CONFIDENTIAL

ENTERPRISE SERVICE AGREEMENT

This Enterprise Services Agreement (“Agreement”) is entered by and between Spreedly, Inc., a Delaware corporation, (“Spreedly”) and Lemonade, Inc., a Delaware corporation, (“Customer”). Spreedly and Customer are each a “Party” and collectively the “Parties”). This Agreement is effective on the last date of signature by a Party in the signature block below (“Effective Date”).

SPREEDLY

Name:	Spreedly, Inc.
Address:	300 Morris Street, Suite 400
City/State:	Durham, NC 27701

CUSTOMER

Name:	Lemonade, Inc.
Address:	5 Crosby Street, 3rd Floor
City/Country:	New York, NY 10013

PRIMARY SPREEDLY CONTACT

Name:	Allen Hooser
Title:	Senior Account Executive
Phone:	972-814-1322
Email:	abhooser@spreedly.com

PRIMARY CUSTOMER CONTACT

Name:	Denis Danskir
Title:	Billing Product Manager
Phone:	—-
Email:	denis.danskir@lemonade.com

SPREEDLY FINANCE CONTACT

Name:	Spreedly Accounting Department
Phone:	888-727-7750
Email:	accounting@spreedly.com

CUSTOMER BILLING CONTACT

Name:	**Accounts Payable**
Phone:	**—**
Email:	**ap@lemonade.com**

Background

Spreedly develops, markets and provides to its customers a web-based payments orchestration and tokenization service, which includes Spreedly’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 Spreedly supports, and, where applicable, automatically update expired or lost credit cards (the “Permitted Use”). 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.

Agreement

The Parties agree for themselves, their successors and permitted assigns as follows:

1. Definitions. As used in this Agreement, the following terms will have the meanings set forth below:

1.1. “Agreement” means, collectively, this Enterprise Services Agreement, the Order Form(s), the Statements of Work, the Support Services Terms, and the Data Security Policy, in each case as amended from time-to-time.

1.2. “Card Associations” means MasterCard, VISA, American Express, Discover, JCB or any other credit card brand or payment card network for or through which Spreedly processes payment card transactions.

1.3. “Card Data” means any credit card data uploaded or otherwise received from Customer by or through the Platform for the purposes of being processed within the Platform.

1.4. “Claim” means any claim, suit, action, proceeding, or investigation by a governmental body.

1.5. “Customer Data” means Card Data and any other data or information that is uploaded or otherwise received from Customer by or through the Platform for the purposes of being processed within the Platform (e.g., Customer’s customer names, addresses, and credit card information, etc.).

1.6. “Documentation” means the then-current online, electronic and written user documentation and guides, and instructional videos that Spreedly makes available to Customer at: https://docs.spreedly.com/, which describe the functionality, components, features or requirements of the Platform, as Spreedly may update from time-to-time in Spreedly’s discretion.

1.7. “Malicious Code” means any software, hardware or other technology, device or means, including any virus, worm, malware or other malicious computer code, the purpose or effect of which is to permit unauthorized access to, or to destroy, disrupt, disable, distort, or otherwise harm or impede in any manner any (a) computer, software, firmware, hardware, system or network or (b) any application or function of any of the foregoing or the security, integrity, confidentiality or use of any data processed thereby.

1.8. “Initial Order Form” means Order Form #1 executed by Customer and Spreedly concurrently with the execution and delivery of this Agreement.

1.9. “Intellectual Property Rights” means all patent rights, copyright rights, mask work rights, moral rights, rights of publicity, trademark, trade dress and service mark rights, goodwill, trade secret rights and other intellectual property rights as may now exist or hereafter come into existence, and all applications therefore and registrations, renewals and extensions thereof, under the Laws of any state, country, territory or other jurisdiction.

1.10. “Laws” means all laws, directives, rules and regulations.

1.11. “Losses” means any and all losses, damages, liabilities, deficiencies, judgments, settlements, costs and/or expenses (including reasonable attorneys’ fees).

1.12. “Order Form” means each ordering document which is substantially like the form in Schedule A that is executed by Customer and Spreedly that references this Enterprise Services Agreement. Each Order Form is hereby incorporated into this Agreement by reference, as amended from time-to-time by the Parties.

1.13. “PCI-DSS” means the Payment Card Industry Data Security Standard.

1.14. "Professional Services” means any consulting or professional services listed under a Statement of Work that are not included as part of the Support Services. Professional Services may include training, implementation, and configuration of the Platform.

1.15. “Statement of Work” means a written statement of work executed by Customer and Spreedly that references this Enterprise Services Agreement, each of which is hereby incorporated into this Agreement by reference, as amended from time-to-time by the Parties.

