeure provisions of Section 20.11 shall not limit Provider's obligations under this Section 9 if the applicable Force Majeure Event would have been avoided with the use by Provider of industry standard redundancies.



9.1 Redundant Hosting and Connectivity. Provider may use Amazon Web Services (AWS) and/or such other reputable hosting provider that implements and maintains commercially reasonable security programs, policies, procedures, controls and technologies (each a "Reputable Hosting Services Provider") for cloud-based infrastructure and hosting and storage services for the SaaS Services, and such Reputable Hosting Services Provider will host and store certain portions of Mastercard Data that is processed through the SaaS Services. Provider shall provision instances of its SaaS Services across at least two (2) geographically separate data centers in at least two (2) AWS Availability Zones (as defined by AWS) (or such other equivalent if a different cloud provider is used) (the "Secondary Backup Facility") each of which shall: (i) be identical in all respects to the primary system; (ii) have hardware and software, network connectivity, power supplies, backup generators, and other similar equipment and services that operate independently of the primary system; (iii) have fully current backups of all Mastercard Data stored on the primary system; and (iv) have the ability to provide the SaaS Services in accordance with this Agreement and the Specifications during the performance of routine and remedial maintenance or any outage or failure of the primary system. Provider shall operate, monitor, and maintain such mirror system so that it may be activated within [24 hours] of any failure of the SaaS Services to be Available.

9.2 Data Backup. Provider shall conduct or have conducted regular backups of Mastercard Data and perform or cause to be performed periodic backups of Mastercard Data and store such backup Mastercard Data in a commercially reasonable location and manner on regular basis at the Secondary Backup Facility.

9.3 Disaster Recovery/Business Continuity. Throughout the Term and at all times in connection with its actual or required performance of the SaaS Services hereunder, Provider shall maintain a Business Continuity and Disaster Recovery Plan for the SaaS Services (the "Plan") and implement such Plan in the event of any unplanned interruption of the SaaS Services. Provider shall actively test, review, and update the Plan on at least an annual basis using industry best practices as guidance.

## 10. Compliance.

10.1 Mastercard Policies and Procedures. In no event will Provider or Provider Personnel have physical and/or remote access to a Mastercard location in connection with performance of the SaaS Services. In the event such access is needed, the Provider and Mastercard shall enter into an amendment to this Agreement setting forth the terms and conditions of such access. Provider shall:

(a) comply with the Mastercard Provider Code of Conduct then in effect, a current copy of which is available at [https://procurement.mastercard.com/information\\_Providers.html](https://procurement.mastercard.com/information_Providers.html). Provider may report violations or potential violations of the Provider Code of Conduct or any ethically questionable behavior in breach of this Agreement by contacting the Mastercard Ethics Hotline (available at [www.mastercardworldwide.com](http://www.mastercardworldwide.com)) or by notifying Mastercard in accordance with Section 20.7 (Notices).

10.2 Compliance with Applicable Laws. Provider shall comply with all local Laws applicable to Provider and Provider's obligations under this Agreement in force in the territory where the obligations are being carried out, and Provider warrants that its Provider Personnel and the SaaS Services shall be in compliance with such Laws, including but not limited to the Laws specifically listed below:

(a) Provider shall verify, before each such Provider Personnel commences performing SaaS Services and as otherwise required by applicable Law, the identity and right to work (under the immigration Laws applicable to the location in which that Provider Personnel is performing SaaS Services) of all Provider Personnel performing SaaS Services.





(b) Provider acknowledges that Mastercard and any Person acting on its behalf must comply with applicable international anti-bribery and anti-corruption Laws (including the Foreign Corrupt Practices Act and the UK Bribery Act). Provider shall comply with all applicable anti-bribery and anti-corruption Laws applicable to its business dealings, including dealings with government body officials. Provider shall not, in connection with the transactions contemplated by this Agreement or in connection with any other business transactions involving Mastercard: (i) make, promise, or offer to make any payment or transfer of anything of value or other advantage, directly or indirectly through a representative, intermediary, agent or otherwise, to a government body official, political party or candidate for political office, or any other Person for the purpose of improperly influencing the conduct or decision of any such government body official, political party, candidate, or Person or securing an improper advantage to assist Mastercard or Provider in obtaining or retaining business; or (ii) accept anything of value from any Person seeking to improperly influence the conduct or decision of Provider secure an improper advantage to that Person. Failure by Provider to comply with the terms of this Section 10.2(b) will constitute a material breach of this Agreement.

(c) Provider shall comply with all trade and economic sanctions programs, including trade and economic sanctions maintained by the Office of Foreign Assets Control ("OFAC") and similar Laws of countries where Provider is located and where Provider Personnel will be traveling or performing SaaS Services. Provider shall not engage in any conduct that would cause Mastercard to violate applicable foreign sanctions programs. Provider shall not offer employment, continue to employ, or contract with a Person included on applicable foreign sanctions lists, including those maintained by OFAC. Provider shall notify Mastercard immediately if any Provider Personnel appear on any such sanctions list and shall immediately replace that Provider Personnel.

**11. Subcontracting.** Notwithstanding any term to the contrary, (i) Provider shall be liable to Mastercard for any damages incurred by Mastercard due to any Provider subcontractor (including any subcontractor of a Provider subcontractor, each, a "Subcontractor") non-compliance with all relevant terms of this Agreement, including all provisions relating to Mastercard Data, Personal Data, or other Confidential Information of Mastercard; (ii) any delegation by Provider to any such Subcontractor shall not relieve Provider of its representations, warranties, or obligations under this Agreement; (iii) Provider shall remain responsible and liable for any and all: (a) performance required hereunder, including the proper supervision, coordination, and performance of the SaaS Services; and (b) acts and omissions of each Subcontractor (including, such Subcontractor's employees and agents, who, to the extent they are involved in providing any SaaS Services, are deemed Provider Personnel) to the same extent as if such acts or omissions were by Provider; (iv) any noncompliance by any Subcontractor or its employees or agents with the provisions of this Agreement will constitute a breach by Provider; and (v) prior to the provision of SaaS Services by any Subcontractor, Provider shall obtain from each such proposed Subcontractor the identity of such Subcontractor and the location of all its data centers, if any, that will be used in Operating any Mastercard Data.

## **12. Confidentiality.**

**12.1 Confidential Information.** In connection with this Agreement, each party (as the "Disclosing Party") may disclose or make available Confidential Information to the other party (as the "Receiving Party"). Subject to Section 12.2, "Confidential Information" means information in any form or medium (whether oral, written, electronic, or other) that (i) contains a marking (such as "confidential", "proprietary" or "For Internal Use Only") indicating its confidential nature; (ii) is designated confidential or proprietary expressly or by the circumstances under which it is provided; or (iii) is known or reasonably should be known by Receiving Party to be confidential or proprietary, including information consisting of or relating to the Disclosing Party's technology, trade secrets, know-how, business operations, plans, strategies, customers, and pricing, and information with respect to which the Disclosing Party has contractual or other confidentiality obligations. Without limiting the foregoing, (i) all Mastercard Data (including all Personal Data) is and will remain the Confidential Information of Mastercard; (ii) the SaaS Services, Specifications, and Documentation as well as all non-public information related to the SaaS Services (including without limitation, pricing information (e.g., price quotes) and the source code for the SaaS Services and the methods,



algorithms, structure and logic, technical infrastructure, techniques and processes used by Provider in developing, producing, marketing and/or providing the SaaS Services, are and will remain the Confidential Information of Provider; and (iii) the terms and existence of this Agreement are the Confidential Information of both parties.

12.2 Exclusions. Subject to Section 12.3, Confidential Information does not include information that the Receiving Party can demonstrate by written or other documentary records: (i) was rightfully known to the Receiving Party without restriction on use or disclosure prior to such information's being disclosed or made available to the Receiving Party in connection with this Agreement; (ii) was or becomes generally known by the public other than by the Receiving Party's noncompliance with this Agreement; (iii) was or is received by the Receiving Party on a non-confidential basis from a third party that was not or is not, at the time of such receipt, under any obligation to maintain its confidentiality; (iv) the Receiving Party can demonstrate by written or other documentary records was or is independently developed by the Receiving Party without reference to or use of any Confidential Information.

12.3 Mastercard Data Exception. Notwithstanding the provisions of Section 12.2 or any other provisions of this Agreement, none of the exclusions set forth in Section 12.2 apply to any Mastercard Data, whether provided by or on behalf of Mastercard to Provider or the SaaS Services for Operating or generated or derived from such Operating and regardless of whether such Mastercard Data may be publicly available or otherwise qualify for exclusion under any of the other provisions of Section 12.2. The preceding sentence does not prohibit or limit Provider from any use or disclosure of any information that may be the same as any Mastercard Data but which Provider can demonstrate by documentary evidence was: (i) obtained by Provider without access to, reference to, or use of any Mastercard Data; and (ii) at all times maintained separately from and not in any way combined, commingled, compared, benchmarked, or in any way associated with any Mastercard Data.

12.4 Confidentiality and Use. Each Receiving Party recognizes and agrees that the Confidential Information of the Disclosing Party is critical to the Disclosing Party's business and that neither party would enter into this Agreement without assurance that such information and its value will be protected as provided in this Section 12 and elsewhere in this Agreement. As a condition to being provided with any disclosure of or access to Confidential Information, the Receiving Party shall:

- (a) not access or use, or permit the access or use of, Confidential Information other than as necessary to exercise its rights or perform its obligations under and in accordance with this Agreement;
- (b) except as may be permitted by and subject to its compliance with Section 12.5, not disclose or permit access to Confidential Information other than to its Representatives who: (i) need to know such Confidential Information for purposes of the Receiving Party's exercise of its rights or performance of its obligations under and in accordance with this Agreement; (ii) have been informed of the confidential nature of the Confidential Information and the Receiving Party's obligations under this Section 12; and (iii) are bound by written confidentiality and restricted use obligations at least as protective of the Confidential Information as the terms set forth in this Section 12;
- (c) safeguard the Confidential Information from unauthorized use, access, or disclosure using at least the degree of care it uses to protect its sensitive information and in no event less than a reasonable degree of care;
- (d) ensure its Representatives' compliance with, and be responsible and liable for any of its Representatives' noncompliance with, the terms of this Section 12; and



(e) notify the Disclosing Party in writing immediately of any unauthorized disclosure or use of the Disclosing Party's Confidential Information and cooperate with the Disclosing Party to protect the confidentiality and ownership of all Intellectual Property Rights, privacy rights, and other rights therein.

**12.5 Compelled Disclosures.** If the Receiving Party or any of its Representatives is compelled by applicable Law to disclose any Confidential Information, then, to the extent permitted by applicable Law, the Receiving Party shall: (i) promptly, and prior to such disclosure, notify the Disclosing Party in writing of such requirement so that the Disclosing Party can seek a protective order or other remedy, or waive its rights under Section 12.4; and (ii) provide reasonable assistance to the Disclosing Party in opposing such disclosure or seeking a protective order or other limitations on disclosure. If the Disclosing Party waives compliance or, after providing the notice and assistance required under this Section 12, the Receiving Party remains required by Law to disclose any Confidential Information, the Receiving Party shall disclose only that portion of the Confidential Information that the Receiving Party is legally required to disclose and, upon the Disclosing Party's request, shall use commercially reasonable efforts to obtain assurances from the applicable court or other presiding authority that such Confidential Information will be afforded confidential treatment. No such compelled disclosure by the Receiving Party will otherwise affect the Receiving Party's obligations hereunder with respect to the Confidential Information so disclosed.

### 13. Privacy and Data Protection.

#### 13.1 Permitted Use.

(a) During the Term and thereafter in perpetuity, Provider shall not cause or permit any operations to access or use Personal Data in any manner or for any purpose other than the sole purpose of performance of the SaaS Services (including enforcement of Provider's rights herein and as required by applicable Laws) in compliance with the express obligations and restrictions set forth in this Agreement and all applicable Laws.

(b) If Provider or any Provider Personnel receives or otherwise has access to Personal Data, Provider shall comply with the requirements of **Exhibit D** which is hereby incorporated into and made a part of this Section 13. For further clarity, **Exhibit D** contains additional terms that apply if Provider or any Provider Personnel receives, has access to, or otherwise Processes Personal Data under this Agreement and **Annex 3** contains additional terms and conditions that apply if Provider or any Provider Personnel receives, has access to, or otherwise Processes Personal Data of Data Subjects subject to the EU General Data Protection Regulation under this Agreement.

☒ Check box in case Provider or any Provider Personnel receives, has access to, or otherwise Processes Personal Data of Data Subjects subject to EU Data Protection Law under this Agreement. If above box is checked, Provider confirms to have signed **Exhibit D**, in a format provided by Mastercard, prior to the processing of personal data in the context of this Agreement pertaining to individuals located in the European Economic Area ("EEA") or Switzerland or prior to engaging in any processing subject to the EU General Data Protection Regulation.

**13.2 Ownership and Treatment of Personal Data.** As between Mastercard and Provider, Mastercard is and shall remain the sole and exclusive owner of all right, title, and interest in and to Personal Data. Without limiting any other representation, warranty, or obligation of Provider under this Agreement, Provider represents, warrants, and covenants that:

(a) except as Mastercard or an Authorized User may submit to Provider Personnel for purposes of Mastercard's or such Authorized User's use of the SaaS Services, or as Mastercard may hereafter expressly direct in advance in writing, Provider will not under or in connection with this Agreement collect any Personal Data from or in connection with Mastercard's or any Authorized User's access to or use of the SaaS Services, or through any access Provider may have to the Mastercard Systems, including through any cookies, applets, beacons, or other



data mining methods or technologies except as strictly necessary for Provider to perform its obligations hereunder; and

(b) Provider shall not capture, maintain, scan, index, share or use Personal Data stored or transmitted by the SaaS Services, or otherwise use any data-mining technology, for any non-authorized activity and shall not permit its agents or subcontractors to do so. For purposes of this requirement, "non-authorized activity" means the data mining or processing of data, stored or transmitted through the SaaS Services, for unrelated commercial purposes, advertising or advertising-related purposes, or for any other purpose other than security analysis that is not explicitly authorized in this Agreement.

(c) Provider shall promptly notify Mastercard in writing when Provider becomes aware of any unauthorized access, use, or other act respecting Personal Data or if Provider becomes the subject of any government, regulatory, or other investigation or proceeding relating to its privacy, data security, or handling practices.

## **14. Intellectual Property Rights.**

14.1 Ownership of Mastercard Data. Mastercard may, but is not required to, provide Mastercard Data to Provider in connection with this Agreement; provided that to the extent Provider is precluded from performing its obligations hereunder due to Mastercard not providing such Mastercard Data, Provider's nonperformance shall be excused without penalty. As between Mastercard and Provider, Mastercard is and will remain the sole and exclusive owner of all right, title, and interest in and to all Mastercard Data, including all Intellectual Property Rights relating thereto, subject only to the limited license granted in Section 14.2.

14.2 Limited License to Use Mastercard Data. Subject to the terms and conditions of this Agreement, Mastercard hereby grants Provider a limited, royalty-free, fully-paid up, non-exclusive, non-transferable, and non-sublicensable license to Operate the Mastercard Data strictly as instructed by Mastercard or an Authorized User and solely as necessary to provide the SaaS Services for Mastercard's benefit as provided in this Agreement, to enforce Provider's rights under this Agreement and as required by applicable Law for so long as Mastercard or any Authorized User uploads or stores such Mastercard Data for Operating by or on behalf of the Provider on the Provider Systems.

14.3 Ownership of Provider Materials. As between Mastercard and Provider, Provider is and will remain the sole and exclusive owner of all right, title, and interest in and to the Provider Materials, including any improvements to the SaaS Services made by Provider based upon Mastercard's use of the SaaS Services, and all Intellectual Property Rights relating to and all derivative works of, any of the foregoing, subject only to the authorization and license granted to Mastercard in Section 2 (SaaS Services). Provider reserves all rights not expressly granted to Mastercard in this Agreement.

14.4 No Implied Rights. Except for the limited license expressly provided: (i) in Section 14.2, nothing contained in this Agreement shall be construed as granting Provider or any third party any right, title, or interest in or to any Mastercard Data; or (ii) in Section 2 (SaaS Services), nothing contained in this Agreement shall be construed as granting Mastercard or any third party any right, title, or interest in or to any Provider Materials, in each case (clause (i) and (ii)) whether by implication, estoppel, or otherwise.

14.5 Usage Data. Notwithstanding any term to the contrary, Mastercard acknowledges and agrees that: (a) Provider may collect metadata and other statistical information regarding Mastercard's and its Authorized Users' use of and the performance of the SaaS Services ("Usage Data"); provided that Usage Data does not contain and is not derived from Mastercard Data; (b) Provider may use Usage Data in connection with providing SaaS Support to Mastercard and for Provider's internal business purposes (such as monitoring, enhancing and improving the SaaS Services); and (c) Provider may publish and share with third parties aggregated Usage



Data that cannot, by itself or with other data, directly or indirectly, identify Mastercard, Mastercard's customers or clients or any other individual or entity.

## 15. Representations and Warranties.

15.1 Mutual Representations and Warranties. Each party represents and warrants to the other party that:

- (a) it is a duly organized, validly existing, and in good standing as a corporation or other entity under the Laws of the jurisdiction of its incorporation or other organization;
- (b) it has and will, and throughout the Term and any additional periods during which it does or is required to perform or use the SaaS Services retain, the full right, power, and authority to enter into this Agreement and perform its obligations hereunder;
- (c) the execution of this Agreement by its representative whose signature is set forth at the end of this Agreement has been duly authorized by all necessary corporate or organizational action of such party; and
- (d) when executed and delivered by both parties, this Agreement will constitute the legal, valid, and binding obligation of such party, enforceable against such party in accordance with its terms.