2. Provision and Use of the Platform.

2.1. Authorization to Use the Platform. Subject to the terms of this Agreement, Spreedly authorizes Customer, during the Term and on a non-exclusive and non-transferable (except as permitted in Section 14.5) basis, to access and use the Platform solely for the Permitted Use. Customer acknowledges and agrees that Spreedly is not a payment gateway or merchant account provider and Spreedly does not assume any direct or indirect liability or responsibility for Customer’s agreements with payment gateways or merchant account providers supported on the Platform.

2.2. Lawful Use. Customer will access and use the Platform, and Spreedly will provide Customer with access to the Platform, solely for lawful purposes and will not use it for any fraudulent, illegal or criminal purposes. Customer hereby grants Spreedly authorization to share information with law enforcement about Customer, Customer’s transactions and Customer’s Spreedly account, in each case if Spreedly receives a subpoena, Spreedly reasonably suspects that Customer’s use of the Platform has been for an unauthorized, illegal, or criminal purpose, and Spreedly gives Customer prior notice, unless Spreedly is prohibited by law to provide notice to Customer. Further, Spreedly reserves the right to not store or submit any transaction Customer submits that Spreedly believes is in violation of this Agreement or applicable Law or otherwise exposes Spreedly or other Spreedly users to harm, including but not limited to, fraud, illegal, and other criminal acts, but in this case, Spreedly shall give Customer a) prior advance notice, and b) the opportunity for Customer to store the Customer Data.

2.3. Limitations and Restrictions. Customer will use commercially reasonable efforts to prevent unauthorized third-party access to or use of the Platform. Customer must not do any of the following:

2.3.1. modify, adapt, translate or create derivative works or improvements of the Platform or any portion thereof;

2.3.2. rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise make available the Platform or any features or functionality of the Platform to any other person (other than Customer's policy holders for the purpose of paying Customer, consistent with the Permitted Use) or entity for any reason, including as part of any time-sharing, service bureau or software as a service arrangement;

2.3.3. reverse engineer, disassemble, decompile, decode, adapt or otherwise attempt to derive, gain access to or discover the source code of the Platform or the underlying structure, ideas, know-how, algorithms or methodology relevant to the Platform;

2.3.4. input, upload, transmit or otherwise provide to or through the Platform any information or materials that are unlawful or injurious, or contain, transmit or activate any Malicious Code;

2.3.5. attempt to gain unauthorized access to, damage, destroy, disrupt, disable, impair, interfere with or otherwise impede or harm in any manner the Platform;

2.3.6. access or use the Platform in any way that knowingly 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

2.3.7. access or use the Platform for purposes of (A) benchmarking or competitive analysis of the Platform, (B) developing, producing, marketing, distributing, licensing or selling any product or service that may compete with the Platform, or (C) disclosing to Spreedly's competitors, for any purpose, otherwise non-public information about the Platform.

2.4. Changes to the Platform. Spreedly may make any changes to the Platform (including, without limitation, the design, look and feel, functionality, content, material, information and/or services provided via the Platform) that Spreedly deems necessary or useful to improve the Platform or for any other reason, from time-to-time in Spreedly's sole discretion, and without notice to Customer; provided, however, that Spreedly will not make any such changes that will materially adversely affect its features or functionality available to Customer 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 Platform governed by all the provisions of this Agreement pertaining thereto.

2.5. Subcontractors. Spreedly may, in Spreedly's discretion, engage subcontractors to aid Spreedly in providing the Platform and performing Spreedly's obligations under this Agreement, but Spreedly will remain liable to Customer for any act or omission by such subcontractors that would be a breach or violation of this Agreement. Spreedly may use Amazon Web Services, Microsoft Azure, Google Cloud Platform 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 Platform, and such Reputable Hosting Services Provider will host and store certain portions of Customer Data that is processed through the Platform. Customer hereby specifically approves and consents to Spreedly's use of a Reputable Hosting Services Provider in the manner described and agrees that the Reputable Hosting Services Provider's security programs, policies, procedures, controls and technologies are consistent with industry best practices and comply with the requirements of the Data Security Policy.

2.6. Beta Services. Spreedly may offer Customer access to beta services that are being provided prior to general release ("Beta Services"). Beta Services will be clearly designated as beta, pilot, limited release, developer preview, non-production, evaluation or by a similar description. Beta Services are for evaluation purposes and not for production use, are not considered "services" under this Agreement, are not supported, and may be subject to additional terms. Spreedly may discontinue Beta Services at any time in its sole discretion and may never make them generally available. ALL BETA SERVICES ARE PROVIDED "AS-IS" AND "AS AVAILABLE," WITHOUT WARRANTIES OF ANY KIND. Spreedly will have no liability for any harm or damage arising out of or in connection with the use of Beta Services. If Customer provides feedback ("Feedback") about the Beta Services, Spreedly will be free to use, disclose, reproduce, distribute, implement or otherwise commercialize all Feedback provided by Customer without obligation or restriction. For the Beta Services only, the terms of this Section 2.6 supersede any conflicting terms and conditions in the Agreement, but only to the extent necessary to resolve conflict.