15.2 Additional Provider Warranties. Provider represents, warrants, and covenants to Mastercard that:

- (a) neither Provider's grant of the rights or licenses hereunder nor its performance of any SaaS Services or other obligations under this Agreement does or at any time will: (i) conflict with or violate any applicable Law, including any Law relating to data privacy, data security, or Personal Data; (ii) require the consent, approval, or authorization of any governmental or regulatory authority or other third party which has not been properly attained by Provider; or (iii) require the provision of any payment or other consideration by Mastercard or any Authorized User to any third party, and Provider shall promptly notify Mastercard in writing if it becomes aware of any change in any applicable Law that would preclude Provider's performance of its material obligations hereunder;
- (b) as accessed and used by Mastercard or any Authorized User in accordance with this Agreement and the Specifications, the SaaS Services, Documentation, and all other SaaS Services and materials provided by Provider under this Agreement, to the best of Provider's knowledge as of the execution of this Agreement will not infringe, misappropriate, or otherwise violate any Intellectual Property Right or other right of any third party; provided that the sole remedy for breach of the warranty in this Section 15.2(b) shall be Provider's obligations under Section 16.2 (iii) below;
- (c) to its knowledge as of the date of execution of this Agreement, there is no settled, pending, or threatened Action, and as of the date of execution of this Agreement it has not received any written, oral, or other notice of any Action (including in the form of any offer to obtain a license): (i) alleging that any access to or use of the SaaS Services does or would infringe, misappropriate, or otherwise violate any Intellectual Property Right of any third party; (ii) challenging Provider's ownership of, or right to use or license, any software or other materials used or required to be used in connection with the performance, accessing or use of the SaaS Services, or alleging any adverse right, title, or interest with respect thereto; or (iii) that, if decided unfavorably to Provider, would reasonably be expected to have an actual or potential adverse effect on its ability to perform the SaaS Services or its other obligations under this Agreement, and as of the date of execution of this Agreement it has no knowledge of any factual, legal, or other reasonable basis for any such litigation, claim, or proceeding;
- (d) the SaaS Services will in all material respects conform to and perform in accordance with the Specifications and all requirements of this Agreement, including the SaaS Support provisions set forth in Section 2.2. and if Provider breaches this warranty, in addition to any remedies available to Mastercard, Provider will, at its





option: (i) promptly correct any portion of the SaaS Services that fails to meet this warranty; (ii) provide Mastercard with a reasonable procedure to circumvent the nonconformity; or (iii) refund to Mastercard on a pro rata basis the share of any fees prepaid by Mastercard for the portion of the applicable Term in which the SaaS Services is non-conforming;

(e) all Specifications are, and will be continually updated and maintained so that they continue to be, current, complete, and accurate so that they do and will continue to fully describe the SaaS Services in all material respects such that at no time during the Term or any additional periods during which Provider does or is required to perform the SaaS Services will the SaaS Services have any material undocumented feature;

(f) it will take commercially reasonable measures to ensure that the Provider Systems and SaaS Services are and will remain free of Harmful Code; and

(g) Provider will perform all SaaS Services in a timely, professional, and workmanlike manner with a level of care, skill, practice, and judgment consistent with industry standards and practices for similar services, using personnel with the requisite skill, experience, and qualifications, and will devote adequate resources to meet Provider's obligations under this Agreement, and in the event Provider breaches this warranty, as Provider's sole obligation and liability to Mastercard and Mastercard's sole and exclusive remedy, Provider will, at its option: (i) promptly correct any portion of the SaaS Services that fails to meet this warranty; (ii) provide Mastercard with a reasonable procedure to circumvent the nonconformity; or (iii) refund to Mastercard on a pro rata basis the share of any fees prepaid by Mastercard for the portion of the applicable Term in which the SaaS Services is non-conforming.

#### 15.3 Additional Mastercard Warranties. Mastercard represents and warrants that:

(a) it will not use the SaaS Services, directly or indirectly, for any fraudulent undertaking or in any manner so as to interfere with the use of the SaaS Services;

(b) Mastercard's use of the SaaS Services and its collection and use of all of Mastercard Data (including Mastercard's processing of Mastercard Data and/or any card authorization, credit, ticket only, capture or settlement request, decline transaction, or other related transaction, completed or submitted under Mastercard's account) will comply with (i) all applicable Laws, (ii) the terms of service of the payment gateways, merchant service providers and/or API endpoints Mastercard connects with on the SaaS Services; (iii) the operating rules, bylaws, schedules, supplements and addenda, manuals, instructions, releases, specifications and other requirements, as may be amended from time-to-time, of any of the payment networks including Visa, MasterCard, American Express, Discover Financial Services, and any affiliates thereof or any other payment network applicable to this Agreement; (iv) PCI-DSS and Payment Application Data Security Standard ("PA-DSS"), as applicable; and (v) any regulatory body or agency having jurisdiction over the subject matter thereof;

(c) Mastercard either owns, or has all rights, permissions and consents that are necessary to process, and to permit Provider, its subcontractors and the SaaS Services to process as contemplated in this Agreement, all Mastercard Data and the credit card transaction related thereto; and

(d) Provider's and its subcontractors' access to and use of Mastercard Data as contemplated by this Agreement does not and will not violate any applicable Law or infringe, misappropriate or otherwise violate any Intellectual Property Right, privacy right or other right of any third party.

**15.4 DISCLAIMER. EXCEPT FOR THE EXPRESS WARRANTIES IN THIS AGREEMENT, EACH PARTY HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE UNDER OR IN CONNECTION WITH THIS AGREEMENT OR ANY SUBJECT MATTER HEREOF INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. WITHOUT LIMITING THE FOREGOING, NEITHER PROVIDER WARRANTS THAT THE SAAS SERVICES WILL BE ERROR-FREE OR UNINTERRUPTED**



## 16. Indemnification.

16.1 General Indemnification. Each party (the "Indemnifying Party") shall indemnify, defend, and hold harmless the other party and each of the other party's Affiliates, and its officers, directors, employees, agents, successors, and assigns (each of the foregoing Persons, an "Indemnitee") from and against any and all Losses incurred by the Indemnitee resulting from any Action by a third party (other than an Affiliate of the Indemnitee) to the extent that such Losses arise out of or result from, or are alleged to arise out of or result from:

- (a) Indemnifying Party's intentional or gross negligence;
- (b) Indemnifying Party's breach of Section 10 (Compliance);
- (c) Indemnifying Party's breach of Section 12 (Confidentiality);
- (d) Indemnifying Party's breach of Section 13 (Privacy and Data Protection);
- (e) Indemnifying Party's breach of an express representation or warranty;

16.2 Infringement Indemnification by Provider. Provider shall indemnify, defend, and hold harmless Mastercard and its Affiliates and their respective officers, directors, employees, agents, successors, and assigns (each a "Mastercard Indemnitee") from and against any and all Losses incurred by Mastercard Indemnitee resulting from any Action by a third party (other than an Affiliate of Mastercard) arising from, in connection with, or based on: (i) a Security Breach that is caused by Provider's material breach of Annex 1 to Exhibit D; (ii) Provider's failure to remain compliant with PCI-DSS; or (iii) allegations whenever made that the SaaS Services, or Mastercard's or any Authorized User's use thereof, infringe, misappropriate, or otherwise violate such third party's Intellectual Property Right, provided however, that Provider shall have no liability or obligation for any Action or Losses to the extent that such Action or Losses arise out of or results from any:

- (a) alteration or modification of the SaaS Services by or on behalf of Mastercard or any Authorized User without Provider's authorization (each, a "Mastercard Modification"), provided that no infringement, misappropriation, or other violation of third party rights would have occurred without such Mastercard Modification and provided further that any alteration or modification made by or for Provider at Mastercard's request shall not be excluded from Provider's indemnification obligations hereunder unless (i) such alteration or modification has been made pursuant to Mastercard's written specifications prepared independently of and without any contribution by Provider; and (ii) the SaaS Services, as altered or modified in accordance with the Mastercard's specifications, would not have violated such third party rights but for the manner in which the alteration or modification was implemented by or for Provider;
- (b) use of the SaaS Services by Mastercard or an Authorized User pursuant to this Agreement in combination with any software or service not provided, authorized, or approved by or on behalf of Provider, if no violation of third party rights would have occurred without such combination;
- (c) access to or use of the SaaS Services that is expressly prohibited by this Agreement or otherwise outside the scope of access or manner or purpose of use described or contemplated anywhere in this Agreement or the Specifications;
- (d) material breach of this Agreement by Mastercard or material noncompliance herewith by any Authorized User; or
- (e) violation of any applicable Law by Mastercard or any of its Authorized Users.



**16.3 Infringement Indemnification by Mastercard.** Mastercard shall indemnify, defend, and hold harmless Provider and its Affiliates and their respective officers, directors, employees, agents, successors, and assigns (each a "Provider Indemnitee") from and against any and all Losses incurred by Provider Indemnitee resulting from any Action by a third party (other than an Affiliate of Provider) arising from, in connection with, or based on allegations whenever made of, any of the following:

(a) any claim that any Mastercard Data is unlawful or actually does or threatens to infringe or misappropriate any Intellectual Property Rights or other rights of any third party, provided however, that Mastercard shall have no liability or obligation with respect to any Action or Losses to the extent that such Action or Losses arise out of or result from any unauthorized access to or use, disclosure, or other Operating of Mastercard Data, including Personal Data, by or on behalf of Provider, or through or enabled by the Provider Systems, whether authorized by Provider, due to a security breach, or otherwise;

(b) any use of the SaaS Services by Mastercard or any Authorized User that is beyond the scope of or otherwise fails to conform to the express requirements or restrictions of this Agreement or any authorization or approval given in writing by Provider to Mastercard or such Authorized User; or

**16.4 Indemnification Procedure.** The party seeking indemnification shall promptly notify the Indemnifying Party in writing of any Action for which it seeks indemnification pursuant to this Section 16 and cooperate with the Indemnifying Party at Indemnifying Party's sole cost and expense. The Indemnifying Party shall immediately take control of the defense and investigation of such Action and shall employ counsel to handle and defend the same, at the Indemnifying Party's sole cost and expense. The Indemnifying Party shall not settle any Action on any terms or in any manner that adversely affects the rights of any Indemnitee without the other party's prior written consent, which shall not be unreasonably withheld or delayed. Any Indemnitee may participate in and observe the proceedings at its own cost and expense with counsel of its own choice. A party's failure to perform any obligations under this Section 16.4 will not relieve the Indemnifying Party of its obligations under Section 16 except to the extent that the Indemnifying Party can demonstrate that it has been materially prejudiced as a result of such failure.

**16.5 Mitigation.**

(a) If Provider receives or otherwise learns of any threat, warning, or notice alleging that all, or any component or feature, of the SaaS Services violates a third party's rights, Provider shall promptly notify Mastercard of such fact in writing, and take all commercially reasonable actions necessary to ensure Mastercard's continued right to access and use such SaaS Services and otherwise protect Mastercard from any Losses in connection therewith.

(b) Subject to the exclusions set forth in Sections 16.2(a) through 16.2(e), if any of the SaaS Services or any component or feature thereof is ruled to infringe or otherwise violate the rights of any third party by any court of competent jurisdiction, or if any use of any SaaS Services or any component thereof is threatened to be enjoined, or in either party's reasonable opinion, is likely to be enjoined or otherwise the subject of an infringement or misappropriation claim, Provider shall, at Provider's sole cost and expense:

(i) procure for Mastercard the right to continue to access and use the SaaS Services to the full extent contemplated by this Agreement and the Specifications; or

(ii) modify or replace all components, features, and operations of the SaaS Services that actually, or are likely or alleged to, infringe or otherwise violate the rights of any third party ("Allegedly Infringing Features") to end and avoid such infringement or violation while providing equally or more suitable features and functionality, which modified and replacement services shall constitute SaaS Services and be subject to the terms and conditions of this Agreement.



(c) If neither of the remedies set forth in Section 16.5(b) is reasonably available with respect to the Allegedly Infringing Features then Provider may direct Mastercard to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that Provider shall:

- (i) refund to Mastercard any prepaid Fees for SaaS Services that have not been provided
- (ii) reserved.

## **17. Limitations of Liability.**

17.1 EXCLUSION OF DAMAGES. IN NO EVENT WILL EITHER PARTY BE LIABLE UNDER THIS AGREEMENT UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE, FOR ANY LOST PROFITS, LOSS OF ANTICIPATED SAVINGS, WASTED EXPENDITURE, LOSS OF BUSINESS OPPORTUNITIES, REPUTATION OR GOODWILL, OR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, ENHANCED, OR PUNITIVE DAMAGES REGARDLESS OF WHETHER SUCH PERSONS WERE ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES OR SUCH LOSSES OR DAMAGES WERE OTHERWISE FORESEEABLE, AND NOTWITHSTANDING THE FAILURE OF ANY AGREED OR OTHER REMEDY OF ITS ESSENTIAL PURPOSE.

17.2 SUBJECT TO SECTION 17.4, NOTWITHSTANDING ANY OTHER PROVISION TO THE CONTRARY SET FORTH IN THIS AGREEMENT MASTERCARD'S TOTAL AGGREGATE LIABILITY UNDER THIS AGREEMENT (INCLUDING, WITHOUT LIMITATION, ANY INDEMNIFICATION OBLIGATIONS HEREUNDER) SHALL NOT EXCEED TWO HUNDRED FIFTY THOUSAND DOLLARS (\$250,000)

17.3 SUBJECT TO SECTIONS 17.4, NOTWITHSTANDING ANY OTHER PROVISION TO THE CONTRARY SET FORTH IN THIS AGREEMENT, THE MAXIMUM AGGREGATE LIABILITY OF PROVIDER AND ITS AFFILIATES ARISING OUT OF OR RELATING TO THIS AGREEMENT INCLUDING WITHOUT LIMITATION, ANY INDEMNIFICATION OBLIGATIONS HEREUNDER, SHALL NOT EXCEED ONE MILLION DOLLARS (\$1,000,000).

17.4 Exceptions. The exclusions and limitations in Section 17.2 and 17.3 shall not apply to:

- (a) Losses arising out of or relating to Provider's unauthorized suspension, termination, or disabling of the SaaS Services in breach of this Agreement;
- (b) Losses arising out of or relating to a party's gross negligence or more culpable conduct, including any willful misconduct or intentional wrongful acts; or
- (c) Losses for death or bodily injury arising out of or relating to a party's negligent or more culpable acts or omissions; or
- (d) Losses arising from or relating to any other matter for which it would be unlawful for the parties to exclude liability.

## **18. Termination.**

18.1 Termination for Convenience. Provided there are no Order Forms or Statements of Work are in effect, Mastercard may terminate this Agreement at any time without cause by providing at least 30 days' prior written notice to Provider. Except as otherwise provided in the applicable Order Form, where any Order Form Term is Month-Month, Mastercard in its sole discretion,



may terminate this said Order Form at any time, without cause, by providing at least thirty (30) days' prior written notice to the Provider. If any Order Form Term is Annual, Mastercard in its sole discretion, may terminate this Agreement, without cause, by providing at least thirty (60) days' prior written notice to the Provider before the one-year anniversary date.

18.2 Limited Suspension Right. Provider may suspend the Services or otherwise restrict access to the Provider network if: (i) required to comply with any Law or regulation, or at the direction of law enforcement; or (ii) the provision of Services is likely to cause material harm to Provider, the SaaS Services or any other party. Any such suspension or restriction will be on the most limited basis as Provider determines is reasonably practical under the circumstance. Unless prohibited by law or court order, Provider will use commercially reasonable efforts to provide notice as soon as practicable to Mastercard of any suspension and resume Service upon remedy of the reason for suspension.

18.3 Termination for Cause. In addition to any right of termination set forth elsewhere in this Agreement:

(a) either party may terminate by written notice of termination to the other party effective as of the date specified in such notice: (i) this Agreement, if the other party materially breaches this Agreement (including payment default by Mastercard); and (ii) provided that such breach (a) cannot be cured; or (b) being capable of cure, remains uncured 30 days after the breaching party receives written notice thereof; and

(b) either party may terminate this Agreement, effective immediately, by written notice to the other party if the other party: (i) is dissolved or liquidated or takes any corporate action for such purpose; (ii) becomes insolvent or is generally unable to pay, or fails to pay, its debts as they become due; (iii) files or has filed against it a petition for voluntary or involuntary bankruptcy or otherwise becomes subject, voluntarily or involuntarily, to any proceeding under any domestic or foreign bankruptcy or insolvency Law, if such proceeding is not fully stayed within seven Business Days or is not dismissed or vacated within 45 days after filing; (iv) makes or seeks to make a general assignment for the benefit of its creditors; or (v) applies for or has appointed a receiver, trustee, custodian, or similar agent appointed by order of any court of competent jurisdiction to take charge of or sell any material portion of its property or business.

18.4 Effect of Termination; Data Retention. Unless otherwise expressly provided in this Agreement:

(a) upon and after the termination or expiration of this Agreement for any or no reason:

(i) subject to the continuing rights, licenses, and obligations of either party expressly provided under this Agreement, including this Section 18.2, all authorizations and licenses granted hereunder will immediately terminate and the respective parties shall cease all activities concerning, including in the case of Mastercard, all use of, the expired or terminated SaaS Services and related Provider Materials, and, in the case of Provider, the Mastercard Data, and further Mastercard will: (A) complete all pending transactions and stop accepting new transactions through the SaaS Services; and (B) except as otherwise expressly permitted in any other then-valid agreements between the parties, discontinue use of any Provider trademarks and promptly remove any Provider references and logos from Mastercard's website;

(ii) Mastercard shall pay to Provider, subject to any credits accrued, under Section 3 (SaaS Support), all undisputed charges and amounts due and payable to Provider, if any, for SaaS Services actually performed under the terminated or expired Agreement through the date of expiration or termination.

(iii) in the event of termination by Mastercard for cause pursuant to Section 18.3, Provider shall repay, on a pro rata basis, all fees, expenses and other amounts paid in advance for any SaaS Services that Provider has not performed as of the effective date of such expiration or termination, as applicable, with respect to SaaS Services required to be performed under the terminated or expired Agreement;





(iv) Provider shall, at Mastercard's option and upon its written request: (i) promptly return or destroy and erase from all systems it directly or indirectly uses or controls (a) all originals and copies of all documents, materials, and other embodiments and expressions in any form or medium that contain, reflect, incorporate, or are based on Mastercard's Confidential Information, in whole or in part, or (b) solely such specific databases or other collections or articles of Mastercard's Confidential Information as Mastercard may request, and (ii) provide a written statement to Mastercard certifying that it has complied with the requirements of this Section 18.4(a)(iv);

(b) without limiting the generality of Section 18.4(a) and subject to the terms of Section 2.4, upon the termination or expiration of this Agreement, the Receiving Party shall, at the Disclosing Party's option and upon its written request: (i) promptly return or destroy and erase from all systems it directly or indirectly uses or controls, all originals and copies of all documents, materials, and other embodiments and expressions in any form or medium that contain, reflect, incorporate, or are based on the Disclosing Party's Confidential Information; and (ii) provide a notarized written statement to the Disclosing Party (signed by an officer or other individual authorized to bind the Recipient) certifying that it has complied with the requirements of this Section 18.4(b);

(c) notwithstanding any provisions of this Agreement to the contrary:

(i) the Receiving Party shall not be required to return, destroy, or erase any Disclosing Party Confidential Information to the extent that any applicable Law or other then-valid agreement between the Parties prevents it from doing so, in which case the Receiving Party shall retain, in its then current state, all such Confidential Information then within its right of control or possession in accordance with the confidentiality, security, and other requirements of this Agreement and perform its obligations under this Section 18.4 as soon as such Law no longer prevents it from doing so; and

(ii) Confidential Information stored in system-type media, such as for example system caches and email backup storage, need not be returned or destroyed, so long as the media: (i) are maintained in confidence; (ii) are not readily accessible to users; and (iii) are periodically overwritten or otherwise destroyed in the ordinary course of business.

(iii) If Receiving Party, for any reason, does not return or destroy particular copies of Disclosing Party Confidential Information; then the Receiving Party's use and/or disclosure of such information continues to be governed by the terms and conditions of this Agreement, notwithstanding any termination or expiration of the Agreement. For the avoidance of doubt this clause does not negate any obligation of the Receiving Party to return or destroy Disclosing Party Confidential Information.

(d) Upon Mastercard's termination of this Agreement for breach pursuant to Section 18.3(a), Mastercard shall have the right and option to continue to access and use the SaaS Services, in whole and in part, for a period not to exceed 180 days from the effective date of such termination pursuant to the terms and conditions of this Agreement, including without limitation the payment of any applicable fees.

18.5 Transition Assistance. If and only if requested by Mastercard in writing, on or before the termination or other expiration of the Agreement and at Provider's then-current rates for such assistance, Provider shall take all actions necessary to help facilitate a smooth, complete and orderly transition for the SaaS Services to, at Mastercard's option, either Mastercard or any replacement provider(s) designated by Mastercard, including, without limitation, (a) regular communication between the Provider SaaS Contact and the Mastercard SaaS Contact, (b) discussion in good faith of a plan for determining the nature and extent of Provider's transition obligations and for the implementation of the plan and transfer of the SaaS Services and Mastercard Data, (c) the provision of sufficient information, documentation and instruction to complete the transition, (d) promptly upon the request of Mastercard, the return to Mastercard in a standard format and media acceptable to Mastercard all of Mastercard Data stored within the SaaS Services and/or any backup or archival storage, and (e) extension, transfer and/or other arrangements with respect to licenses and any other agreements to complete the transition.



18.6 Survival. The provisions set forth in the following Sections, and any other right or obligation of the parties in this Agreement that, by its nature, should survive termination or expiration of this Agreement, will survive any expiration or termination of this Agreement: Section 1 (Definitions), Section 8 (Security), Section 13 (Privacy and Data Protection), Section 14 (Intellectual Property Rights), Section 15 (Representations and Warranties), Section 16 (Indemnification), Section 17 (Limitations of Liability), Section 18.4 (Effect of Termination; Data Privacy), Section 18.5 (Transition Assistance) and this Section 18.6 (Survival).

## 19. Insurance.

19.1 Required Coverage. At all times during the Term, Provider shall procure and maintain, at its sole cost and expense, all insurance coverage required by applicable Law, and in any event insurance coverage in the following types and amounts:

- (a) Statutory workers' compensation insurance (or other workplace injury insurance required by applicable local Law), and employer's liability insurance in an amount not less than \$1,000,000 or local currency equivalent;
- (b) A commercial general liability policy (including contractual liability and personal injury coverages) with aggregate limits of not less than \$2,000,000 or local currency equivalent;
- (c) Reserved.;
- (d) A professional liability policy with aggregate limits of not less than \$5,000,000 and that is kept in force during the term of the applicable SOW and for a period of at least one year after termination of that SOW;
- (e) A network security liability (cyber) insurance policy of not less than \$5,000,000, or not less than \$10,000,000 or local currency equivalent if Supplier processes Personal Data, and that is kept in force during the term of the applicable SOW and for a period of at least three years after termination of that SOW; and
- (f) An excess/umbrella liability policy with aggregate limits of not less than \$5,000,000 or local currency equivalent.

19.2 Policy Terms. All insurance policies required pursuant to this Section 19 shall:

- (a) be issued by insurance companies with a Best's Rating of no less than A;
- (b) Reserved;
- (c) Reserved;
- (d) Reserved.; and
- (e) Reserved.

19.3 Certificates of Insurance. Upon Mastercard's written request, Provider shall provide Mastercard with copies of the certificates of insurance and policy endorsements for all insurance coverage required by this Section 19. Provider shall not do anything to invalidate such insurance. Provider shall give 30 days' prior written notice to Mastercard of any cancellation, non-renewal, or material change in coverage, scope, or amount of any insurance policy required by or affecting the Mastercard's rights or remedies under this Agreement.

19.4 Non-Waiver. This Section 19 is not intended to and shall not be construed in any manner as to waive, restrict, or limit the liability of either party for any obligations under this Agreement (including any provisions hereof requiring a party to indemnify, defend and hold harmless the other party).



## 20. Miscellaneous.

20.1 Provider SaaS Contact. Provider shall appoint a Provider employee to serve as Provider's primary contact with respect to the SaaS Services, who will have the authority to act on behalf of Provider in matters pertaining to the SaaS Services (the "Provider SaaS Contact").

20.2 Mastercard SaaS Manager. Mastercard shall appoint and, in its reasonable discretion, replace, a Mastercard employee to serve as Mastercard's primary contact with respect to the SaaS Services, who will have the authority to act on behalf of Mastercard in matters pertaining to the SaaS Support.

20.3 Media and Apparatus Disposal. Prior to disposing of any media or apparatus that contains or may contain the Disclosing Party's Confidential Information, the Receiving Party shall ensure, using industry best practices, that all of Disclosing Party's Confidential Information contained by such media or in such apparatus has been completely deleted or otherwise destroyed.

20.4 Further Assurances. On a party's reasonable request, the other party shall, at the requesting party's sole cost and expense, execute and deliver all such documents and instruments, and take all such further actions, as may be necessary to give full effect to this Agreement.

20.5 Relationship of the Parties. The relationship between the parties is that of independent contractors. Nothing contained in this Agreement shall be construed as creating any agency, partnership, joint venture, or other form of joint enterprise, employment, or fiduciary relationship between the parties, and neither party shall have authority to contract for or bind the other party in any manner whatsoever.

20.6 Public Announcements. Neither party shall issue or release any announcement, statement, press release, or other publicity or marketing materials relating to this Agreement or otherwise use the other party's trademarks, service marks, trade names, logos, domain names, or other indicia of source, affiliation, or sponsorship, in each case, without the prior written consent of the other party.

20.7 Notices. Any notice, request, consent, claim, demand, waiver, or other communications under this Agreement have legal effect only if in writing and addressed to a party as follows (or to such other address or such other person that such party may designate from time to time in accordance with this Section 20.7):

If to Provider:	Spreedly, Inc. 300 Morris Street, Suite 400 Durham, NC 27701 Attention: Legal Department
If to Mastercard:	Mastercard International Incorporated 2000 Purchase Street, Purchase, NY 10577 USA Attention: Legal Department

Notices sent in accordance with this Section 20.7 will be deemed effectively given: (i) when received, if delivered by hand, with signed confirmation of receipt; (ii) when received, if sent by a nationally recognized overnight courier, signature required; and (iii) on the 3<sup>rd</sup> Business Day after the date mailed by certified or registered mail, return receipt requested, postage prepaid.



**20.8 Interpretation and Headings.** For purposes of this Agreement: (i) the words "include," "includes," and "including" are deemed to be followed by the words "without limitation"; (ii) the word "or" is not exclusive; (iii) the words "herein," "hereof," "hereby," "hereto," and "hereunder" refer to this Agreement as a whole; (iv) words denoting the singular have a comparable meaning when used in the plural, and vice-versa; and (v) words denoting any gender include all genders. Unless the context otherwise requires, references in this Agreement: (i) to Sections, exhibits, schedules, attachments, and appendices mean the Sections of, and exhibits, schedules, attachments, and appendices attached to, this Agreement; (ii) to an agreement, instrument, or other document means such agreement, instrument, or other document as amended, supplemented, and modified from time to time to the extent permitted by the provisions thereof; and (iii) to a statute means such statute as amended from time to time and includes any successor legislation thereto and any regulations promulgated thereunder. The parties intend this Agreement to be construed without regard to any presumption or rule requiring construction or interpretation against the party drafting an instrument or causing any instrument to be drafted. The exhibits, schedules, attachments, and appendices referred to herein are an integral part of this Agreement to the same extent as if they were set forth verbatim herein. The headings in this Agreement are for reference only and do not affect the interpretation of this Agreement.

**20.9 Entire Agreement.** This Agreement, and the attachments and exhibits, constitutes the sole and entire agreement of the parties with respect to the subject matter of this Agreement and supersedes all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of this Agreement, the related exhibits and attachments and the Agreement, the following order of precedence governs: (i) first, this Agreement, excluding its exhibits and attachments; (ii) second, the exhibits and attachments to this Agreement; and (iii) third, the Agreement. No browse-wrap, shrinkwrap, clickwrap, or other non-negotiated terms and conditions provided with any of the SaaS Services, Documentation, or other Provider Materials hereunder will constitute a part or amendment of this Agreement or be binding on Mastercard or any Authorized User for any purpose. All such other terms and conditions have no force and effect and are deemed rejected by Mastercard and the Authorized User, even if access to or use of such Service, Documentation, or other Provider Materials requires affirmative acceptance of such terms and conditions. Purchase orders will be for the sole purpose of defining quantities, prices and describing the SaaS Services to be provided under this Agreement and to this extent only are incorporated as a part of this Agreement and all other terms in purchase orders are rejected.

**20.10 Assignment.**

(a) Neither party shall assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance, under this Agreement, in each case whether voluntarily, involuntarily, by operation of law, or otherwise, without the other party's prior written consent, which consent shall not unreasonably be withheld or delayed .

(b) Except for Provider's engagement of Subcontractors pursuant to Section 11, Mastercard shall have the right to terminate this Agreement in its entirety pursuant to Section 18 if Provider delegates or otherwise transfers any of its obligations or performance hereunder, whether voluntarily, involuntarily, by operation of law, or otherwise, and no such delegation or other transfer will relieve Provider of any of such obligations or performance. The effects of any termination of this Agreement pursuant to this Section 20.10(b), including the resulting rights and obligations of the parties, shall be governed by Section 18.

(c) Any purported assignment, delegation, or transfer in violation of this Section 20.10 is void. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective permitted successors and assigns.

## 20.11 Force Majeure.

(a) No Breach or Default. Subject to Section 20.11(b), neither party shall be liable or responsible to the other party, or be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement, when and to the extent such failure or delay is caused by any criminal acts of third parties, epidemics and/or pandemics as designated by governing authorities, acts of God, flood, fire, earthquake or other natural disasters, explosion; war, invasion, hostilities (whether war is declared or not), terrorist threats or acts, riot, or other civil unrest; embargoes or blockades in effect on or after the date of this Agreement; national or regional emergency; or passage of Law or any action taken by a governmental or public authority, including imposing any export or import restriction, quota, or other restriction or prohibition; (each of the foregoing, a "Force Majeure Event"), in each case, provided that (i) such event is outside the reasonable control of the affected party; (ii) the affected party provides prompt notice to the other party, stating the period of time the occurrence is expected to continue; and (iii) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

(b) Termination. Each party may terminate this Agreement by written notice to the other party if the Force Majeure Event affecting the other party continues substantially uninterrupted for a period of at least twenty (20) consecutive Business Days. Unless a party terminates this Agreement pursuant to the preceding sentence, any date specifically designated for the other party's performance under this Agreement shall automatically be extended for a period up to the duration of the period the Force Majeure Event has a material adverse effect on such performance, provided that the other party uses diligent efforts to resume full performance hereunder and to minimize the effects of such Force Majeure Event.

(c) Exclusions; Non-Suspended Obligations. Notwithstanding the foregoing or any other provisions of this Agreement:

(i) in no event shall any of the following be considered a Force Majeure Event:

(A) shutdowns, disruptions, or malfunctions of the Provider Systems or Mastercard Systems as applicable or any of Provider's or Mastercard's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to the Provider Systems or Mastercard Systems as applicable; or

(B) the delay or failure of any Provider Personnel, or any contractor or agent of Mastercard, as applicable to perform any obligation of Provider or Mastercard hereunder unless such delay or failure to perform is itself by reason of a Force Majeure Event; and

(ii) reserved.

20.12 No Third-Party Beneficiaries. This Agreement is for the sole benefit of the parties hereto and their respective successors and permitted assigns and nothing herein, express or implied, is intended to or shall confer upon any other Person any legal or equitable right, benefit, or remedy of any nature whatsoever, under or by reason of this Agreement.

20.13 Amendment and Modification; Waiver. No amendment to or modification of this Agreement is effective unless it is in writing. No waiver by any party of any of the provisions hereof shall be effective unless explicitly set forth in writing and signed by the party so waiving. Except as otherwise set forth in this Agreement, no failure to exercise, or delay in exercising, any rights, remedy, power, or privilege arising from this Agreement will operate or be construed as a waiver thereof; nor shall any single or partial exercise of any right, remedy, power, or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

20.14 Severability. If any term or provision of this Agreement is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability shall not affect



any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal, or unenforceable, the parties hereto shall negotiate in good faith to modify this Agreement so as to effect the original intent of the parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

20.15 Governing Law; Submission to Jurisdiction. This Agreement is governed by and construed in accordance with the laws of New York without giving effect to any choice or conflict of law provision or rule that would require or permit the application of the laws of any jurisdiction other than those of New York. Any legal suit, action, or proceeding arising out of or related to this Agreement or the licenses granted hereunder shall be instituted in the courts of New York, and each party irrevocably submits to the jurisdiction of such courts in any such suit, action, or proceeding.

20.16 Equitable Relief. Each party acknowledges and agrees that a breach or threatened breach by such party of any of its obligations under Section 2.2 (SaaS Support), Section 2.3 (Use Restrictions), Section 3 (SaaS Service Availability), Section 8 (Security), Section 9 (Redundancy, Data Backup and Disaster Recovery), Section 10 (Compliance), Section 12 (Confidentiality), Section 13 (Privacy and Data Protection), and Section 14 (Intellectual Property Rights), would cause the other party irreparable harm for which monetary damages would not be an adequate remedy and agrees that, in the event of such breach or threatened breach, the other party will be entitled to seek equitable relief, including a restraining order, an injunction, specific performance, and any other relief that may be available from any court, without any requirement to post a bond or other security, or to prove actual damages or that monetary damages are not an adequate remedy. Such remedies are not exclusive and are in addition to all other remedies that may be available at law, in equity, or otherwise.

**21. Attachments and Exhibits.** The following attachments and exhibits are attached hereto and incorporated herein as an integral part of this Agreement:

21.1 Attachment A – Definitions

21.2 Exhibit A – SaaS Application (Description, Access, Use, Fees, Term and Pricing)

21.3 Exhibit B – SaaS Support

21.4 Exhibit C – SaaS Service Availability

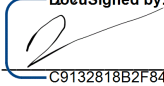
21.5 Exhibit D – Personal Data Protection Requirements

21.6 Counterparts. This Agreement may be executed in counterparts, each of which is deemed an original, but all of which together are deemed to be one and the same agreement. A signed copy of this Agreement delivered by facsimile, email, or other means of electronic transmission (including pdf or any electronic signature complying with the U.S. federal ESIGN Act of 2000, e.g., [www.docusign.com](http://www.docusign.com)) is deemed to have the same legal effect as delivery of an original signed copy of this Agreement.



IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date first above written.

**Spreedly, Inc.**

By:  \_\_\_\_\_  
C9132818B2F844A...

Name: Justin Benson

Title: CEO

**Mastercard International Incorporated**

By: Sapan Mandloi

Name: Sapan Mandloi

Title: SVP, Acceptance Solutions

## ATTACHMENT A

### DEFINITIONS

#### 1. Definitions.

1.1 "Action" means any claim, action, cause of action, demand, lawsuit, arbitration, inquiry, audit, notice of violation, proceeding, litigation, citation, summons, subpoena, or investigation of any nature, civil, criminal, administrative, regulatory, or other, whether at law, in equity, or otherwise.

1.2 "Affiliate" of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. The term "control" (including the terms "controlled by" and "under common control with") means the direct or indirect power to direct or cause the direction of the management and policies of a Person, whether through the ownership of voting securities, by contract, or otherwise.

1.3 "Allegedly Infringing Features" has the meaning set forth in Section 15.5.

1.4 "Authorized Users" means all Persons authorized by Mastercard to access and use the SaaS Services through Mastercard's account under this Agreement.

1.5 "Business Day" means a day other than a Saturday, Sunday, or other day on which commercial banks in the United States are authorized or required by Law to be closed for business.

1.6 "Confidential Information" has the meaning set forth in Section 11.1.

1.7 "Data Subjects" has the meaning set forth in Exhibit D.

1.8 "Disclosing Party" has the meaning set forth in Section 11.1.

1.9 "Documentation" means all then-current generally available electronic documentation relating to the SaaS Services that Provider makes available to Mastercard at <https://docs.spreadly.com>, including any such user manuals, operating manuals, and other instructions, specifications, documents, and materials available at such URL that describe any component, feature, requirement, or other aspect of the SaaS Services, including any functionality, testing, operation, or use thereof, as Provider may update from time-to-time in Provider's discretion.

1.10 "Fees" has the meaning set forth in Section 6.

1.11 "Force Majeure Event" has the meaning set forth in Section 19.11(a).

1.12 "Harmful Code" means any software, hardware, or other technologies, devices, or means, the purpose or effect of which is to: (a) permit unauthorized access to, or to destroy, disrupt, disable, distort, or otherwise harm or impede in any manner, any (i) computer, software, firmware, hardware, system, or network, or (ii) any application or function of any of the foregoing or the integrity, use, or Operation of any data thereby; or (b) prevent Mastercard or any Authorized User from accessing or using the SaaS Services or Provider Systems as intended by this Agreement, and includes any virus, bug, Trojan horse, worm, backdoor, or other malicious computer code and any time bomb or drop dead device.



1.13 "Indemnifying Party" has the meaning set forth in Section 15.1.

1.14 "Intellectual Property Rights" means any and all registered and unregistered rights granted, applied for, or otherwise now or hereafter in existence under or related to any patent, copyright, trademark, trade secret, database protection, or other intellectual property rights laws, and all similar or equivalent rights or forms of protection, in any part of the world.

1.15 "Law" means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree, or other requirement of any federal, state, local, or foreign government or political subdivision thereof, or any arbitrator, court, or tribunal of competent jurisdiction.

1.16 "Losses" means any and all losses, damages, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

1.17 "Mastercard Data" means any and all information, data, materials, works, expressions, or other content, including any that are (a) uploaded, submitted, posted, transferred, transmitted, or otherwise provided or made available by or on behalf of Mastercard or any Authorized User for Operating by or through the SaaS Services, or (b) collected, downloaded, or otherwise received by the SaaS Services from Mastercard or any Authorized User pursuant to this Agreement. Subject to the terms of Section 13.3 (Ownership of Provider Materials), all output, copies, reproductions, improvements, modifications, adaptations, translations, and other derivative works of, based on, derived from, or otherwise using any Mastercard Data are themselves also Mastercard Data. For the avoidance of doubt, Mastercard Data includes all User Data and Personal Data.

1.18 "Mastercard Modification" has the meaning set forth in Section 15.2(a).

1.19 "Mastercard SaaS Contact" has the meaning set forth in Section 19.2.

1.20 "Mastercard Systems" means the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems), and networks, of Mastercard or any of its designees.

1.21 "Operate" means to perform any operation or set of operations on any data, information, material, work, expression, or other content, including to (a) collect, receive, input, upload, download, record, reproduce, store, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate, or make other improvements or derivative works, (b) process, retrieve, output, consult, use, disseminate, transmit, submit, post, transfer, disclose, or otherwise provide or make available, or (c) block, erase, or destroy. "Operating" has a correlative meaning.

1.22 "PCI-DSS" means the Payment Card Industry Data Security Standard.

1.23 "Person" means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association, or other entity.

1.24 "Personal Data" has the meaning set forth in Exhibit D.

1.25 "Processes" has the meaning set forth in Exhibit D.

1.26 "Provider Materials" means the SaaS Services, Specifications, Documentation, and Provider Systems and any and all other information, data, documents, all devices, documents,



data, know-how, methods, processes, hardware, software, and other technologies and inventions, including any deliverables, technical or functional descriptions, requirements, plans, or reports, that are provided or used by Provider or any Subcontractor in connection with the SaaS Services or otherwise comprise or relate to the SaaS Services or Provider Systems.

1.27 "Provider Personnel" means all employees and agents of Provider, and all Subcontractors and all employees and agents of any Subcontractor, involved in the performance of SaaS Services.

1.28 "Provider Security Contact" has the meaning set forth in Section 7.6.

1.29 "Provider Service Contact" has the meaning set forth in Section 19.1.

1.30 "Provider Systems" has the meaning set forth in Section 7.2.

1.31 "Receiving Party" has the meaning set forth in Section 11.1.