2.7. Suspension of Services and Platform Access. Spreedly may suspend or deny Customer's access to or use of all or any part of the Platform and Support Services, without any liability to Customer or others, if (i) Spreedly is required to do so by Law or court order; or (ii) Customer has (A) failed to comply with Section 2.2 or 2.3), or (B) otherwise breached a material term of this Agreement and have failed to cure such breach within ten (10) days after Spreedly provides written notice thereof to Customer. Spreedly's remedies in this Section are in addition to, and not in lieu of, Spreedly's termination rights in Section 10.

2.8. Customer Data Export; Customer Data Retention. Customer may elect at any time to perform an automatic export of any Card Data and/or other Customer Data to a third-party endpoint for which Spreedly supports third-party vaulting as set forth at Spreedly's website (currently: https://docs.spreedly.com/guides/third-party-vaulting. For any endpoint for which automatic export is not supported, Customer may request that Spreedly perform one (1) free-of-charge manual export during the Term, of any Card Data or other credit card or user information associated with Customer's account to a recipient designated by Customer, provided that the recipient has proven that it is PCI-DSS compliant, and the transfer is not in violation of any applicable Laws. If Customer requires additional manual exports during the Term, each additional manual export will incur an export charge at Spreedly' then-current rates. Upon the expiration or termination of the Agreement for any reason, Spreedly shall, free of charge, deliver to Customer a complete and accurate export of all Customer Data and Card Data in an encrypted, password-protected file via SFTP, at Customer's option, within ten (10) days after the expiration or termination of the Agreement. Spreedly reserves the right to delete all of Customer's Card Data and any other Customer Data thirty (30) days after the later of: a) the date that Customer confirms that it received and can access the final export, or b) effective date of termination of this Agreement (the "Data Transfer Window"). If Customer requires to arrange the additional export of its Card Data to a PCI-DSS compliant third party, it may extend the Data Transfer Window for additional thirty (30) day periods by providing notice to Spreedly and continuing to pay a prorated portion of the applicable Fees set forth in the Order Forms.

3. Support Services and Availability.

3.1. Support Services. During the Term, so long as Customer complies with this Agreement, Spreedly will provide customer support services (the "Support Services") to Customer in accordance with Spreedly's Support Service Terms appended as Schedule C.

3.2. Availability. During the Term, so long as Customer complies with this Agreement, Spreedly will make the Platform available for access and use by Customer in accordance with Spreedly's Availability Commitments in Schedule C, corresponding to the support level specified on the Order Form. SPREEDLY'S SOLE OBLIGATION AND LIABILITY TO CUSTOMER FOR ANY FAILURE TO MEET THE AVAILABILITY COMMITMENTS ARE THE SERVICE CREDITS SPECIFIED IN THE SUPPORT SERVICE TERMS REFERENCED ABOVE.

4. Professional Services. If Customer and Spreedly execute a written Statement of Work for Professional Services, the following additional terms will apply:

4.1. Scope of Services; Statements of Work. Subject to the terms of this Agreement, Spreedly will perform the training, consulting, advisory, implementation, configuration, customization and/or other professional services (the "Professional Services") that are mutually agreed upon and described in one or more Statements of Work.

4.2. Personnel. Spreedly reserves the right to determine which of Spreedly's personnel or subcontractors will be assigned to perform Professional Services, and to replace or reassign such personnel during the Term; provided, however, that Spreedly shall devote sufficient resources to ensure that the Services are performed in a timely and reliable manner.

4.3. Customer Responsibilities. In connection with Spreedly's provision of the Professional Services, Customer will: (i) reasonably cooperate with Spreedly in all matters relating to the performance of the Professional Services; (ii) respond promptly to Spreedly's requests to provide direction, information, approvals, authorizations or decisions that are reasonably necessary for Spreedly to perform the Professional Services in accordance with the Statement of Work; (iii) provide the content, data and materials that Customer 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 ("Customer Responsibilities"). Customer understands and agrees that Spreedly's performance is dependent on Customer's timely and effective satisfaction of Customer Responsibilities.

4.4. Spreedly shall provide the professional services (a) in accordance with the terms and subject to the conditions set forth in the respective Statement of Work and this Agreement; (b) using personnel of required skill, experience, and qualifications; (c) in a timely, workmanlike, and professional manner; (d) in accordance with the highest professional standards in Spreedly's field; and (e) to the reasonable satisfaction of Customer.

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

4.6. Ownership of Work Product. Unless Customer and Spreedly have otherwise expressly provided in a Statement of Work (including by making a specific reference to this Section 4.5), all Deliverables (as defined below) will be deemed to be a part of the Platform hereunder and therefore owned by Spreedly (pursuant to Section 8.1 below) and provided to Customer (pursuant to Section 2.1 above) under the terms of this Agreement. "Deliverables" means all results and proceeds of the Professional Services provided by Spreedly.