1.32 "Regulator" has the meaning set forth in Section 7.4.

1.33 "Representatives" means, with respect to a party, that party's employees, officers, directors, consultants, agents, independent contractors, service providers, subcontractors and legal advisors and, with respect to Provider, Provider's Subcontractors, and, with respect to Mastercard, solely its independent contractors or service providers that are Authorized Users.

1.34 "SaaS Services" or "Services" has the meaning set forth in Section 2.

1.35 "SaaS Support" or "Support Services" has the meaning set forth in Section 2.2.

1.36 "Secondary Backup Facility" has the meaning set forth in Section 8.1.

1.37 "Specifications" means the specifications for the SaaS Services set forth in Exhibit A to this Agreement and the Documentation.

1.38 "Term" has the meaning set forth in Section 5.

1.39 "User Data" means any and all information reflecting the access or use of the SaaS Services by or on behalf of Mastercard or any Authorized User, including any end user profile-, visit-, session-, impression-, click through-, or click stream-data, and any statistical or other analysis, information, or data based on or derived from any of the foregoing.

1.40 "Indemnatee" has the meaning set forth in Section 15.1.

1.41 "Mastercard Indemnatee" has the meaning set forth in Section 15.2.

1.42 "Provider Indemnatee" has the meaning set forth in Section 15.3.

1.43 "Subcontractor" has the meaning set forth in Section 10.



## **Exhibit A**

### **SaaS Services and Fees**

#### Description of SaaS Application

Spreadly develops, markets and provides to its customers a web-based payments orchestration and tokenization platform, which includes Spreadly's proprietary API integration (collectively, the "Platform"), which enables its customers to validate, tokenize and vault credit cards (and other payment types) and then transact with one or more of the payment gateways that are integrated to the Platform and/or third-party payment method receivers that Spreadly supports, and, where applicable, automatically update expired or lost credit cards. Customer desires to acquire a subscription to access and use the Platform for the Permitted Use, subject to the terms and conditions set forth herein.

#### Term of SaaS Services

The term will be specified in an accompanying Order Form, subject to the Terms and Conditions of this Agreement. A sample of the Order Form is included on the next page.

#### Fees for the SaaS Services

All fees will be specified in an accompanying Order Form, subject to the Terms and Conditions of this Agreement. A sample of the Order Form is included on the next page.

**ORDER FORM [#]****Spreedly, Inc.**

300 Morris Street

Suite 400

Durham, NC 27701

**To:****Order Form Issued:****Customer Legal Name:****Offer Valid Until:****Tax ID:****Billing Address:****Sales Rep:**

This Order Form is entered into between the entity identified above as "Customer" and Spreedly, Inc. (each a "Party" and collectively, the "Parties") as of the last day it is signed (the "Order Form Effective Date") and is subject to the Agreement (defined below) which is hereby incorporated by reference. For purposes of this Order Form, "Agreement" means the enterprise services agreement (an "ESA") currently in force between the Parties.

In the event of any conflict between the terms of the Agreement and this Order Form, this Order Form will govern. Capitalized terms used but not defined in this Order Form have the meanings set forth in the Agreement or in the Documentation.

**1) Order Form Term****2) Platform Fees:****3) API Usage Fees:****4) Account Updater:****5) Payments:**

Customer may elect to pay all amounts due under this Agreement either by:

- (a) ACH payment or wire transfer to the following account:

Receiver: Webster Bank  
ABA/Routing #: 211170101  
SWIFT Code: WENAUS31  
Beneficiary: 0024760830  
Spreedly, Inc.  
300 Morris Street, Suite 400  
Durham, NC 27701  
USA

- (b) check delivered to the address specified in the relevant invoice.

**SAMPLE ONLY DO NOT SIGN**



## Exhibit B

### SaaS Support

#### SUPPORT OPTIONS

Our Support Services are designed to provide Spreadly customers and partners with world-class customer support from a global team committed to ensuring your success with our solutions.

Every Spreadly customer receives our base Business Support with 24x7 ticket submission and first response. Business Support ensures all customers have answers to product questions and troubleshooting guidance through email and our online ticketing system. Company has access to the Spreadly [Help Center and Knowledge Base](#) and to product [Documentation](#); and can enroll for status notifications at the Spreadly [API Status Page](#). Spreadly does not guarantee response, resolution, or uptime for the Business Support level.

In addition to our Business Support, three levels of additional support services are available under an annual subscription plan (a “Subscription Support Services Plan”).

**Advanced Support** includes the same services as Business Support and adds annual performance and business reviews and a leadership sponsor to supervise service delivery as well as guaranteed response and resolution times and an uptime SLA.

**Professional Support** includes the same services as Advanced Support and adds access to our Red Alert escalation system, implementation and project consulting during your onboarding phase, a technical account manager, gateway consultations, bi-annual business reviews, and quarterly performance check-ins.

**Premium Support** includes our Professional Support and adds critical case notification, shared Slack channel support, a dedicated Strategic Account Manager, monthly check-ins with your account team, executive sponsorship, consulting on implementation, project management and gateway integrations through a technical account manager.

Provider will be provided with the Subscription Support Services Plan set forth in the applicable Service Order.

#### CONTACTING SUPPORT

Contact Spreadly’s technical support by emailing [support@spreadly.com](mailto:support@spreadly.com) or by submitting a request via our [intake form](#) at [support.spreadly.com](https://support.spreadly.com).

Please include the following information in all support requests:

- The organization name associated with the Spreadly account
- A detailed summary of the issue or question
- Troubleshooting information (if applicable) including:
  - Gateway/Endpoint being used
  - Transaction, Payment Method and/or Gateway Token(s)
  - Link to Spreadly Dashboard
  - Error code received (Transaction Error or HTTP Status Code)
  - Steps to recreate issue
- Priority/Severity Level/Business Impact (see below for Severity Level definitions)

For customers on a Subscription Support Services Plan, critical case notification and phone support contact information



will be provided by your technical account manager.

### **Support Hours**

Spreadly's email support is available 24 hours a day, 7 days of the week, 365 days of the year. We may have reduced staffing during major holidays and we will advise through our [Support Page](#) if this is the case.

### **Expanded Support Regions**

When submitting a new support ticket, you can optionally provide us more information on your preferred region for support. This helps us assign support staff from your region and means you'll be more likely to receive replies during your selected business hours. If you choose a preferred region, the support hours for your support ticket are as follows for all 7 days of the week:

Europe, Middle East, Africa (EMEA): 8am-6pm EET Cape Town (UTC+2)

Americas (AMER): 8am-9pm ET US+Canada (UTC-4)

Asia Pacific (APAC): 8am-6pm SGT (UTC+8)

### **Self Help Resources**

Spreadly customers can take full advantage of our self-help tools available within our [Help Center](#), our [API Status Page](#), and from there you can find [product Documentation](#), [technical Documentation](#), [Knowledge Base](#) articles, and access technical guides.

### **RESPONSE AND RESOLUTION TIMES**

Spreadly is committed to rapid response of each request for support. All requests can be logged with Spreadly 24 hours-per-day, 7 days-per-week, 365 days-per-year via email at [support@spreadly.com](mailto:support@spreadly.com) or via our request [intake form](#) at [support.spreadly.com](https://support.spreadly.com).

Spreadly will use commercially reasonable efforts to promptly respond to each support request. Spreadly will provide continuous efforts (24x7x365) to resolve availability issues with the Transaction Processing Service until a workaround or resolution can be provided or until the incident can be downgraded to a lower priority.

### **CUSTOMER SATISFACTION**

Your satisfaction is important to Spreadly. After your case is resolved we may ask for your feedback via ZenDesk. Our support team regularly reviews responses, monitors customer satisfaction, and may contact customers where opportunities for improvement are identified.

We may also reach out via other mechanisms to inquire about your willingness to recommend Spreadly and our services. We appreciate your responses and value your feedback in helping us to continuously enhance our services.

### **SUBSCRIPTION SUPPORT LEVEL OBJECTIVES**

Subscription Support Services Plans come with guaranteed response and resolution times prioritized by the severity and the selected plan as presented in the following Table 1.

As used below, "Transaction Processing Service" means Spreadly's core API responsible for processing customer's payment transaction requests and does not include any beta features or non-payment transaction Spreadly services such as dashboard reporting.

Table 1

Severity	Definition	Speedily Acknowledgement Time			Resolution Time		
		Advanced	Professional	Premium	Advanced	Professional	Premium
Level 3 (Low)	Non-critical maintenance, configuration or troubleshooting requests not impacting Transaction Processing Service	Up to 72 hours	Up to 48 hours	Up to 24 hours	Next update	Next update	Next update
Level 2 (Serious)	Transaction Processing Service is severely impaired due to a Speedily issue	Up to 8 hours	Up to 4 hours	Up to 2 hours	Within 5 days	Within 3 days	Within 24 hours
Level 1 (Critical)	Transaction Processing Service is unavailable due to a Speedily issue	Up to 2 hours	Up to 1 hours	Up to 30 minutes	Within 2 days	Within 1 days	Within 8 hours

### Severity Level Definitions

Mastercard should indicate a priority when submitting a support ticket based on the severity level of their issue, however, Speedily may adjust the priority if the request no longer fits the original severity level definition. Speedily is not responsible for any failure to meet performance standards caused by the misassignment of the priority in a support request. Support tickets submitted without a priority will default to Severity Level 3.

### Severity levels are defined as follows:

**Level 1 (Critical):** Transaction Processing Service is unavailable due to an issue under Speedily's control and no work around exists.

**Level 2 (Serious):** Transaction Processing Service is severely impaired due to an issue under Speedily's control although a workaround may exist.

**Level 3 (Low):** Non-critical maintenance, configuration or troubleshooting requests not impacting the Transaction Processing Service. Includes product questions, feature requests, bugs, and development issues that require investigation by Speedily.

Before submitting a support request, please first check the Speedily [API Status Page](#) to see if the outage has already been reported or if your issue is due to scheduled maintenance.

### Support Escalation

Speedily's support team works to ensure that the appropriate resources are focused to ensure a timely resolution. If you are not satisfied with the progress of your support request, you can request an escalation. Subscription Support Services Plans come with a dedicated escalation path and Speedily management supervision to oversee support procedures and resource prioritization to solve your support request.

### Availability Commitments

Subscription Support Services Plans come with guaranteed service levels and service credits based on the selected support plan as presented in the following Table 2.





Table 2

Uptime Availability Commitment		
Advanced	Professional	Premium
99.90%	99.95%	99.99%

The following conditions will apply to the calculation of uptime availability commitments in Table 2:

“Availability” means that the services are up and running, accessible by Mastercard, without interruption or undue delay. Any downtime resulting from outages of third-party connections or utilities or other reasons beyond Spreadly’s control are excluded.

“Base Annual Fee” means the base annual fee set forth on the applicable Service Order for use of the Software Services, or if such fee is set forth on a monthly basis, then 12 times that monthly fee.

Downtime will begin to accrue as soon as the Transaction Processing Service is unavailable to Mastercard and continues until the Transaction Processing Service is restored.

Spreadly will give no less than 5 business days’ prior written notice to Mastercard of all scheduled maintenance. Spreadly will perform scheduled maintenance in such a way that any interruption of the Transaction Processing Service is kept to a minimum and will provide a maintenance window that will not exceed 60 minutes individually or 24 hours in the aggregate in any month.

If Spreadly fails to meet or exceed the applicable service levels for Mastercard’s given Subscription Support Services Plan, Spreadly will issue a credit to Mastercard in the following amounts based on the actual Availability during the applicable calendar month and the Mastercard’s selected Subscription Support Services Plan as presented in the following Table 3 and as further described below.

Table 3

Service Credits			
Monthly Availability Percentage			Credit
Advanced	Professional	Premium	
Less than 99.90% but greater than or equal to 99.80%	Less than 99.95% but greater than or equal to 99.90%	Less than 99.99% but greater than or equal to 99.95%	5% of 1/12th of Base Annual Fee
Less than 99.80% but greater than or equal to 99.70%	Less than 99.90% but greater than or equal to 99.80%	Less than 99.95% but greater than or equal to 99.80%	10% of 1/12th of Base Annual Fee
Less than 99.70% but greater than or equal to 99.60%	Less than 99.80% but greater than or equal to 99.70%	Less than 99.80% but greater than or equal to 99.70%	15% of 1/12th of Base Annual Fee
Less than 99.60%	Less than 99.70%	Less than 99.70%	20% of 1/12th of Base Annual Fee

Service Credits may not be redeemed for cash and will be applied to Mastercard's next applicable payment. The issuance of Service Credits is Spreadly's sole obligation and liability and Mastercard's sole remedy for any Service Level Failure.

Notwithstanding the foregoing, Spreadly has no obligation to issue any Service Credit unless Mastercard requests such Service Credit in writing within ten (10) business days of the Service Level Failure.

## CUSTOMER RESPONSIBILITIES

### Internal Help Desk

Mastercard must establish and maintain an internal help desk for its customers to act as first-line support. Your first-line support will at a minimum include:

1. a direct response to users with respect to inquiries concerning the performance, functionality or operation of the product,
2. a direct response to users with respect to problems or issues with the product,
3. a diagnosis of problems or issues of the product, and
4. a resolution of known problems or issues with the product with the help of technical knowledge base articles, repositories and experience.

If after reasonable efforts you are unable to diagnose or resolve the product problems or issues, and you have reason to believe the issue originates with Spreadly, please contact Spreadly for technical support by email at [support@spreadly.com](mailto:support@spreadly.com) or via our request [intake form](#) at [support.spreadly.com](https://support.spreadly.com)

## TECHNICAL LEADS

Mastercard will establish a technical lead to manage troubleshooting and establish best practices. Your technical leader will be the liaison between Company and Spreadly for technical support. These persons must have sufficient knowledge of the Spreadly product and your own environment in order to work with Spreadly to analyze and resolve Support Requests. They are responsible for engaging Spreadly technical support and monitoring the resolution of all Support Requests and escalated support issues.



Your technical or project lead should be assigned to monitor and administer your integration with the Spreadly product and should have experience in network and third-party application troubleshooting as well as browser knowledge & debugging skills.

Technical Leads are responsible for checking Spreadly's online resources (e.g. website [product Documentation](#), [technical Documentation](#) and [Knowledge Base](#)) and the Spreadly [Status Page](#) before submitting a Support Request.

## **PROTECTION OF API KEYS AND CREDENTIALS**

Mastercard must safeguard and protect unauthorized access to API keys and other credentials to access the Spreadly services. Spreadly will not issue credits or refunds for unauthorized use of Spreadly services through Company's issued API keys or other access credentials including compromises or abuse of Company's payment flows that subsequently interact with Spreadly services.

## **PRODUCT AND SUPPORT UPDATES**

### **Updates to Spreadly Services**

Spreadly may release Updates to its products and services pursuant to Spreadly's standard release cycle. Spreadly will provide Updates at no additional charge. Spreadly may make changes to its products and services (including, without limitation, the design, look and feel, functionality, content, material, information) that Spreadly deems necessary or useful to improve the products or services or for any other reason and at any time, provided however Spreadly will not make any changes that will materially adversely affect its features or functionality without prior notice to and a reasonable opportunity to review and/or transition.

Where practical, Spreadly will schedule such Updates during non-business hours. Notice to Mastercard will be sent via email or posted at the Spreadly [API Status Page](#).

### **Updates to these Support Policies**

Mastercard understands that these Support Services terms are subject to change at Spreadly's reasonable discretion upon posting to Spreadly's website at [www.spreadly.com/support-services-terms](http://www.spreadly.com/support-services-terms); provided that Spreadly will not materially degrade the Support Services provided to Mastercard during the Term.



## Exhibit D

### Privacy and Data Protection

1. **Privacy and Data Protection.** If Provider or any Provider Personnel receives, has access to or otherwise Processes Personal Data, Provider shall comply with the requirements of this Exhibit D. The Exhibit D regulates the Processing of Personal Data subject to Privacy and Data Protection Law for the Services provided in this Agreement.

2. **Data Processing Addendums:**

2.1. **EEA Data Processing Addendum.** Where the Provider Processes Personal Data of individuals subject to the General Data Protection Regulation (EU) 2016/679, Directive 2002/58/EC (as amended by Directive 2009/136/EC), or any other data protection law of the European Union, the European Economic Area, or their respective member states, Switzerland and the United Kingdom (“EEA Data Protection Law”), Provider will enter the terms set forth in Annex 3 of the Agreement for the purpose of complying with EEA Data Protection Law (the “EEA Data Processing Addendum”). The Parties agree that the terms set out below apply to the Processing of Personal Data subject to Privacy and Data Protection Laws, but which is not covered by EEA Data Processing Addendum. In case of conflict between this Exhibit and EEA Data Processing Addendum (Annex 3), the EEA Data Processing Addendum will prevail.

2.2. Reserved.

3. The terms used in this Exhibit have the meaning set forth in this Exhibit. Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement remain in full force and effect. Annexes 1, 2, 3, and 4 form an integral part of this Agreement.

4. **Definitions.** In this Exhibit D, the following definitions apply:

“**Business Purpose**” means the use of Personal Data for Mastercard or Provider’s operational purposes, or other notified purposes, provided that the use of Personal Data is reasonably necessary and proportionate to achieve the operational purpose for which the Personal Data was collected or processed or for another operational purpose that is compatible with the context in which the Personal Data was collected.

“**Data Protection Rights**” means all rights granted to individuals under Privacy and Data Protection Law, which may include – depending on applicable Privacy and Data Protection law – the right to know, the right of access, reproduction, supplement, rectification or erasure to or of Personal Data, the rights relating to data portability, restriction on Processing and objection to the Processing (including the right to withdraw consent) and the rights relating to automated decision-making.

“**Government Agency**” means any public and quasi-public authority that may have jurisdiction over Mastercard or Supplier to request for Personal Data.

“**Privacy and Data Protection Law**” means any law, statute, declaration, decree, legislation, enactment, order, ordinance, regulation, circular or rule (as amended and replaced from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which the Parties are subject, including but not limited to the California Consumer Privacy Act; the U.S. Gramm-Leach-Bliley Act; the Brazil General Data Protection Act; the South Africa Protection of Personal Information Act; the Personal Information Protection Law of the PRC and other PRC Laws relating to privacy and protection of Personal Information; Argentina Personal Data Protection Act; laws regulating unsolicited email, telephone, and text message communications; security breach notification laws; laws imposing minimum security requirements; laws requiring the secure disposal of records containing certain Personal Data; laws governing the portability and/or cross-border transfer of Personal Data; and all other similar international, federal, state, national, provincial, and local requirements; each as applicable.

“**Personal Data**” (or “Personal Information”) means any information relating to an identified or identifiable individual, including but not limited to contact information, demographic information, passport number, Social Security number or



other national identification number, bank account information, Primary Account Number and authentication information (e.g. identification codes, passwords).

**“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, or other unauthorized Processing of Personal Data transmitted, stored or otherwise Processed.

**“Process”** or **“Processing”** or **“Processing of Personal Data”** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**“Sell”** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s Personal Data by the business to another business or a third party for monetary or other valuable consideration.

**“Sensitive Data”** (or **“Sensitive Personal Data,”** which may be used interchangeably in this Agreement) means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person’s sex life or sexual orientation, as well as any other type of data that will be considered to be sensitive according to any Privacy and Data Protection Law.

**“Sub-Processor”** means the person (whether a natural person, a legal entity or any other organization) engaged by the Provider or any further sub-contractor to Process Personal Data on behalf of and under the instructions of Mastercard.

## 5. General Privacy and Data Protection.

### 5.1. Reserved.

5.2. **Compliance with Privacy and Data Protection Law.** Both Parties represent and warrant that they will comply with Privacy and Data Protection Law when Processing Personal Data in the context of the Services, and that they will perform their obligations under this Agreement in compliance with Privacy and Data Protection Law.

5.3. **Roles of the Parties.** Provider must only Process Personal Data on Mastercard’s behalf and instructions, or of Mastercard’s customers, for a Business Purpose as strictly necessary to provide the Services specified in, the Principal Agreement or as otherwise required by applicable Law. Mastercard, or the customers on whose behalf Mastercard may act, have the sole and exclusive authority to determine the purposes and means of the Processing of Personal Data that are disclosed to Provider. Provider is prohibited from Processing Personal Data for any other purpose, in particular from Selling any Personal Data and any data derived or inferred from Personal Data or from Processing Personal Data to develop or promote competing services.

5.4. **Instructions.** Mastercard’s instructions are documented in Annex 2 of Exhibit D to this Agreement, SOW and any applicable relevant document. Mastercard may issue additional instructions to Provider as it deems necessary to comply with Privacy and Data Protection Law. Provider must notify Mastercard when any law or legal requirement prevents Provider (1) from fulfilling its obligations under this Agreement or Privacy and Data Protection Law, and (2) from complying with the instructions received from Mastercard. In both situations, the Parties shall come to a mutual agreement to identify the solution to ensure compliance. Mastercard may in part or as a whole, as applicable, suspend the Processing of Personal Data by Provider, until such event resulting in non-compliance has ceased or rectified. If the Provider fail to correct the non-compliance, Mastercard is entitled to terminate any further Personal Data Processing and this Agreement, if doing so is required to comply with Privacy and Data Protection Law.

### 5.5. Provider Obligations. Provider agrees and warrants that it will:

5.5.1. where required under Privacy and Data Protection Law, appoint a data protection officer or similar function who will oversee the Processing of Personal Data conducted on behalf of Mastercard (**“Data Protection Officer”**).

5.5.2. immediately inform Mastercard, in writing, in relation to any Personal Data Processed in the context of the Services of: (i) any requests from individuals to exercise their Data Protection Rights; (ii) any request or complaint received from Mastercard’s customers, consumers, employees or any other individual; (iii) any question, complaint, investigation or other inquiries from regulators; and (iv) any public authority of whatever jurisdiction requesting disclosure of or information about the Personal Data that are Processed by Provider. Provider agrees and warrants that it will provide a copy of any such requests within 48 (forty-eight) hours (or a shorter period of time if required by Privacy





and Data Protection Law) of receipt by email to [privacyanddataprotection@mastercard.com](mailto:privacyanddataprotection@mastercard.com) and that it will respond to such requests only in accordance with Mastercard's prior written authorization ("**Notification Obligations**").

5.5.3. taking into account the nature of the Processing, cooperate with Mastercard to ensure compliance with Privacy and Data Protection Law, this Agreement, and Mastercard's customers' instructions, and to assist Mastercard in fulfilling its own obligations under Privacy and Data Protection Law and as applicable Mastercard's customer's instructions, including complying with individuals' requests to exercise their Data Protection Rights; verifying the identity of the individual making a request; replying to inquiries or complaints from individuals; replying to investigations and inquiries from competent Government Bodies; conducting data protection impact assessments and consultations and other interactions with competent Government Bodies. Where required by Mastercard, the Provider shall submit the Personal Data it holds on the individual through a portal designated by Mastercard in a format agreed and within the timeframe agreed. ("**Cooperation and Assistance**").

5.5.4. upon expiry or termination of this Agreement and/or relevant SOW, or if this Agreement or any relevant part of this Agreement authorizing Provider to Process Personal Data has been revoked, rescinded, or held void, invalid or unenforceable, or as set forth within the relevant SOW or the Agreement (such as Section 2.4 thereof), comply with Mastercard's request, and at Mastercard's sole option securely delete existing copies of the Personal Data or return the same to Mastercard without retention of any hard or soft copies, unless applicable local law requires storage of the Personal Data, in which case Provider will protect the confidentiality of the Personal Data, will not actively Process the Personal Data anymore, and will continue to comply with this Agreement ("**Termination**").

5.6. **Security of the Processing, Confidentiality, and Personal Data Breach Notification.** Provider agrees and warrants that:

5.6.1. it has implemented and maintains a comprehensive written information security program that complies with Privacy and Data Protection Law and Annex 1 of Exhibit D to this Agreement, including appropriate technical, operational and organizational measures to protect from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access or other unauthorized Processing of Personal Data transmitted, stored or otherwise Processed ("**Information Security Program**"). Provider's Information Security Program shall comply with the applicable Payment Card Industry Data Security Standards to the extent Provider Processes payment card information.

5.6.2. Provider's Information Security Program must, among other things, include (1) regular assessment, testing or otherwise monitoring of the effectiveness of Provider's information safeguards, (2) controls to ensure that Primary Account Number (PAN) is encrypted both at rest and in transit, (3) a process for maintaining and regularly reviewing logs and periodic password renewal and (4) the application of multi-factor authentication (where appropriate) in accordance with the controls referenced in Annex 1 of Exhibit D to this Agreement. Provider undertakes to notify Mastercard of any technical, operational, organizational or other change having a material impact on the security, confidentiality or protection of Personal Data, no less than 15 (fifteen) working days prior to implementing any such change. Provider agrees to submit its Information Security Program in the course of the Data Protection and Security Audit as defined under Section 5.9 of this Exhibit D.

5.6.3. Provider must take steps to ensure that any person acting under its authority, including any Sub-Processor, who has access to Personal Data is only granted access to Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only Processes Personal Data in accordance with this Agreement and Mastercard's instructions ("**Confidentiality**").

5.6.4. Provider will inform Mastercard of any Personal Data Breach i) by contacting the Mastercard Security Operations Center at +1-636-722-3600 or 1-800-358-3060 (US toll-free number) and /or; ii) in writing to [SOC@mastercard.com](mailto:SOC@mastercard.com), [TPRM@mastercard.com](mailto:TPRM@mastercard.com) and the account manager or person they are doing business with inside of Mastercard under this Agreement, without undue delay, and no later than 24 (twenty-four) hours (or a shorter period of time if required by Privacy and Data Protection Law) after having become aware of a Personal Data Breach. Such notice shall summarize in reasonable detail the effect on Mastercard, if known, of the Personal Data Breach, the corrective action taken and to be taken by Provider and/or its Sub-Processor and other information as required by Privacy and Data Protection Law. Provider shall, and shall cause, its Sub-Processors (if any) to promptly take all necessary and advisable corrective actions and fully cooperate with Mastercard in all reasonable and lawful efforts to prevent, mitigate, investigate or rectify such Personal Data Breach, including in relation to any forensic investigation or related audit requested by Mastercard. Mastercard is free to use the forensic investigator of its choice. Provider will be responsible for the costs and expenses associated with the performance of its and its Sub-Processor's obligations described in this



paragraph , unless the Personal Data Breach is caused by the acts or omissions of Mastercard. Provider will assist Mastercard in complying with its own obligations or with Mastercard's customers' obligations under Privacy and Data Protection Law to notify of a Personal Data Breach. In case of conflict between this section 5.6.4 and section 5.9, this section 5.6.4 will prevail.

5.6.5. Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, Provider must obtain the written approval of Mastercard prior to the publication or communication of any filings, communications, notices, press releases or reports related to any Personal Data Breach that expressly mention Mastercard or its Affiliates. Provider acknowledges and agrees that a violation of Section 5.6, or the occurrence of any Personal Data Breach, may cause immediate and irreparable harm to Mastercard for which money damages may not constitute an adequate remedy. Therefore, Provider agrees that Mastercard may seek injunctive or other equitable relief for any such violation or incident, in addition to its remedies at law, without proof of actual damages ("**Personal Data Breaches**").

## 5.7. International Data Transfers

5.7.1. Provider agrees and warrants that it will not transfer Personal Data or allow access to Personal Data from outside the countries listed below, except if it obtains the prior explicit written consent of Mastercard.

List of jurisdictions to which Personal Data are transferred or from which Personal Data are accessed
United States and any other jurisdictions in which Provider and its Sub-processors throughout the term of the Agreement operate their businesses

5.7.2. If Provider is authorized under this Agreement to transfer Personal Data, it must ensure that the Personal Data will be protected with the same level of protection as provided by this Agreement and, where required, implement any data transfer mechanism required by Privacy and Data Protection Law.

5.7.3. Provider represents and warrants that it is not subject to a requirement under applicable law that would prevent Provider from transferring Personal Data in accordance with this Agreement.

5.7.4. If the Processing of Personal Data of Data Subjects is subject to the Argentina Personal Data Protection Act 25.326 (PDPA) (Ley de Protección de los Datos Personales) is involved, Provider agrees to comply with the obligations of a data importer as set out in the model contract titled Contrato Modelo de Transferencia Internacional de Datos Personales con Motivo de Prestación de Servicios adopted by the Data Protection Agency of the Republic of Argentina under Disposition 60 — E/2016 (the 'Argentinian SCCs') for the transfer of Personal Data to data processors established in third countries.

(a) Provider acknowledges that each Data Exporter in the Republic of Argentina will be a Data Controller. In particular, and without limiting the above obligation:

- (i) Provider agrees to grant third party beneficiary rights to data subjects, as set out in Clause 3 of the Argentinian SCCs, provided that Supplier's liability shall be limited to its own processing operations; and
- (ii) Provider agrees that its obligations under the Argentinian SCCs shall be governed by the laws of the Republic of Argentina in which the Data Exporter(s) are established; and
- (iii) the details of the appendices applicable to the Argentinian SCCs are set out in Annex 2 of this Agreement insofar as it relates to Data Processor purposes.

(b) For the purposes of Annex A to the Argentinian SCCs, the data exporter is a Mastercard entity; the data importer is Provider and details about the data subjects, categories of data, processing operations and security measures are as set out in Annex 1 and Annex 2 of Exhibit D from this Agreement.

5.7.5. If the Processing of Personal Data of Data Subjects is subject to the Argentina Personal Data Protection Act 25.326 (PDPA) (Ley de Protección de los Datos Personales), Provider shall neither apply nor use the exported Personal Information , as defined under the Argentina Personal Data Protection Act for any purpose other than the [ones specified as 'Processor' purposes in Annex 2 of Exhibit D from this nor shall the Provider, except as permitted in this Agreement, communicate to other parties such exported Personal Information, even for storage purposes. Once the corresponding



contractual obligations have been performed, the exported Personal Information processed must be destroyed, except where there is an express authorization given by the person for account of whom such services are rendered, by reason of a possibility of the exported Personal Information being used for future services, in which case the exported Personal Information may be stored under due security conditions for a maximum term of up to two years. The Parties agree to adopt confidentiality measures to protect the exported Personal Information following section 9 of the Data Protection Act and its Regulations. Provider shall process the exported Personal Information following only instructions from the Data Controller.

#### 5.8. Data Disclosures

Provider must not share, transfer, transmit, disclose or otherwise provide access to or make available any Personal Data to any person (whether a natural person, legal entity or any other organization other than those listed below or as otherwise authorized by Mastercard in writing in advance.

Name and address of Sub-Processor	Location(s) where Personal Data Are stored or from which Personal Data Are Accessed by the Sub-Processor	Description of service
Auth0 10800 NE 8th Street Suite 700 Bellevue, WA 98004	USA	Speedly direct customer portal login
AWS 410 Terry Avenue North, Seattle, WA 98109- 5210	USA	Cloud data processing
FiveTran 1221 Broadway Floor 20 Oakland, CA 94612	USA	SaaS data integration service
FIS/Global/Vantiv The Walbrook Building, 25 Walbrook, London, EC4N 8AF, United Kingdom	UK	Account updater service
Looker 1600 Amphitheatre Parkway Mountain View, CA 94043	USA	Business intelligence and visualization for analytics
Slack 500 Howard Street San Francisco, CA 94105	USA	Private customer communication
Snowflake	USA	Data warehousing



106 East Babcock Street, Suite 3A, Bozeman, Montana 59715		
Zendesk 1019 Market Street San Francisco, CA 94103	USA	Inbound customer support and help center/community

5.8.1. Without prejudice to Section 5.8.1., Provider must ensure that, in each instance in which it engages a Sub-Processor to Process Personal Data on Mastercard's behalf it must enter into a binding written agreement with the Sub-Processor with the same security and privacy and data protection obligations that apply to Provider under this Agreement and Privacy and Data Protection Law.

5.8.2. Prior to any sub-processing, Provider must carry out adequate due diligence to ensure that the Sub-Processor is capable of Processing Personal Data with at least the same level of protection for the Processing of Personal Data and of complying with the same security and privacy and data protection obligations as are imposed on Provider under this Agreement and Privacy and Data Protection Law.

5.8.3. Provider must inform Mastercard in writing at least 60 calendar days prior to any change to the role or status of the Sub-Processor.

Provider will remain fully liable towards Mastercard for the performance by each Sub-Processor of any and all Sub-Processor obligations under such agreement between Supplier and such Sub-Processor and any other act or omission by such Sub-Processor in relation to the Processing of Personal Data thereunder.

5.8.4. Mastercard and Provider acknowledge that Mastercard may engage a third-party payment gateway service provider and/or a third-party payment processing service provider to facilitate payment transactions in connection with the Agreement ("Third Party Gateway or Payment Service"). Any such Third Party Gateway or Payment Service engaged by the Mastercard shall not be deemed a Sub-processor of the Provider for purposes of this Exhibit. Accordingly, nothing in this Exhibit obligates Provider to enter into a data protection agreement with such Third Party Gateway or Payment Service or to be responsible or liable for such Third Party Gateway or Payment Provider's acts or omissions. Third Party Gateway or Payment Service or to be responsible or liable for such Third Party Gateway or Payment Provider's acts or omissions.

## 5.9. Data Protection and Data Security Audit

5.9.1. Upon request by Mastercard and subject to Mastercard's reasonable discretion, Provider allows Mastercard or, as applicable, Mastercard's customers, or an inspection body composed of independent members selected by Mastercard or Mastercard's customers, to audit and review Provider's Information Security Program, data processing facilities, and data protection compliance program to verify compliance with this Agreement, Privacy and Data Protection Law, and as applicable with Mastercard's customers' instructions or own obligations under the Privacy and Data Protection Law; provided that such audit will not take place more than once annually. ("**Data Protection and Security Audit**").

5.9.2. The Parties will mutually agree upon the scope, timing, and duration of the Data Protection and Security Audit. The Data Protection and Security Audit may be conducted by an independent third-party auditor designated by Mastercard, in which case Provider will make available to Mastercard, or where applicable Mastercard's customer, the result of the The Data Protection and Security Audit.

5.9.3. Provider agrees to fully cooperate with such Data Protection and Security Audit and implement all commercially reasonable changes to its Information Security Program, data processing facilities and data protection compliance program that, as a result of the Data Protection and Security Audit, are required to ensure Provider's compliance with this Agreement, Privacy and Data Protection Law, and as applicable with Mastercard's customer's instructions or own obligations under the Privacy and Data Protection Law. Provider's failure to allow or cooperate to any Data Protection and Security Audit or implement any such required changes to its information security program, data Processing facilities or data protection compliance program within a reasonable period of time (at least 30 days)



after receipt of such audit results shall entitle Mastercard to suspend the Processing of Personal Data by Provider, and to terminate any further Personal Data Processing and terminate the Agreement, if doing so is reasonably required or expected by Mastercard to comply with this Agreement, Privacy and Data Protection Law, and as applicable with Mastercard's customers' instructions or own obligations under the Privacy and Data Protection Law.

5.9.4. Upon request by Mastercard, Provider must provide a certification of compliance with applicable Privacy and Data Protection Law and information security standards, such as the annual Payment Card Industry Data Security Standards (PCI-DSS) and SOC2 Type II certifications, as applicable.

5.10. **Liability.** The Parties agree that:

5.10.1. Provider is fully liable to Mastercard for any violations of Privacy and Data Protection Law or of this Agreement by Provider or any of its Sub-Processors that impact the Processing of Personal Data covered under this Agreement.

5.10.2. If Mastercard has paid, has been imposed an obligation to pay, or has otherwise been held liable for payment of any compensation, damages or fines to any individual, competent government body or other third party due to any violations or breaches by Supplier or any of its Sub-Processors of the Privacy and Data Protection Law, Mastercard is entitled to claim back from Provider that part of the compensation, damages or fines, corresponding to Provider's part of responsibility for the compensation, damages or fines.



## **ANNEX 1: SECURITY MEASURES**

### **TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Unless Mastercard has provided Provider an exception in writing, Provider will, as a minimum, implement the security measures as set forth herein. These security measures must be implemented in addition to any standards, certifications or audit requirements that Provider adheres to (or has been certified to) with regard to the Services or Deliverables, including but not limited to the Payment Card Industry Data Security Standards (PCI-DSS) and ISO certifications, as applicable.

THIRD PARTY RISK MANAGEMENT

# Security Requirements for Suppliers and Business Partners

20 MAY 2020



Security Requirement for Suppliers and Business Partners

This document defines the security controls that Mastercard expects suppliers and other third parties to implement if they have access to, store, or process Mastercard’s information resources (including Personal Information). These controls must be implemented in addition to any legal, regulatory, or industry-defined standards or audit / certification requirements that may be applicable (e.g., the Payment Card Industry Data Security Standard).

If you have questions, visit [procurement.mastercard.com](https://procurement.mastercard.com) or contact our Third Party Risk Management team at [TPRM@mastercard.com](mailto:TPRM@mastercard.com). Additional resources regarding cybersecurity are also available at [mastercard.com](https://mastercard.com).



If you have experienced, or suspect you may have experienced, a security incident or potential data breach that could potentially affect Mastercard, you must **immediately** call Mastercard’s global security operations center at +1 636 722 3600, and e-mail [TPRM@mastercard.com](mailto:TPRM@mastercard.com) and your Mastercard relationship contact.

This document applies to companies working with Mastercard as a supplier, strategic partner, or other non-customer relationship. Requirements for Mastercard’s licensed customers and their service providers are different; more information is available on [mastercard.com](https://mastercard.com).

Contents

1.0 Information Security Organization ..... 3

2.0 Risk Management..... 3

3.0 Personnel Security ..... 4

4.0 Physical Security ..... 5

5.0 Operations Management..... 5

6.0 Security Defense, Monitoring, and Response ..... 7

7.0 Securing Data in Transit and at Rest..... 7

8.0 Access Control ..... 8

9.0 Network Security..... 10

10.0 Third Party Services ..... 10

11.0 Application Management ..... 11

12.0 Enterprise Resilience (Business Continuity) ..... 11

13.0 Compliance..... 12

14.0 Information Technology Management..... 12

15.0 IT Incident Management..... 13

16.0 Privacy..... 13

17.0 Audit Management..... 13

Glossary of Terms ..... 14



## Security Requirement for Suppliers and Business Partners

### 1.0 Information Security Organization

1. The organization must appoint a Chief Security Officer (CSO) responsible for establishing, implementing, maintaining and enforcing the organization's Information Security department program.
2. Formal information security functions and responsibilities must be defined and implemented into an Information Security department
3. The Information Security department develops and maintains a comprehensive security strategy.
4. Comprehensive security policies, standards and procedures are developed and maintained by the Information Security department.
5. Reviews are completed annually on the information security department policies and procedures.
6. An Internal Audit committee or similar separate function must review the information security policy with the Chief Security Officer at least annually.
7. Ownership for all information systems or resources must be designated. Owners are responsible for oversight and alignment with organization policies and standards.
8. All organizational information systems and resources must have a designated resource administrator responsible for protecting and maintaining those assets.
9. The organization must designate teams composed of business, information technology, and security personnel whose mission is to address security incidents and vulnerabilities on organization-owned or leased information resources.
10. The organization must evaluate its security awareness training program for input for future curriculum definition and training sessions.
11. The organization's Information Security department must provide organization personnel, third party consultants, and contractors with annual information security department awareness training.
12. The organization must designate a person responsible for privacy and data protection compliance (e.g., a Chief Privacy Officer) who is appointed and works with the Information Security department to ensure that the organization is in compliance with national and international legal and regulatory requirements that relate to data protection and privacy.