4.7. Acceptance of Deliverables. If Customer reasonably believes that any final Deliverable provided by Spreedly as part of Professional Services fails to conform in some material respect to the specifications set forth in the applicable Statement of Work, then Customer will provide Spreedly with a detailed written description of each alleged non-conformance within ten (10) business days after receipt of such Deliverable. In such an event, Spreedly will either confirm the non-conformance and commence work on making corrections to such Deliverable or inform Customer that Spreedly does not agree that a non-conformance exists and provide Customer with a written explanation for Spreedly's conclusion. If Spreedly does not agree that a non-conformance exists, Customer and Spreedly agree to work together in good faith to try to resolve the matter. If Spreedly does not receive a non-conformance notice from Customer 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.

5. Confidentiality.

5.1. Confidential Information. In connection with this Agreement, each Party (as the "Disclosing Party") may disclose or make available its Confidential Information to the other Party (as the "Receiving Party"). "Confidential Information" means all proprietary, non-public information or materials of any character, whether written, electronic, verbal or otherwise furnished by the Disclosing Party or its directors, officers, employees, consultants, contractors, agents or advisors that (i) is marked or otherwise identified as "Confidential" and/or "Proprietary" (or, if disclosed verbally, is reduced to writing and marked or identified as "Confidential" and/or "Proprietary" and forwarded to the other Party within thirty (30) days of oral disclosure) or (ii) should reasonably be understood from all the relevant circumstances to be of confidential or of a proprietary nature, including but not limited to, all (A) trade secrets, (B) financial information and pricing, (C) technical information, such as research, development procedures, algorithms, data, designs, and know-how, (D) individually identifiable personal information, (E) business and operational information, such as planning, marketing interests, pricing and products, and (F) customer lists and all related information. For avoidance of doubt, all non-public information related to the Platform (including without limitation, pricing information (*e.g.,* price quotes) and the source code for the Platform and the methods, algorithms, structure and logic, technical infrastructure, techniques and processes used by Spreedly in developing, producing, marketing and/or providing the Platform) are Spreedly's Confidential Information, Customer Data is Customer's Confidential Information, and the terms of this Agreement and any Order Form or Statement of Work are the Confidential Information of both Parties.

5.2. Exclusions. Confidential Information of a Disclosing Party 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 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 or any of its Representatives' (as defined in Section 5.3 below) 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; or (iv) was or is independently developed by the Receiving Party without reliance upon any Confidential Information.

5.3. Protections. As a condition to being provided with any disclosure of or access to Confidential Information, the Receiving Party will: (i) not use the Disclosing Party's Confidential Information other than as necessary to exercise its rights or perform its obligations under and in accordance with this Agreement; (ii) except as may be permitted under the terms and conditions of Section 5.4 below, not disclose or permit access to such Confidential Information other than to its affiliates and its affiliates' respective officers, employees, directors, attorneys, accountants, professional advisors, contractors, subcontractors, agents and/or consultants (collectively, its "Representatives") who: (x) 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; and (y) have been informed of the confidential nature of the Confidential Information and the Receiving Party's obligations under this Agreement; (iii) safeguard the Confidential Information from unauthorized use, access or disclosure using at least the degree of care it uses to protect its own Confidential Information and in no event less than a reasonable degree of care; and (iv) promptly notify the Disclosing Party of any unauthorized use or disclosure of Confidential Information of which it becomes aware and take all reasonable steps to prevent further unauthorized use or disclosure. Each Party will be liable for any breach of this Agreement by its Representatives to whom it discloses Confidential Information.

5.4. Legally Required Disclosures. If a Receiving Party or one of its Representatives is required by any Law, rule or order of any governmental body or agency, or as otherwise necessary to maintain or comply with any regulatory certifications or requirements, to disclose any Confidential Information, such Receiving Party (i) will, to the extent legally permissible, give the Disclosing Party prompt notice of such request so that the Disclosing Party may (at its own expense) seek an appropriate protective remedy, and (ii) will, and will cause its Representatives to, cooperate with the Disclosing Party (at the Disclosing Party's expense) in the Disclosing Party's efforts to obtain any such protective remedy. In the event that the Disclosing Party is unable to obtain such a protective remedy, the Receiving Party or its Representatives, as applicable, will (A) furnish only that portion of the Confidential Information that the Receiving Party or its Representatives is required to disclose in the opinion of the Receiving Party's or its Representatives' outside counsel, (B) exercise reasonable efforts to assist the Disclosing Party (at the Disclosing Party's expense) in obtaining assurances that confidential treatment will be accorded the Confidential Information so required to be disclosed, and (C) give notice to the Disclosing Party of the information to be disclosed as far in advance of disclosure of the same as is reasonably possible and legally permissible.

5.5. Ownership. All Confidential Information will remain at all times the sole and exclusive property of the Disclosing Party and the Receiving Party will not acquire any rights in or to such Confidential Information by reason of its disclosure to the Receiving Party hereunder.

6. Data Protection and Privacy.

6.1. Data Security. During the Term, Spreedly will implement commercially reasonable safeguards to protect against unauthorized access to the Platform and anticipated threats or hazards to the security, confidentiality or integrity of Customer Data in accordance with Spreedly's Data Security Policy described in Schedule B, as amended from time-to-time (the "Data Security Policy") and applicable law, provided however that no amendments shall materially reduce the security of Customer Data from the version in effect at the time this Agreement became effective.

6.2 Data Privacy. In the event that the Parties enter into an Order Form and/or SOW whereby Spreedly collects, accesses, processes, stores, transfers, transmits, uses, discloses or otherwise handles any Customer Data that includes "personal information," "personal data" or "personally identifiable information" as defined under applicable law, the Parties will comply with the Data Processing Addendum attached thereto as Schedule D, which is hereby incorporated into this Agreement by reference.

7. Fees and Payment.

7.1. Fees. Customer will pay to Spreedly the fees and charges described in each Order Form and Statement of Work entered into by Customer and Spreedly (the "Fees") in accordance with such Order Form or Statement of Work and this Section 7. All purchases are final, all payment obligations are non-cancelable and (except as otherwise expressly provided in this Agreement or in the applicable Order Form or Statement of Work) all Fees once paid are non-refundable.

7.2. Taxes. If Spreedly is required by law to pay, withhold or deduct any taxes, levies, imports, duties, charges, fees or other amounts from Customer's payments, such amounts will be invoiced to and paid by Customer in addition to the Fees, unless Customer provides Spreedly with a valid exemption certificate from the corresponding authority. If Customer is required by law to withhold or deduct any portion of the Fees due to Spreedly (a "Customer Withholding"), Spreedly will be entitled to "gross-up" the applicable Fees in an amount equal to the Customer Withholding so that Spreedly receives the same Fees it would have received but for the withheld amounts required by law. Customer remains liable for the payment of all such Customer Withholdings, however designated, that are levied or based on Customer's use of the Platform.

7.3. Payment. Customer will make all payments in US dollars. Unless otherwise set forth in an applicable Order Form or Statement of Work, all invoiced amounts are due net forty-five (45) days from the invoice date. Customer is responsible for providing complete and accurate billing and contact information and notifying Spreedly of any changes to that information. If Customer reasonably disputes the accuracy of any invoice, Customer will notify Spreedly, in which case any undisputed amounts will be paid, and the parties will engage in good faith discussions to timely resolve any questions or disagreements regarding the disputed amounts.

7.4 Late Payment. If Customer fails to make any payment within thirty (30) days of the due date then, in addition to all other remedies that may be available to Spreedly (including Spreedly's rights under Section 2.7 and Section 9.3), Spreedly may charge interest on the past due amount at the rate of 1% per month calculated daily and compounded monthly or, if lower, the highest rate permitted under applicable law.

8. Ownership and Intellectual Property Rights.

8.1. Platform and Documentation. Customer acknowledges and agrees that Spreedly owns all right, title and interest in and to the Platform and the Documentation, including all Intellectual Property Rights therein and all derivative works thereof. Spreedly is not granting Customer any right, license or authorization with respect to the Platform or the Documentation, except as specifically provided in Section 2.1 above (and subject to the limitations and restrictions in Section 2.3 above). Spreedly reserves all rights not expressly granted to Customer in this Agreement.

8.2. Customer Data. As between Customer and Spreedly, Customer is and will remain the sole and exclusive owner of all right, title and interest in and to all Customer Data, including all Intellectual Property Rights therein, subject to the rights Customer grants to Spreedly in this Section 8. During the Term, Customer hereby grants to Spreedly and its subcontractors all such rights and permissions in or relating to Customer Data as are necessary to: (i) provide the Platform to Customer; and (ii) enforce this Agreement and exercise Spreedly's rights and perform Spreedly's obligations under this Agreement.

8.3. Improvements. To the extent Spreedly makes any improvements to the Platform based upon Customer's use of the Platform, Customer agrees that Spreedly exclusively owns all right, title and interest in and to such improvements, including all related Intellectual Property Rights.

8.4. Usage Data. Customer acknowledges and agrees that Spreedly may collect metadata and other statistical information regarding Customer's use of and the performance of the Platform ("Usage Data"). Usage Data does not contain and is not derived from Customer Data. Customer agrees that Spreedly may use Usage Data in connection with providing Support Services to Customer and for Spreedly's internal business purposes (such as monitoring, enhancing and improving the Platform), and that Spreedly may publish and share with third parties aggregated Usage Data that cannot, by itself or with other data, directly or indirectly, identify Customer, Customer's customers or clients or any other individual or entity.