### 2.0 Risk Management

1. The organization must establish risk assessment roles and responsibilities.
2. The organization must ensure that all information resources are inventoried and operate in a secure manner so that they may be included as part of the organizational risk management program.
3. The organization must designate security requirements for classifying information resources which specifies procedures based on classification delegating the handling, retention, labeling, copying, distributing, storing, transporting, disposing and printing.
4. The organization's personnel must handle any sensitive information (including Personal Information) of its clients (including Mastercard) with integrity and discretion and in accordance with all applicable laws. Information that is obtained by the organization, or through one of the organization's clients is considered 'sensitive'. Personnel, third party consultants, contractors and vendors are required to adhere to the organization's defined guidelines with respect to the handling of information in hard copy form.
5. The organization must adopt a risk mitigation strategy which may involve accepting the identified risk, transferring the risk to third parties by purchasing insurance or contractual agreements or choose to shut down the risk prone services if they are not critical for organization existence.



## Security Requirement for Suppliers and Business Partners

6. The organization must ensure information systems implement cryptographic mechanisms to prevent unauthorized disclosure and modification of sensitive information (including Personal Information). Security policies and operational procedures are in place for protecting sensitive information and are documented, in use, and known to all affected parties.
7. The organization employs automated mechanisms no less than quarterly to update the list of vulnerabilities scanned, track the continued presence of security vulnerabilities on information systems and identify when new vulnerabilities are identified and reported.
8. The organization must establish processes and procedures for assets on its network to include Industrial Control Systems (ICS).
9. The organization must perform vulnerability and risk assessment for assets on its network to include Industrial Control System (ICS) components.
10. Workstations must be protected with a standard, secure configuration including both client/desktop controls and individual application controls, e.g. browser configurations.
11. Removable media drives must be specifically approved and based on business requirements. Removable media containing organization information (e.g. CDs, USB sticks, floppy disk, tapes, removable hard drives, DVDs and printed media) must be registered with a designated owner and scanned automatically / manually for potential threats.
12. Access to offsite sensitive media storage areas must be restricted to authorized individuals. Transfer must be completed using mechanisms with appropriate security from the source to destination such as utilizing authorized courier with tracking mechanism, confirmation of receipt, encryption and/or tamper evident packaging, and chain of custody as appropriate with the data classification of the information.
13. The organization must establish processes and procedures for disposing information specific to electronic media.
14. The organization must establish processes and procedures for storing and destruction of information in hard copy form.

## 3.0 Personnel Security

1. The Human Resource Department must subject employment candidates (including contractors and temporary staff) to pre-employment screening, which includes a formal background investigation, to the extent permitted by applicable laws. If contractors or temporary staff are provided through an agency, the contract with the agency must clearly specify the agency's responsibilities for screening and the notification they need to follow if screening has not been completed or if the results give cause for doubt or concern.
2. The organization employees and contingent staff sign a non-disclosure or confidentiality agreement prior to accessing organization facilities or information.
3. The organization's personnel sign an employment contract that clearly states their responsibilities related to information security.
4. The organization must develop and document an acceptable use & responsibility standard relative to information security.
5. Disciplinary action must be consistent with the severity of the incident, as determined by an investigation.
6. The organization must establish processes and procedures for revoking system access.





## Security Requirement for Suppliers and Business Partners

### 4.0 Physical Security

1. For all organization facilities, a secure physical perimeter must be established.
2. Access to organization facilities is appropriately restricted to authorized personnel.
3. When constructing or selecting computing facilities, organization defined environmental concerns must be considered as part of a site risk assessment.
4. Physical security controls are in place over information assets and systems at all organization computing facilities to address security threats, environmental hazards and disaster recovery requirements.
5. Electronic access control systems are implemented to prevent unauthorized access to computer facilities. The system records all entries and produces audit trails.
6. Access logs, whether maintained in electronic or printed form, are reviewed on a regular basis relative to the classification of assets at that location.
7. Physical intrusion detection devices must be implemented in organization facilities.
8. The organization must develop and document procedures for security guards or other personnel designated with protecting the physical security environment.
9. Recordings / videos from cameras used to monitor sensitive areas of computing facilities are audited.
10. The organization must establish processes and procedures for working in secured areas.
11. Areas containing sensitive information (including Personal Information) resources are secured when unattended and at the end of each business day.
12. Computing systems processing highly sensitive data (such as Sensitive Personal Information) must be physically and/or logically isolated to reduce the risk of unauthorized access.
13. The organization has developed, documented and implemented policies and procedures to protect sensitive information (including Personal Information) stored on mobile computing devices.
14. The organization must establish processes and procedures for guidelines for protecting off-site equipment.

### 5.0 Operations Management

1. The Information Technology function is defined and responsible for establishing and maintaining operational control procedures. These operational control procedures are used by resource administrators when installing or maintaining information resources of the organization. Access to the operational control procedures is made available only to authorized personnel.
2. All organization information resources are established and maintained in accordance with information technology standard builds and the applicable platform-specific security baseline.
3. The organization must establish processes and procedures to disable, restrict, or secure unnecessary functions, services, utilities, and commands.
4. Platform and application administrators are responsible for installing available patches on the information resources under their control in a timely fashion. Critical security patches relevant to the protection of sensitive information (including Personal Information, such as cardholder information) must be installed within one month of release.
5. The organization network architecture is clearly documented to facilitate identification of components during network analysis operations and incident investigations.
6. Vulnerability remediation efforts, including patch implementations, must be coordinated and processed according to the corporate change management process, including meeting all testing and/or documentation requirements.
7. The organization must establish processes and procedures for deploying Off-The-Shelf software (COTS).



## Security Requirement for Suppliers and Business Partners

8. The organization must have established processes and procedures for installation and use of vendor software.
9. System lifecycle and change management processes and controls are established.
10. The organization has established activities that are to be logged by information resources. These must include, at the minimum, the following activities: application start/stop times, system boot/restart times, system configuration changes, abnormal system events, confirmation that files and output were handled correctly and critical file changes.
11. The organization must implement automated monitoring and alerting strategies to generate warning when allocated audit record storage volume nears or reaches the defined maximum audit record storage capacity.
12. Development, test and production environments must be separated physically, or at a minimum logically, to reduce the risk of accidental change or unauthorized access to production software and data.
13. The organization must establish processes and procedures for separation of duties between development/test and production environments.
14. The IT Operations Manager must establish a change control process for the change of Backup and Restore documentation. The change control process must include proper authorization and business documentation for all changes to the Backup and Restore documentation. The IT Operations department must deploy appropriate technologies to manage backup and restore tasks.
15. The organization must have designated network personnel to provide operational technical support for all network related issues.
16. Management must establish procedures for timely monitoring of the clearance of customer queries. Long outstanding queries must be investigated and acted upon.
17. The Information Security department and Information Technology department are responsible for developing, implementing, maintaining and communicating a malicious code control program to limit the introduction and spread of computer viruses, worms, Trojan Horses, spam, spyware, denial of service attacks, etc., within the organization computing environments. They are also responsible for reviewing and selecting approved virus detection software to be used by organization.
18. The organization must update anti-malware software once a week to ensure system scans can identify all known viruses.
19. All organization computing devices that are commonly known to be affected by malware have approved virus detection or integrity software installed and active.
20. Virus scans or integrity checks must be completed prior to the first use of each executable file that is brought into the organization computing environment.
21. Virus scans or integrity checks must be performed prior to any removable media being sent outside organization.
22. The organization must establish processes and procedures for virus detection software configuration.
23. The organization provides centralized SPAM protection as part of its email infrastructure.
24. The organization has a defined operations department which is responsible for developing, documenting and implementing backup schedules, outlining the type of backup, interval, storage location and the number of copies of information resources requested to be backed up by the resource owners.
25. Information resources are backed up and can be recovered in a timely manner.
26. The organization must establish processes and procedures for backup classifications and associated schedules.
27. The organization must establish processes and procedures for information system backups.
28. The organization's data is stored offsite based on the data's level of classification and policy governing the backup of classified information.



## Security Requirement for Suppliers and Business Partners

29. The organization has a defined record retention schedule which documents types of records and relevant retention for a period commensurate with the record's usefulness within organization legal and regulatory requirements and other organization directives.
30. The organization must establish a record retention schedule that supports regulatory requirements.
31. The organization employees, third party contractors and vendors must adhere to all copyright laws and packaged software license agreements.
32. Configuration management and software standards are established.

## 6.0 Security Defense, Monitoring, and Response

1. The organization must employ centrally managed automated tools to reassesses the integrity of software and information by performing daily integrity scans of the information system, detect unauthorized changes to the software and information and notify the designated individuals upon discovering discrepancies during integrity verification. (e.g. file integrity monitoring tools).
2. The organization must continuously monitor network/system activity to ensure secure operation and alert the designated individuals of any anomalies.
3. The organization ensures boundary protection processes and procedures are established.
4. Organization systems are configured to log to centralized systems.
5. The organization ensures that all its information resources are subject to audit logging, which is continuous and protected from unauthorized access, modification and destruction. Audit logs must be stored for defined periods of time for audit trail analysis and retained for at least one year (twelve months).
6. Intrusion Detection Systems/Intrusion Protection Systems (IDS/IPS) must be implemented to protect the organization from threats, vulnerabilities and malicious code.
7. The Information Security department is responsible for developing, implementing, maintaining and communicating a security incident reporting process and related procedures that includes cardholder information.
8. A designated Incident Response Team must be established and held responsible for documenting information security incidents.
9. Incident team roles and responsibilities are established to include appropriate 'authority to operate' rights while responding to incidents
10. The organization must develop an incident response procedure for all security and privacy related incidents involving a 'breach of security' to Personal Information.

## 7.0 Securing Data in Transit and at Rest

1. Encryption use standards are established to protect sensitive information (including Personal Information) when being transmitted and/or stored on organization information resources. Primary Account Number (PAN) and other Personal Information must be encrypted both in rest and in transit.
2. Employees responsible for implementing encryption technologies must sign a statement acknowledging their responsibilities. Employees must not install any encryption software not validated and approved by the Information Security department.
3. Connections to wireless access points must be authenticated over an industry best practice, strong encrypted channel.
4. Information classified as 'Confidential' or higher, including Personal Information, such as cardholder information, must not be sent over the Internet, via Remote Access or transmitted over public or external networks unless the transition utilizes a strong encryption method or protocol as designated by NIST.



## Security Requirement for Suppliers and Business Partners

5. The organization must have a policy governing appropriate web usage. All web browsing activities by organization personnel are intercepted by a web proxy which authenticates the system user and logs attributes necessary to identify malicious or unapproved activity.

### 8.0 Access Control

1. The organization must manage information system accounts by implementing automated centralized control of user access and administrator functions.
2. The performance of critical functions is appropriately segregated and monitored.
3. The organization must establish processes and procedures for periodic review of general access accounts.
4. The Human Resources department is responsible for reporting changes in user's duties or employment status to resource administrators and access management personnel to ensure entitlements are updated in a timely manner.
5. Controls and procedures are in place to revoke unnecessary access privileges.
6. Access is assigned and periodically reviewed to ensure least privilege access is granted.
7. The organization must complete an annual review and certification of logical access accounts.
8. All users with access to organization's information resources must utilize User IDs that are specifically assigned to them.
9. User IDs must be unique across all systems and forever connected with the single user to whom it has been assigned. The use of Primary Account Number (PAN) as a unique ID must be prohibited, unless this is explicitly authorized by Mastercard.
10. User IDs are not utilized by anyone except the individual to whom the IDs have been issued. Users are responsible for all activity performed with their personal User IDs.
11. Controls are in place to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
12. All default, pre-set, or temporary passwords and accounts assigned internally must be set to a unique value per user and changed immediately after first use. Vendor-supplied defaults must be changed prior to installation of third party software on the network, which must be disabled if not necessary for business purposes.
13. Access control systems must be implemented that are tamper proof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.
14. The organization must establish processes and procedures for password strength requirements in line with applicable regulatory or industry guidelines.
15. Users must choose easily remembered passwords that are, at the same time, difficult for unauthorized parties to brute force. Security must provide guidance to users to aid in creating passwords such as: Stringing several words together (the resulting passwords are also known as passphrases), shifting a word up, down, left or right one row on the keyboard, combining punctuation or numbers with a regular word, creating acronyms from words in a song, a poem or another known sequence of words.
16. The following password expiration guidelines are followed for users, administrators and at the group level:
  - a) Passwords for user and administrator accounts have a maximum validity of sixty (60) days;
  - b) Automatically forces users (including administrators) to change user account passwords every sixty (60) days; and
  - c) Passwords are not changeable within one (1) day of the previous change unless overridden by a security access administrator.



## Security Requirement for Suppliers and Business Partners

17. Passwords for device or non-user identifiers must be forced to expire automatically on all systems at least every ninety (90) days. Exception: Identifiers that are logically restricted to an approved path or source may have a non-expiring password.
18. Users must be provided the capability to change their password through secure protocols. A valid password must be given before a new password can become effective. The password change process must include entry of the current password followed by entry of the new password twice. Both entries of the new password must match in order to successfully complete a password change and the password change function must verify the strength (e.g., length and composition) of the password prior to accepting the change. Users must not be allowed to change their password more than once in a twenty-four (24) hour period, without the intervention of a security administrator.
19. Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable using strong cryptography, during transmission and storage on all system components.
20. Passwords cannot be coded into login scripts, dial-in communications programs, files, browsers or any executable program. The practice of hard coding passwords increases the risk of passwords being compromised.
21. Storage of passwords and use of automated systems to record, replay or provide authentication must be protected through strong cryptography and patched according to vendor recommendations
22. Authentication controls are in place to ensure personnel are positively identified and authenticated prior to granting access.
23. Designated access control personnel, whether it is the information owner, resource administrator or help desk, verify the identity and access level of the user prior to resetting their password.
24. Temporary passwords that are provided to users who maintain their own passwords must be unique to each individual, not be easily guessable; meet password complexity requirements, expire upon initial use and require users to create a new one, follow established procedures for verifying the identity of the user prior to providing them with the temporary password and be distributed to the user in a secure manner (never be sent in clear text).
25. The organization must establish processes and procedures to disable and remove inactive login IDs.
26. The organization's Human Resources department must notify access management administrators of extended absences to ensure that access is temporarily disabled.
27. The organization must establish processes and procedures for password history in line with applicable regulatory and industry standards.
28. The organization must establish processes and procedures for session management, requiring re-authentication after a period of 15 minutes of inactivity.
29. Users cannot leave any organization information resource unattended that contains sensitive information or is connected to an organization network, and must logoff or activate a screen saver program if the information resource is not used for more than 15 minutes.
30. Access to information resources is restricted to authorized users only.
31. The organization utilizes a centralized access management system to avoid the need to independently grant privileges to users.
32. User activity reports must be reviewed regularly to identify misuse or inappropriate access rights.
33. All external and local connections to the organization's systems, networks or information resources, including Personal Information that the organization processes on behalf of Mastercard, whether managed onsite or by a third party, require strong multi-factor authentication for (privileged and non-privileged) accounts.



## Security Requirement for Suppliers and Business Partners

### 9.0 Network Security

1. Requirements are established for ensuring users only have direct access to the network services for which they have been specifically authorized to use.
2. The Industrial Control System (ICS) network must be logically separated from the corporate network on physically separate network devices. The organization must ensure that minimal access points exist between the ICS network and the corporate network and document them. Firewalls between the ICS network and corporate network must be configured to reject all unauthorized traffic.
3. The organization must ensure that administration of network and non-network devices is carried out on different networks.
4. Internal systems which access external networks must be logically isolated from internal networks. Logical isolation must result in the inability for systems to communicate unless intentional action is taken by authorized personnel. All external access from untrusted systems or networks (i.e. Extranet) to any internal network must be controlled through the implementation of an Information Security approved firewall.
5. The organization must establish and implement a firewall rule base to include a default-deny rule to prohibit traffic which is not specifically permitted for valid business purposes.
6. Router configuration standards must include security considerations such as disabling source routing, blocking of FTP, TFTP and telnet, strong authentication for router administrative access and synchronization of startup and running configurations.
7. A baseline configuration of the network device host operating system must be developed and maintained and under configuration control. Baseline configurations must consider business need, vendor recommendations and "best practices".
8. The organization must establish processes and procedures for email systems.

### 10.0 Third Party Services

1. The organization must establish processes and procedures for analysis of services to be outsourced.
2. The organization must evaluate and perform thorough due diligence before engaging a third-party service provider.
3. Depending on the sensitivity and criticality of the services provided, the organization requests or commissions a review of the service provider's security control structure.
4. The organization employs safeguards to ensure that the interests of third-party service providers are consistent with and reflect organization interests.
5. A written agreement containing the appropriate terms and conditions must be executed for all third party service provider relationships.
6. An individual or member of the Information Technology Operations must be assigned the responsibility of managing the relationship with the third party.
7. Security requirements of the third party information service are defined and incorporated into all formal agreements.
8. The organization is responsible for ensuring that an assessment is performed for each outsourced or subcontracted activity through third party service providers.
9. If a third party service provider, onshore or offshore, is being considered for the provision of critical information processing services (including the processing of Personal Information), organization requires outsourcing service providers to develop and establish a business continuity and disaster recovery framework, which defines its role and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures. The





## Security Requirement for Suppliers and Business Partners

vendor must review, update and test its business continuity plans regularly in accordance with changing technologies, conditions and operation requirements.

10. The organization must establish processes and procedures for monitoring third party service providers.
11. When granting customer access to organization information or assets, procedures must be in place to ensure compliance with the organization Security Monitoring and Response Policy.

### 11.0 Application Management

1. The Application Management Lifecycle must include a formal methodology defining standards for the building of applications.
2. The organization requires the integration of security requirements in system design that are consistent and supportive of the organization security architecture.
3. The Information Security department must review and approve security requirements for systems that will be used to process sensitive information (including Personal Information) before the initiation of project design. The review process must address requirements related to information security, internal controls, privacy protection and legal/regulatory considerations.
4. The organization must establish processes and procedures for addressing risks of internet-based applications.
5. The disclosure of application configuration information that could be exploited by outsiders must be prevented.
6. The organization has designated an Enterprise Architecture or other IT technology selection working group responsible for defining an overall IT technology selection and acquisition framework consistent with IT strategies.
7. Data input into application systems must be validated to ensure the completeness and accuracy of the information processed can be confirmed.
8. The organization must establish processes and procedures for maintaining a secure encryption key infrastructure.
9. The organization must compile audit records into a system-wide (logical or physical) time-correlated centralized audit trail.
10. The organization must implement processes and procedures for testing of security features and controls as part of application testing.
11. All significant modifications, major enhancements, and new systems must be integration tested prior to deployment in production environments. Automated tools must be used to improve the overall testing process. System stress testing and volume testing must be performed, and in some cases, parallel testing will be required. Integration testing must be conducted in a separate, independently controlled environment.