8.5. Publicity Rights. During the Term, Customer agrees that Spreedly may, with separate written consent from Customer, include Customer's name, trademarks and logos on Spreedly's website and in other sales and marketing materials in order to factually identify Customer as a current customer.

9. Term and Termination.

9.1. Term. Unless otherwise terminated in accordance with this Agreement, the initial term of this Agreement will be for the duration specified in the Initial Order Form (the "Initial Term"). Thereafter, this Agreement (excluding any Order Form(s)) will automatically renew for successive renewal terms (each, a "Renewal Term" and, together with the Initial Term, the "Term"), subject to, and in accordance with, the terms of the Initial Order Form. Unless otherwise mutually agreed upon by the Parties, the term of each additional Order Form will be the same as the term set forth in the Initial Order Form.

9.2. Termination. In addition to any other termination rights described in this Agreement, this Agreement may be terminated at any time by either Party, effective when that Party provides written notice to the other Party: (i) at any time that there are no active and outstanding Order Forms and Statements of Work; or (ii) if the other Party materially breaches the terms of this Agreement (including, for avoidance of doubt, the terms of any Order Form or Statement of Work incorporated herein) and such breach remains uncured five (5) days after the non-breaching Party provides the breaching Party with written notice regarding such breach. For the purposes of this Agreement, a material breach includes but is not limited to, Spreedly's inability to process payments for Customer (due to issues with the Platform, API or otherwise), breach of confidentiality, and breach of the Data Security Policy.

9.3. Effect of Termination. The exercise of any right of termination under this Agreement will not affect any rights of either Party (including rights to payment or reimbursement) that have accrued prior to the effective date of termination and will be without prejudice to any other legal or equitable remedies to which a Party may be entitled. If this Agreement is terminated or expires, then: (i) Customer will complete all pending transactions and stop accepting new transactions through the Platform; (ii) Customer will discontinue use of any Spreedly trademarks and immediately remove any Spreedly references and logos from Customer's website. .

Notwithstanding anything to the contrary herein, upon the termination or expiration of this Agreement for any reason Spreedly shall: (a) deliver to Customer all Customer Confidential Information, Customer Data, and any other Customer data, materials and deliverables in Spreedly's possession and related to its performance under this Agreement, and (b) reasonably cooperate with Customer for the transition of the Services to Customer and/or Customer's vendor(s). Upon written request by Customer made prior to the expiration date, Spreedly will continue to provide access and use of the Platform and will cooperate in the transition of services to a replacement service provider ("Transition Services") for additional fees and subject to the same terms, provided however, no Transition Services will be provided by Spreedly until: (i) Customer has fully paid all outstanding amounts that are due pursuant to Section 7 and the applicable Order Form or Statement of Work; and (ii) the parties mutually agree on the duration and a date for completion of the Transition Services in writing.

9.4. Surviving Terms. Sections 1 (Definitions), 5 (Confidentiality), 7 (Fees and Payment), 8 (Ownership and Intellectual Property Rights), 9.3 (Effect of Termination), 10.c (Disclaimer of Warranties), 11 (Indemnification), 13 (Limitations of Liability), 14 (Miscellaneous) and this Section 9.4 will survive any expiration or termination of this Agreement along with any provision which by its nature or express terms should survive termination.

10. Representations and Warranties.

10.1. Mutual Representations. The Parties each represent and warrant as applicable that: (i) it is 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; (ii) it has the full right, power and authority to enter into and perform its obligations under this Agreement; (iii) the execution of an Order Form by its representative has been duly authorized by all necessary corporate or organizational action of Customer; and (iv) when executed and delivered by both Parties, the Agreement will constitute the legal, valid and binding obligation of Customer, enforceable against Customer in accordance with its terms

10.2. Customer Representations. Customer represents and warrants that: (i) it will not use the Platform, directly or indirectly, for any fraudulent undertaking or in any manner so as to interfere with the use of the Platform; (ii) Customer's use of the Platform and its collection and use of all of Customer Data (including Customer's processing of Customer Data and/or any card authorization, credit, ticket only, capture or settlement request, decline transaction, or other related transaction, completed or submitted under Customer's account) will comply with (A) all applicable Laws, (B) the terms of service of the payment gateways, merchant service providers and/or API endpoints Customer connects with on the Platform; (C) 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; (D) PCI-DSS and PA-DSS, as applicable; and (E) any regulatory body or agency having jurisdiction over the subject matter thereof; (iii) Customer either owns, or has all rights, permissions and consents that are necessary to process, and to permit Spreedly, its subcontractors and the Platform to process as contemplated in this Agreement, all Customer Data and the credit card transaction related thereto; (iv) Spreedly's and its subcontractors' access to and use of Customer Data (including, for the avoidance of doubt, the Card Data and all personal data included with Customer 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.