### 12.0 Enterprise Resilience (Business Continuity)

1. Critical information systems must be protected by Uninterruptible Power Supply (UPS) devices.
2. The organization must perform preventive maintenance regularly on all equipment used to support information systems or data center operations in conformance with manufacturer recommendations.
3. The organization must establish processes and procedures for the use of backup generators, to include fuel vendors, for maintaining power during electrical supply outage.
4. The mission and purpose of Business Continuity Management must be clearly defined within a policy or charter.
5. The organization's Disaster Recovery Program Manager is responsible for the development, maintenance and testing of organization's technical recovery plans.
6. Business continuity plans are formulated to ensure that employees are aware of the steps they would be required to take in the event of a business disruption or disaster.



## Security Requirement for Suppliers and Business Partners

7. Contingency plans are designed to maintain or restore business operations, including computer operations, in the event of emergencies, system failures, or a disaster.
8. The organization must establish requirements for business continuity plans.
9. The organization must establish processes and procedures for identifying possible business disruptions and impacts.
10. Management is responsible for ensuring that an annual review of business continuity plans is completed. The business continuity plan must be referenced against an inventory of information resources and applications to ensure that all critical processes are adequately protected.
11. Processes are in place to ensure that critical systems have business continuity plans, contingency arrangements and are tested annually.

### 13.0 Compliance

1. The organization must establish processes and procedures for documentation of legal and compliance obligations.
2. The organization must have an established privacy and data protection program specifying management practices, roles and responsibilities and technical and organizational measures to ensure that Personal Information is processed in compliance with applicable laws.
3. Personal Information must not be transferred to a country or territory outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of protection of the rights and freedoms of the data subjects in relation to the processing of Personal Information.
4. Personal Information must only be obtained by organization for specified and lawful purposes and must not be further processed or disclosed in any manner incompatible with those purposes.
5. The organization must have procedures for the data subjects to exercise their rights relating to their Personal Information held by organization. The procedures must allow for data subjects to specify legitimate reasons regarding the challenges, updates or corrections regarding the organization processing of their Personal Information. The procedures shall also identify any fee associated with such challenges, updates or corrections.
6. Standards are defined for protecting Personal Information, including customer data, when processing is outsourced to a third party. The same standard of protection must be required from all third parties, contractors and vendors who have access to systems of record that maintain Personal Information.
7. The organization has designated a specific department to ensure that independent audits, assessments and penetration tests are performed on an annual basis, or as otherwise necessary (i.e. segmentation controls, significant infrastructure or application upgrade or modification). Audits must ensure compliance with organization security policies, standards, procedures and other documented security requirements.
8. The organization must employ automated mechanism to scan the network no less than quarterly to detect the addition of unauthorized components/devices into the information system.

### 14.0 Information Technology Management

1. IT management must institute a training program, at least annually, to provide education and awareness of internal practices and policy as well as external guidance towards the proficiency and use of technology within organization. The training program must be allocated sufficient funding for both internal and external events to further the education and skills of IT resources.
2. All IT practices and standards must be overseen through formal review processes approved by the Chief Information Security Officer.
3. The organization must establish processes and procedures for access control for mobile devices.



## Security Requirement for Suppliers and Business Partners

4. Cloud service providers shall be contractually bound to protect organization information stored and/or processed in the cloud.

### 15.0 IT Incident Management

1. The organization must review log files and audit trails at least every 24 hours for anomalous activity. Log files and audit trails must include, at the minimum: system records initialization sequences, logons and errors, system processes and performance, system resources utilization anomalies and network traffic, bandwidth utilization rates.
2. Administrative groups must be inspected at least every 7 days to ensure unauthorized administrator accounts have not been created, or authorized administrator accounts have not been used in an unauthorized manner, and spot checks of system audit records must be completed at least once every thirty (30) days to validate ongoing integrity.
3. The organization must create event logs, which must include, but are not limited to: User identification (source and destination), Success or failure indication, Origination of event (system and application), Internet Protocol (IP) of systems (source and destination [for many events, the source will be the user's IP]), Ports in use (source and destination), Identity or name of affected data, system component, or resource Date and time stamp, Description of the activity performed must include Event ID or event type, Reason for logging event (e.g., access failure). Event logs are reviewed on a regular basis in order to identify security incidents and potential vulnerability in the security structure.
4. The organization must establish IT event monitoring processes that identify relevant IT events, alert proper personnel of anomalous IT activities, filter, correlate and analyze event data and provide the appropriate response to IT events.
5. The Information Security department must establish a channel for the reporting of IT incidents; in particular, security incidents and potential vulnerabilities in the security structure.
6. ITSM-BizOps Incident management is responsible for establishing processes that stretch through five phases of the Incident lifecycle: Identification, logging, categorization, prioritization, and Incident response.

### 16.0 Privacy

1. The organization must establish processes and procedures for the collection, processing and retention of Personal Information in accordance with defined Mastercard privacy and information security procedures, and the Data Protection Agreement (DPA) and other contractual data protection and privacy terms, as applicable.

### 17.0 Audit Management

1. The organization must provide meaningful procedures for timely hearing and resolving enrollee grievances. A grievance may also include a complaint that an organization refused to expedite a coverage determination or redetermination, complaints regarding the timeliness, appropriateness, access to, and/or setting of a provided item.
2. The organization must define, develop and document a bribery prevention policy that covers activities related to bribery, inclusive of public officials, penalties and prosecution of offenders, periodic review and training /dissemination to the organization's staff.
3. The organization must define, develop and document a policy that covers activities related to prohibited foreign trade practices, inclusive of public officials, penalties and prosecution of offenders, periodic review and training /dissemination to the organization's staff.
4. An independent internal audit committee chaired by a member of the Board of Directors must be established. The audit committee must be responsible for designating roles and responsibilities for audit functions, performance of



## Security Requirement for Suppliers and Business Partners

audits, effectiveness, and oversight of external auditors. The audit committee must meet periodically to review outstanding audit issues, ongoing projects, findings and recommendations from audit projects.

5. Findings (control deficiencies, gaps or issues) and recommendations for improvements must be reported to the appropriate management as well as the audit committee and/or Board of Directors.

## Glossary of Terms

**Backup and Restore** - Backing up files and recovering them after a system failure.

**Chief Privacy Officer** - a senior level executive responsible for managing data protection and privacy risks, and for the development and oversight of related policies and programs.

**Chief Security Officer** - an organization's most senior executive accountable for the development and oversight of policies and programs intended for the mitigation and/or reduction of compliance, operational, strategic, financial and reputational security risk strategies relating to the protection of people, intellectual assets and tangible property.

**Event ID** - unique ID related to any observable occurrence in a network or system.

**Incident Response Team** - Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents.

**Industry Control System (ICS)** - An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

**Intrusion Detection System/Intrusion Protection System (IDS/IPS)** - software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

**Internet Protocol (IP)** - Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.

**Payment Card Industry Data Security Standard (PCI DSS)** - an information security standard for organizations that handle payment card information.

**Personal Information** - any information relating to an identified or identifiable natural person.

**Port** - the entry or exit point from a computer for connecting communications or peripheral devices.

**Sensitive Personal Information** - any Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, geo-location data, and information relating to criminal convictions and offences or related security measures.

Proprietary and Confidential. For Mastercard supplier and partner engagements only.

Mastercard is a registered trademark, and the circles design is a trademark, of Mastercard International Incorporated.

©2020 Mastercard. All rights reserved. Mastercard, 2000 Purchase Street, Purchase, NY 10577.



## **ANNEX 2: DESCRIPTION OF THE PROCESSING ACTIVITIES**

### **Nature and Purpose of the Processing**

Provider Processes Personal Data pursuant to this Agreement for the performance of the services as described in this Agreement and/or any corresponding documents.

### **Types of Personal Data (including Sensitive Data)**

Provider processes Personal Data to the extent permitted by Mastercard or Mastercard's customers as applicable pursuant to the Agreement, including but not limited to, the following categories of Personal Data:

With respect to personnel of Mastercard, personal details, including information that identifies the Data Subject such as name, employer, address, e-mail, telephone number, location and other contact details. With respect to customers of Mastercard, name, address, e-mail, telephone number, location, and billing and payment details such as bank account and credit or debit card numbers.

Provider does not process Sensitive Personal Data

### **Categories of Data Subjects**

Provider Processes Personal Data relating to the following categories of Data Subjects, as applicable:

Cardholders; Mastercard's staff; Staff of Mastercard's customers; Mastercard's websites, applications and platforms users; Consumers of Mastercard's services; and Individual merchants.

### **Duration of the Processing**

Personal Data may be Processed and stored for the period necessary to fulfill the agreed purposes of processing pursuant to and for the duration of this Agreement within the limitations set forth in the relevant document, and to comply with applicable Privacy and Data Protection Law.

## ANNEX 3

### EEA DATA PROCESSING ADDENDUM

Provider, Mastercard, and Mastercard Europe SA agree that the terms and conditions set out below are added as an EEA Data Processing Addendum (“**Addendum**”) to, and form an integral part of, the Agreement to which it is attached. For the purposes of this Annex 3, a “Party” and the “Parties” shall mean Provider, Mastercard, and Mastercard Europe SA. This Addendum regulates the Processing of Personal Data of Data Subjects subject to the EU Data Protection Law (as defined in Section 1.3. below). Provider’s Processing of Personal Data shall be limited to the purposes set forth in Annex 1 by the Parties in the context of the Services. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement (including all applicable documents) and Exhibit D thereto, as amended by, and including, this Addendum.

**1. Definitions.** The following terms have the meanings set out below for this Addendum:

- 1.1. The terms “**Controller**” “**Data Subject**”, “**Personal Data**”, “**Processing/Process of Personal Data**”, “**Processor**” and “**Supervisory Authority**” shall have the meanings given to them under EU Data Protection Law.
- 1.2. “**EU Data Protection Law**” means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) and their respective national implementing legislations; the Swiss Federal Data Protection Act (as amended and replaced from time to time); the Monaco Data Protection Act (as amended and replaced from time to time); the UK Data Protection Act (as amended and replaced from time to time); and the Data Protection Acts of the European Economic Area (EEA) countries (as amended and replaced from time to time), in each case solely to the extent applicable.
- 1.3. “**EU GDPR**” means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time).
- 1.4. “**Europe**” means the European Economic Area, Switzerland, Monaco and the United Kingdom.
- 1.5. “**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, or other unauthorized Processing of Personal Data transmitted, stored or otherwise Processed.
- 1.6. “**Processor**” means the entity which Processes Personal Data on behalf of a Controller.
- 1.7. “**Processing of Personal Data**” ((or “Processing/Process”) means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- 1.8. “**Pre-2021 Standard Clauses**” or “**Pre-2021 SCCs**” means
  - 1.8.1.the standard contractual clauses for the transfer of personal data to data processors established in third countries adopted by the European Commission decision of 5 February 2010, published under document number C(2010) 593 2010/87/EU;
  - 1.8.2.the standard contractual clauses the transfer of personal data to third countries adopted by the European Commission decision of 15 June 2001, published under document number C(2001) 1539); and





1.8.3. the standard contractual clauses the transfer of personal data to third countries adopted by the European Commission decision of 27 December 2004, published under document number C(2004) 5271 (as applicable).

1.9. **“Sensitive Data”** has the meaning set forth in Section 4 of Exhibit D.

1.10. **“Services”** has the meaning set forth in Attachment A, Section 1 of the Agreement.

1.11. **“Sub-Processor”** means the entity engaged by the Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller

1.12. **“UK GDPR”** means the UK Data Protection Act 2018 (as amended and replaced from time to time)

1.13. **“2021 Standard Contractual Clauses”** or **“2021 SCCs”** means in respect of Personal Data to which the EU GDPR was applicable prior to its processing by Supplier as Processor, the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 including the text from the modules of such clauses as specified in this Agreement.

## 2. **Roles of the Parties.** In the context of the Agreement, the Parties agree that:

2.1. Mastercard acts as Controller, or as Processor acting on behalf of Mastercard’s customers who act as Controllers.

2.2. Mastercard appoints Provider as Processor, or as Sub-Processor of Mastercard’s customers, for the Processing of Personal Data for the purpose of providing the Services specified in the Agreement as implemented by each individual Statement of Work where applicable. In that context, Mastercard, as Controller, or Processor acting on behalf of its customers, has the sole and exclusive authority to determine the purposes and means of the Processing of Personal Data that are disclosed to and collected by Provider. Provider will Process Personal Data only on behalf and for the benefit of Mastercard, or of Mastercard’s customers, and only to carry out its obligations under the Agreement as implemented and to the extent required by each individual Statement of Work, where applicable, and Mastercard’s written instructions. Provider shall not share, transfer, transmit, disclose or otherwise provide access to or make available any Personal Data to any third party unless Mastercard has authorized Provider to do so in writing, including as applicable in this Agreement.

## 3. **Compliance with EU Data Protection Law.** Both Parties represent and warrant that they will comply with EU Data Protection Law when Processing Personal Data in the context of the Services, in particular with the requirements applicable to Processors, including sub-processing, audit and data transfers requirements as described respectively under Sections 6, 7 and 8 of this Addendum.

## 4. **Provider’s obligations.** Provider agrees and warrants that it will:

4.1. notify Mastercard when any law or legal requirement prevents Provider (1) from fulfilling its obligations under the Agreement or EU Data Protection Law, and (2) from complying with the instructions received from Mastercard via this Addendum. In both situations, the Parties shall come to a mutual agreement to identify the solution to ensure compliance. Mastercard may in part or as a whole, as applicable, suspend the Processing of Personal Data by Provider, until such event resulting in non-compliance has ceased or rectified. If Provider fails to correct the non-compliance, Mastercard is entitled to terminate any further Personal Data Processing and this Agreement, if doing so is required to comply with EU Data Protection Law (**“Instructions”**).

4.2. maintain internal records of all Processing conducted on behalf of Mastercard, with at the minimum the categories of information required under EU Data Protection Law and provide them to Mastercard upon request (**“Internal Records”**).

4.3. where applicable, comply with all opt-in and opt-out requirements for sending marketing communications, consult any opt-out registers where applicable and comply with legal requirements applicable to cookies and similar technologies to the extent required under EU Data Protection Law (**“Marketing Communications, Cookies and Similar Technologies”**).



- 4.4. immediately inform Mastercard, in writing, in relation to any Personal Data Processed in the context of the Services of: (i) any Data Subjects' requests to their rights of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing, (f) objection to the Processing; and (g) not being subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them; (ii) any request or complaint received from Mastercard's customers, consumers, employees or from any other individual; (iii) any question, complaint, investigation or other inquiries from Data Protection Authorities; and (iv) any public authority of whatever jurisdiction requesting disclosure of or information about the Personal Data that are Processed by Provider. Provider agrees and warrants that it will provide a copy of any such requests within 48 (forty-eight) hours and to the extent legally permissible that it will respond to such requests only in accordance with Mastercard's prior written authorization and instructions. Provider will assist Mastercard in fulfilling its obligations or Mastercard's customers' obligations to respond to individuals' requests in accordance with EU Data Protection Law ("**Notification Obligations**").
- 4.5. taking into account the nature of the Processing, cooperate with Mastercard to comply with EU Data Protection Law, this Addendum, Mastercard's customers' instructions when Mastercard acts as Processor, and to assist Mastercard fulfil its own obligations under EU Data Protection Law and as applicable Mastercard's customer's instructions, including complying with Data Subjects' requests to exercise their rights, replying to complaints from Data Subjects, replying to investigation and inquiries from supervisory authorities, conducting data protection impact assessments and prior consultations with supervisory authorities. Where required by Mastercard, the Provider shall submit the Personal Data it holds on the individual through a portal designated by Mastercard in a format agreed and within the timeframe agreed ("**Cooperation and Assistance**"). Notwithstanding the foregoing, such Cooperation and Assistance will only be provided by Provider to the extent legally permissible, t.
- 4.6. upon termination of the Agreement or upon request to securely delete or return Personal Data, comply with Mastercard's request, and securely delete existing copies unless EU or Member States law requires storage of the Personal Data (in which case Provider will protect the confidentiality of the Personal Data, will not actively Process the Personal Data anymore, and will continue to comply with the Agreement) ("**Termination**").

**5. Security of the Processing, Confidentiality, and Personal Data Breach Notification.** Provider agrees and warrants that:

- 5.1. it has implemented and maintains a comprehensive written information security program that complies with EU Data Protection Law, Annex 1 of Exhibit D, and, to the extent Provider Processes payment card information, the applicable Payment Card Industry Data Security Standards. Provider's written information security program must include appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which includes at the minimum the security measures listed in Annex 1 of Exhibit D and as appropriate: (a) the pseudonymization and encryption of Personal Data (including the encryption of Primary Account Number (PAN) in transit and in rest); (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services (including by appropriately maintaining and reviewing logs, performing periodic password renewal and applying multi-factor authentication, in accordance with the controls referenced in Annex 1 of Exhibit D to this Agreement); (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing of Personal Data. In assessing the appropriate level of security, Provider must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing of Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects and the risks that are presented by the Processing of Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed ("**Information Security Program**").
- 5.2. Provider's Information Security Program must, among other things, include regular testing or otherwise monitoring of the effectiveness of Provider's information safeguards. Provider undertakes to notify Mastercard of any technical, operational, organizational or other change having a material impact on the security, confidentiality or protection of Personal Data, no less than 15 (fifteen) working days prior to implementing any such change.



Provider agrees to submit its Information Security Program to the Data Protection and Security Audit provided under Section 8 .

- 5.3. Provider must take steps to ensure that any person acting under its authority who has access to Personal Data is only granted access to Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only Processes Personal Data in accordance with Mastercard's instructions ("**Confidentiality**").
- 5.4. Provider will inform Mastercard of any Personal Data Breach i) by contacting the Mastercard Security Operations Center at +1-636-722-3600 or 1-800-358-3060 (US toll-free number) and; ii) in writing to TPRM@mastercard.com, SOC@mastercard.com and the account manager or person they are doing business with inside of Mastercard , without undue delay, and no later than 24 (twenty-four) hours after having become aware of a Personal Data Breach. Such notice will summarize in reasonable detail the effect on Mastercard, if known, of the Personal Data Breach and the corrective action taken or to be taken by Provider, and/or its Sub-Processors. Provider will promptly take all necessary and advisable corrective actions, and will cooperate fully with Mastercard in all reasonable and lawful efforts to investigate, prevent, mitigate or rectify such Personal Data Breach. Provider shall collect, preserve and document all evidence regarding the discovery and cause of, and vulnerabilities, response, remedial actions, and impact, related to the Personal Data Breach, and shall provide such documentation to Mastercard upon request. Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, Provider must obtain the approval of Mastercard prior to the publication or communication of any filings, communications, notices, press releases or reports related to any Personal Data Breach that expressly mention Mastercard or Mastercard Affiliates. Provider will be responsible for the costs and expenses associated with the performance of its and its Sub-Processor's obligations described in this paragraph unless the Personal Data Breach is caused by the acts or omissions of Mastercard. Provider will assist Mastercard in complying with its own obligations or with Mastercard's customers' obligations under EU Data Protection Law to notify of a Personal Data Breach.
- 5.5. Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, Provider must obtain the approval of Mastercard prior to the publication or communication of any filings, communications, notices, press releases or reports related to any Personal Data Breach that expressly mention Mastercard or its Affiliates. Provider acknowledges and agrees that a violation of this clause, or the occurrence of any Personal Data Breach, may cause immediate and irreparable harm to Mastercard for which money damages may not constitute an adequate remedy. Therefore, Provider agrees that Mastercard may seek injunctive or other equitable relief for any such violation or incident, in addition to its remedies at law, without proof of actual damages ("Personal Data Breaches").
- 5.6. Provider agrees and warrants that it has not purposefully created back doors or similar programming that could be used to access the Personal Data in transit or at rest, or otherwise created business processes to facilitate mass and indiscriminate access to Personal Data by Government Agencies. Provider must notify Mastercard by email to privacyanddataprotection@mastercard.com as soon as it becomes aware of the existence of a back door or similar programming or of a new business process which enables mass and indiscriminate access to Personal Data ("Government Data Request").