10.3. Spreedly Representations. Spreedly represents and warrants that:

10.3.1. it will comply with all applicable rules and guidelines regarding service providers, third-party agents and processors as issued by the Card Associations (the "Card Rules"), as updated from time to time, and including Card Rules applicable to U.S. and international credit card transactions;

10.3.2. it will (A) be compliant with PCI-DSS and all other applicable standards and guidelines issued by the PCI Security Standards Council, LLC, (the "Council"); (B) validate its PCI-DSS compliance as required by the applicable Card Rules; (C) undergo annual PCI-DSS assessments by a Qualified Security Assessor; and (D) notify Customer if it becomes aware that it is no longer in compliance with PCI-DSS. Spreedly will provide proof of its PCI-DSS compliance to Customer upon request and evidence of its successful completion of its annual assessments on its website (currently available at https://www.spreedly.com/pci);

10.3.3. the Platform will perform in all material respects in accordance with the functional specifications set forth in the applicable Documentation. If Spreedly breaches this warranty, as Spreedly's sole obligation and liability to Customer and Customer's sole and exclusive remedy , Spreedly will, at its option: (a) promptly correct any portion of the Platform that fails to meet this warranty; (b) provide Customer with a reasonable procedure to circumvent the nonconformity; or (c) refund to Customer on a *pro rata* basis the share of any Fees prepaid by Customer for the portion of the applicable Term in which the Platform is non-conforming;

10.3.4. it will perform all Professional Services in a professional and workmanlike and timely manner and in accordance with industry standards and applicable Laws. If Spreedly breaches this warranty, as Spreedly's sole obligation and liability to Customer and Customer's sole and exclusive remedy , Spreedly will promptly re-perform the non-conforming Services at no additional cost to Customer.

10.3.5 the Platform do not and will not violate or infringe upon the intellectual property right or any other right whatsoever of any third party.

10.4. Disclaimer of Warranties. EXCEPT FOR THE EXPRESS LIMITED WARRANTIES SET FORTH IN THIS AGREEMENT, THE PLATFORM AND ALL SERVICES PROVIDED BY SPREEDLY HEREUNDER ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS AND SPREEDLY HEREBY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHER, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. WITHOUT LIMITING THE FOREGOING, NEITHER SPREEDLY NOR ANYONE ASSOCIATED WITH SPREEDLY, INC. REPRESENTS OR WARRANTS THAT THE PLATFORM WILL BE RELIABLE, ERROR-FREE OR UNINTERRUPTED, THAT DEFECTS WILL BE CORRECTED OR THAT THE PLATFORM WILL OTHERWISE MEET CUSTOMER'S NEEDS OR EXPECTATIONS.

11. Indemnification.

11.1. Spreedly Indemnification. Spreedly will defend Customer from and against any Claims brought by a third party, and will indemnify and hold Customer harmless from any Losses associated with such third party Claims arising from: (i) an allegation that the Platform (excluding Customer Data) infringes any U.S. patent, copyright or trademark of such third party, or misappropriate the trade secret of such third party (each, an "Infringement Claim"); (ii) a "Data Incident" that is caused by Spreedly's material breach of the Data Security Policy (as defined in Schedule B attached hereto); (iii) Spreedly's failure to remain compliant with PCI-DSS; or (iv) breach of this Agreement or violation of any law.

11.2. Customer Indemnification. Customer will defend Spreedly and Spreedly's subcontractors and personnel from and against any Claims brought by a third party, and Customer will indemnify and hold Spreedly and Spreedly's subcontractors and personnel harmless from any Losses associated with such third party Claims, in each case to the extent the same are based on (i) Customer's use of the Platform in violation of the terms of this Agreement and/or any applicable Law, and/or (ii) Customer's breach of Section 5 (Confidentiality).

11.3. Indemnification Process. Each Party will promptly notify the other Party in writing of any Claim for which such Party believes it is entitled to be indemnified pursuant to Section 11.1 or 11.2. The Party seeking indemnification (the "Indemnitee") will cooperate with the other Party (the "Indemnitor") at the Indemnitor's sole cost and expense. The Indemnitor will promptly assume control of the defense and investigation of such Claim and will employ counsel of its choice to handle and defend the same, at the Indemnitor's sole cost and expense. The Indemnitee's failure to perform any obligations under this Section 11.3 will not relieve the Indemnitor of its obligations under this Section 11 except to the extent that the Indemnitor can demonstrate that it has been materially prejudiced as a result of such failure. The Indemnitee may participate in and observe the proceedings at its own cost and expense with counsel of its own choosing. The Indemnitor will not enter into any settlement that imposes any liability or obligation on the Indemnitee without the Indemnitee's prior written consent.