## **6. International data transfers.**

- 6.1. Provider agrees and warrants that it is prohibited from transferring Personal Data outside of Europe except if it obtains the explicit written consent of Mastercard and provided that the Personal Data are transferred to a country which has been considered to provide an adequate level of protection under EU Data Protection Law or to a data recipient which has implemented adequate safeguards under EU Data Protection Law such as approved Binding Corporate Rules or Standard Contractual Clauses.
- 6.2. In the context of the Services, Mastercard agrees that Provider transfers or stores Personal Data Processed on behalf of Mastercard in the countries listed in Section 5.7.1 of Exhibit D to this Agreement as necessary to perform services on behalf of Mastercard. Provider agrees to protect Personal Data in the countries listed in Section 5.7.1 of Exhibit D to this Agreement in compliance with EU Data Protection Law, and this Addendum and will not use the Personal Data transferred to the countries listed in Section 5.7.1 of Exhibit D to this Agreement for its own purposes in violation of the Agreement.

- 6.3. To the extent that no adequate safeguards referenced in Section 6.1 above are in place at the time of execution of this Annex, the Parties shall be deemed to have executed the 2021 Standard Contractual Clauses for Personal Data transfers subject EU GDPR or the Swiss Federal Data Protection Act (“**EU Transfers**”). For the avoidance of doubt, the 2021 Standard Contractual Clauses will apply to Personal Data Processed by Provider in the context of the Services that are transferred outside of EEA and Switzerland, either directly or via an onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data under EU GDPR or to a recipient which has not implemented adequate safeguards under EU GDPR or Swiss Federal Data Protection Act.
- 6.4. For the purposes of the 2021 SCCs that apply pursuant to Clause 6.3 of this Annex, the Parties agree the following:
- 6.4.1. the text from module two of the 2021 SCCs shall apply where Mastercard is the Controller, the text from module three of the 2021 SCCs shall apply where Mastercard is a Processor on behalf its customers and no other modules or any clauses marked as optional in the 2021 SCCs shall apply;
- 6.4.2. for the purposes of clause 9(a) of the 2021 SCCs, as applicable under modules two and three, option 1 applies with 60 business days as the specified time period for submitting the request for specific authorisation. Any request pursuant to clause 9(a) of the 2021 SCCs shall be made pursuant to Clause 7.8 of this Annex, including the information required thereof, which shall be provided in addition to any other information necessary to enable Mastercard to decide on the authorisation. The list of Sub-processors already authorised by Mastercard required by Annex III of the 2021 SCCs is set out in Clause 5.8.1 of Exhibit D of this Agreement;
- 6.4.3. the information as required by Annex I of the 2021 SCCs is as set out in Annex 4 of Exhibit D of this Agreement and the signatures for the purpose of Annex I of the 2021 SCCs are the signatures to this Agreement and the date is the date of this Agreement;
- 6.4.4. the technical and organisational measures required by Annex II of the 2021 SCCs are as set out in Annex 1 and 4 of Exhibit D of this Agreement and the information in relation to the technical and organisational measures in relation to Data Subject rights as required by clause 10(b) and Annex II of the 2021 SCCs as applicable under modules two and three are as set out in Annex 4 of Exhibit D of this Agreement;
- 6.4.5. any notice provided under clause 9(d) of the 2021 SCCs shall be provided according to the timing and to the email address as set out in Clause 7.9 to this Annex of this Agreement;
- 6.4.6. any notice provided under clause 14(e) or clause 16 of the 2021 SCCs shall be provided according to the timing and to the email address as set out in Clause 6.9 to this Annex of this Agreement;
- 6.4.7. for the purposes of clause 17 of the 2021 SCCs, option 1 applies and the 2021 SCCs shall be governed by the laws of Belgium and for the purposes of clause 18 of the 2021 SCCs, the courts of Belgium shall have jurisdiction in relation to the 2021 SCCs; and
- 6.4.8. notwithstanding anything contrary in this Agreement, clause 5 of the 2021 SCCs shall apply and, as such, in the event of a contradiction between the 2021 SCCs and the provisions of this Agreement, the 2021 SCCs shall prevail.
- 6.5. In the event that Pre-2021 SCCs are no longer valid for use under Article 46 of the UK GDPR and new standard contractual clauses are implemented in the UK, the parties agree that (subject to Clause 6.6 of this Annex) the 2021 SCCs shall apply to the parties as they apply to EU Transfers pursuant to Clauses 6.3 and 6.4 of this Annex in relation to any transfer of Personal Data made under the Agreement by Mastercard to Supplier to a country that is not recognised as adequate under UK adequacy regulations where:
- 6.5.1. the UK GDPR was applicable prior to its Processing by Supplier as Processor; and Mastercard has permitted such transfer under the Agreement (“**UK Transfers**”).
- 6.6. The parties agree any addendum to the 2021 SCCs which are standard data protection clauses issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 (“**UK Addendum**”) is incorporated by reference in this Agreement and modifies the 2021 SCCs (that are agreed under clause 6.5 of this Agreement) as set out in such standard data protection clauses in respect of UK Transfers only.





- 6.7. The parties agree, notwithstanding anything to the contrary in the Agreement, that Mastercard may make any amendments to the application of the 2021 SCCs, the application of the UK Addendum and/or any other amendments to this Clause 6.5 and 6.6 in respect of UK Transfers as it deems necessary to implement any replacement standard contractual clauses approved for use under Article 46 of the UK GDPR by notifying the Supplier of any such amendments to this Agreement in writing and such amendments shall be effective upon such notice.
- 6.8. Supplier will notify Mastercard in writing to [TPRM@mastercard.com](mailto:TPRM@mastercard.com), with the subject line “EEA Data Processing Addendum Notification”, at least 60 calendar days prior to any new intended data transfer to a country that is not subject to a European Commission adequacy decision, including the justification of the necessity of the transfer, an explanation of any adequate supplementary measures implemented by the Supplier to ensure essential equivalence if necessary or justified and an explanation if Supplier considers that such safeguards are not necessary. Any such transfer is subject to Mastercard’s prior written consent. Where Mastercard does not consent to such transfer and further Processing of Personal Data is not possible without such transfer, Mastercard may in part or as a whole, as applicable, suspend the Processing of Personal Data by Supplier or terminate the Agreement, whichever is appropriate.
- 6.9. Supplier will promptly and no later than 48 hours from becoming aware inform Mastercard in writing to [TPRM@mastercard.com](mailto:TPRM@mastercard.com), with the subject line “EEA Data Processing Addendum Notification”, if (1) it has reason to believe that it is or has become subject to laws or practices that prevent the Supplier from fulfilling its obligations under the 2021 Standard Contractual Clauses, and (2) it is unable to comply with the 2021 Standard Contractual Clauses, for whatever reason. Supplier shall provide the description of the non-compliance and the reasons for the non-compliance, and its impact or likely impact on Mastercard or Mastercard customers if applicable.

## **7. Provider’s Sub-Processing.**

- 7.1. Provider will not share, transfer, disclose, make available or otherwise provide access to any Personal Data to any third party, or contract any of its rights or obligations concerning Personal Data performed on behalf of Mastercard under the Agreement to a Sub-Processor or a subsequent Sub-Processor without the specific prior written consent of Mastercard. For the avoidance of doubt, Mastercard’s prior consent must be obtained for each and any change in Sub-Processor(s) or subsequent Sub-Processor(s) and no later than 60 days prior for any such change.
- 7.2. Where Provider sub-contracts any of its Processing of Personal Data under the Agreement, with the consent of Mastercard, it shall do so by way of a written agreement with the Sub-Processor which imposes at least the same level of protection for the Processing of Personal Data and the same obligations on the Sub-Processor as are imposed on Provider under this Addendum and under EU Data Protection Law, including the requirements applicable to Processors, such as sub-processing audit, and data transfers requirements as described in Sections 6, 7, and 8 of this Addendum.
- 7.3. Provider has appointed the Sub-Processors listed in Section 5.8.1 of Exhibit D to this Agreement to Process Personal Data in the context of the Services specified in the Agreement and each individual Statement of Work with Mastercard’s prior written consent, and Provider represents and warrants that such Sub-Processors have each entered into binding written agreements with Provider that are substantially the same as those that are imposed on Provider under this Addendum.
- 7.4. Prior to any Sub-Processing, Provider must carry out adequate due diligence to ensure that the Sub-Processor is capable of providing Personal Data with at least the same level of protection for the Processing of Personal Data and the same obligations on the Sub-Processor as are imposed on Provider under this Addendum.
- 7.5. Provider will promptly send to Mastercard an extract of any Sub-Processor agreement it concludes in the context of this Addendum in order to demonstrate its compliance with Section 7.2. of this Addendum, upon Mastercard’s written request.
- 7.6. Provider will provide Mastercard with the necessary information to help verifying the Sub-Processor’s compliance with its data protection obligations (including, where appropriate, attestations and certifications of the Sub-Processor’s compliance with data protection and information security standards, such as the Payment Card Industry Data Security Standards (PCI-DSS) and SOC2 and ISO certifications, as applicable).



- 7.7. Provider shall remain fully liable towards Mastercard for the performance of any and all Sub-Processor obligations under such agreement.
- 7.8. Supplier will notify Mastercard in writing to [TPRM@mastercard.com](mailto:TPRM@mastercard.com), with the subject line “EEA Data Processing Addendum Notification”, about engaging any intended new Sub-Processor(s) or subsequent Sub-Processor(s) with at least 60 business days’ notice prior to the engagement of the Sub-processor and such notice shall include the description of the Processing by each such Sub-Processor, categories of Data Subjects and the categories of Personal Data Processed, and the location of the Processing of Personal Data. Where Mastercard does not consent to the intended new Sub-Processor(s) or subsequent Sub-Processor(s) and the Processing of Personal Data is not possible without the involvement of the particular Sub-Processor(s) or subsequent Sub-Processors(s) that was objected to by Mastercard, Mastercard may in part or as a whole, as applicable, suspend the Processing of Personal Data by Supplier or terminate the Agreement, whichever is appropriate.
- 7.9. Supplier will promptly and no later than 48 hours from becoming aware notify Mastercard, in writing to [TPRM@mastercard.com](mailto:TPRM@mastercard.com), with the subject line “EEA Data Processing Addendum Notification”, of any failure by Supplier or any Sub-Processor(s) or subsequent Sub-Processor(s) to fulfil its obligations under this Agreement or sub-agreement, including but not limited to where Supplier has engaged any new Sub-Processors, or where Personal Data has been transferred to any new locations, without Mastercard's prior written consent.

## 8. Data Protection and Security Audit.

- 8.1. Upon request by Mastercard and subject to Mastercard’s reasonable discretion, Provider allows Mastercard or, as applicable, Mastercard’s customers, or an inspection body composed of independent members selected by Mastercard or Mastercard’s customers, to audit and review Provider’s Information Security Program, data processing facilities, and data protection compliance program to verify compliance with this Addendum, EU Data Protection Law, and as applicable with Mastercard’s customers’ instructions or own obligations under the EU Data Protection Law; provided that such audit will not take place more than once annually. Where a Personal Data Breach was caused by a Sub-Processor engaged by Provider, Provider undertakes to ensure that Sub-Processor fully cooperates with Mastercard, and where requested by Mastercard, allow Mastercard to audit and review the Sub-Processor’s Information Security Program, data processing facilities, and data protection compliance program. (“**Data Protection and Security Audit**”).
- 8.2. The Parties will mutually agree upon the scope, timing, and duration of the Data Protection and Security Audit. Such Audit may be conducted by an independent third-party auditor designated by Mastercard, in which case Provider will make available to Mastercard, or where applicable, Mastercard’s customers, the result of the audit. Provider agrees to fully cooperate with such Data Protection and Security Audit and implement all commercially reasonable changes to its Information Security Program, data processing facilities and data protection compliance program that, as a result of the Data Protection and Security Audit, are required to ensure Provider’s compliance with this Addendum, EU Data Protection Law, and as applicable with Mastercard’s customer’s instructions or own obligations under the EU Data Protection Law.
- 8.3. Upon request by Mastercard, Provider must provide a certification of compliance with applicable EU Data Protection Law and information security standards, such as the annual Payment Card Industry Data Security Standards (PCI-DSS) and SOC2 Type II certifications, as applicable.
- 8.4. Provider’s failure to allow or cooperate to any Data Protection and Security Audit or implement any such required changes to the information security program within a reasonable period of time (at least 30 days) after receipt of such audit results shall entitle Mastercard to suspend the Processing of Personal Data by Provider, and to terminate any further Personal Data Processing and terminate the Agreement, if doing so is required to comply with the Agreement, EU Data Protection Law, and as applicable with Mastercard’s customers’ instructions or own obligations under the EU Data Protection Law.

## 9. Liability Towards Data Subject. The Parties agree that they will be held liable for violations of EU Data Protection Law towards Data Subjects as follows:

- 9.1. Provider is responsible for the damage caused by the Processing of Provider or its Sub-processors which infringes EU Data Protection Law or this Addendum.





- 9.2. Mastercard will be liable for the damage caused by the Processing only where it has not complied with obligations of EU Data Protection Law specifically directed to Controllers .
- 9.3. If Mastercard paid full compensation for the damage suffered, it is entitled to claim back from Provider that part of the compensation corresponding to Provider's part of responsibility for the damage but only to the extent arising from Provider's or its Sub-processors' violation of this Addendum.

**10. Applicable Law and Jurisdiction.** The Processing of Personal Data under this Addendum is governed by Belgian law. Any disputes between the Parties relating to the Processing of Personal Data under this Addendum will be subject to the exclusive jurisdiction of the courts in Belgium.

The Parties are signing this Addendum on the Effective Date as defined in the Agreement.

<b>Mastercard International Incorporated</b>	
By:	<i>Sapan Mandloi</i>
Name:	Printed Name Sapan Mandloi
Title:	Title Description SVP, Acceptance Solutions
Date:	06/30/2023

<b>Mastercard Europe SA</b>	
By:	<i>Joanna Lopatowska</i> <small>Joanna Lopatowska (Jul 5, 2023 22:36 GMT+2)</small>
Name:	Printed Name Joanna Lopatowska
Title:	Title Description Senior Managing Counse
Date:	07/05/2023

<b>Spreedly, Inc.</b>	
By:	<i>Justin Benson</i> <small>DocuSigned by: C9132818B2F844A...</small>
Name:	Printed Name Justin Benson
Title:	Title Description CEO
Date:	6/30/2023

## ANNEX 4

**This Annex incorporates the European Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.**

This Annex forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Annex.

This Annex incorporates, as if it was contained herein, Annex 2 of the Exhibit D to this Agreement.

### PROCESSING DETAILS

#### A. LIST OF PARTIES

Data exporter:

- **Name:** The entity or entities defined as Mastercard in the Agreement to which this annex is included.
- **Address:** As provided in the Agreement to which this Annex 4 is annexed. For UK Data Transfer, Mastercard Europe Services Limited, 10 Upper Bank Street, Canary Wharf, London, E14 5NP, United Kingdom
- **Contact person's name, position and contact details:** See data protection officer details below.
- **Data protection officer (if applicable):** Europe Data Protection Officer, [privacyanddataprotection@mastercard.com](mailto:privacyanddataprotection@mastercard.com)
- **Representative in the European Union:** N/A
- **Representative in the UK (where Clause 6.5 of Annex 3 applies):** N/A
- **Activities relevant to the data transferred under the 2021 SCCs:** The receipt of the Services under the Agreement.
- **Signature and date:** The signature and date of the Agreement to which this Annex 4 is annexed.
- **Role (controller/processor):** Controller or Processor on behalf of its customers

Data importer:

- **Name:** The entity defined as Supplier in the Agreement to which this Annex 4 is annexed.
- **Address:** As provided in the Agreement to which this Annex 4 is annexed.
- **Contact person's name, position and contact details:** Jennifer Rosario, CISO, [security@spreadly.com](mailto:security@spreadly.com)
- **Activities relevant to the data transferred under the 2021 SCCs:** The provision of the Services under the Agreement.
- **Signature and date:** The signature and date of the Agreement to which this Annex 4 is annexed.
- **Role (controller/processor):** Controller or Processor (where Mastercard is a Controller) or Sub-Processor (where Mastercard is a Processor on behalf of its customers)

#### B. DESCRIPTION OF TRANSFER

**Controller to Processor or Processor to Sub-Processor transfers:**

- Categories of Data Subjects whose personal data is transferred

As set out in the Agreement

- Categories of Personal Data transferred

As set out in the Agreement

- Sensitive Data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Information regarding sensitive data transferred is as set out in the Agreement

None

- The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis

- Nature of the Processing

As set out in the Agreement

- Purpose(s) of the data transfer and further processing

As set out in the Agreement

- The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The duration of the Processing is as set out in the Agreement

- Supplemental technical and organisational measures

As set out in Annex 1 of Exhibit D to the Agreement

## C. COMPETENT SUPERVISORY AUTHORITY

Belgian Data Protection Authority (except where clause 6.5, 6.6 and 6.7 of Annex 3 applies, in which case, the UK Information Commissioner's Office)




# SaaS Agreement Spreedly

Final Audit Report

2023-07-05

Created:	2023-07-05
By:	Nicholas Wade (nicholas.wade@mastercard.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAoEpUH0A9PK7rF7J3XDH3hfzXjYoAdy76

## "SaaS Agreement Spreedly" History

-  Document digitally presigned by DocuSign\, Inc. (enterprisesupport@docusign.com)  
2023-06-30 - 8:22:39 PM GMT
-  Document created by Nicholas Wade (nicholas.wade@mastercard.com)  
2023-07-05 - 6:00:01 PM GMT
-  Document emailed to Joanna Lopatowska (Joanna.Lopatowska@mastercard.com) for signature  
2023-07-05 - 6:05:05 PM GMT
-  Email viewed by Joanna Lopatowska (Joanna.Lopatowska@mastercard.com)  
2023-07-05 - 8:35:52 PM GMT
-  Document e-signed by Joanna Lopatowska (Joanna.Lopatowska@mastercard.com)  
Signature Date: 2023-07-05 - 8:36:14 PM GMT - Time Source: server
-  Agreement completed.  
2023-07-05 - 8:36:14 PM GMT