11.4. Additional Terms for Infringement Claims.

11.4.1. Spreedly will have no liability or obligation with respect to any Infringement Claim to the extent based upon or arising out of: (A) access to or use of the Platform in combination with any hardware, system, software, network or other materials or service not provided or otherwise approved by Spreedly in the Platform Documentation; (B) use of the Service in the practice of a process or system other than that for which it was intended; or (C) any action taken by Customer relating to use of the Platform that is outside the scope of the rights and authorizations granted or otherwise in breach of this Agreement and/or any applicable Order Form.

11.4.2. If the Platform is, or in Spreedly's opinion is likely to be, the subject of an Infringement Claim, or if Customer's use of the Platform is enjoined or threatened to be enjoined, Spreedly may, at Spreedly's option and Spreedly's sole cost and expense: (A) obtain the right for Customer to continue to use the allegedly infringing Platform as contemplated by this Agreement, (B) modify or replace the allegedly infringing Platform to make the Platform (as so modified or replaced) non-infringing, or (C) if Spreedly determine the remedies in clauses (A) and (B) are not commercially reasonable, then Spreedly may terminate the applicable Order Form upon written notice and without any liability to Customer and Spreedly will promptly refund to Customer on a *pro rata* basis the share of any Fees prepaid by Customer for the future portion of the applicable Term that would have remained but for such termination.

11.4.3 THIS SECTION 11 SETS FORTH CUSTOMER'S EXCLUSIVE REMEDIES, AND SPREEDLY'S SOLE OBLIGATION AND LIABILITY TO CUSTOMER OR ANY OTHER PERSON OR ENTITY, FOR ANY ACTUAL, THREATENED OR ALLEGED CLAIMS THAT THE PLATFORM (INCLUDING CUSTOMER'S USE THEREOF) INFRINGES, MISAPPROPRIATES OR OTHERWISE VIOLATES ANY INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

12. Insurance. During the Term, Spreedly will maintain (i) commercial general liability insurance with at least $1,000,000 per occurrence and (ii) "errors and omission" (tech and cyber coverage) insurance in an amount not less than $5,000,000. Upon Customer's request, Spreedly will provide Customer with a certificate of insurance evidencing the same.

13. Limitation of Liability. IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY LOST PROFITS, LOSS OF ANTICIPATED SAVINGS, WASTED EXPENDITURE, LOSS OF BUSINESS OPPORTUNITIES, REPUTATION OR GOODWILL, LOSS OR CORRUPTION OF DATA OR ANY INDIRECT, EXEMPLARY, PUNITIVE, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF BUSINESS PROFITS) ARISING OUT OF OR RELATING TO THIS AGREEMENT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THE TOTAL AND CUMULATIVE LIABILITY OF A PARTY ARISING UNDER OR IN CONNECTION WITH THIS AGREEMENT WILL NOT EXCEED TWO TIMES THE AMOUNT OF FEES PAID TO SPREEDLY BY CUSTOMER DURING THE TWELVE-MONTH PERIOD IMMEDIATELY PRECEDING SUCH CLAIM, PROVIDED HOWEVER, THAT THIS LIMIT ON LIABILITY WILL NOT APPLY TO THE EXTENT THE LIABILITY IS A DIRECT RESULT OF THE FRAUDULENT, CRIMINAL OR GROSSLY NEGLIGENT OR MORE CULPABLE ACTS OR OMISSIONS OF THAT PARTY, FRAUDULENT REPRESENTATION, DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE OR ANY MATTER FOR WHICH IT WOULD BE UNLAWFUL FOR THE PARTIES TO EXCLUDE LIABILITY. THE LIMITATIONS IN THIS SECTION WILL APPLY EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

14. Miscellaneous.

14.1. Entire Agreement. This Agreement and each Order Form and Statement of Work constitute the entire agreement, and supersede all prior negotiations, understandings or agreements (oral or written), between the Parties regarding the subject matter of this Agreement (and all past dealing or industry custom).

14.2. Amendment, Severability and Waiver. No change, consent or waiver under this Agreement will be effective unless in writing and signed by the Party against which enforcement is sought. Any delay or failure of either Party to enforce its rights, powers or privileges under this Agreement, at any time or for any period, will not be construed as a waiver of such rights, powers and privileges, and the exercise of one right or remedy will not be deemed a waiver of any other right or remedy. If any provision of this Agreement is determined to be illegal or unenforceable, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable.

14.3. Governing Law and Venue. This Agreement will be deemed to have been made in and will be governed by and construed in accordance with the laws of the State of New York, without regard to its conflicts of law provisions. The sole jurisdiction and venue for actions related to this Agreement will be the state or federal courts located in New York, New York, and both Parties consent to the exclusive jurisdiction of such courts with respect to any such action.

14.4. Notices. All notices, instructions, requests, authorizations, consents, demands and other communications hereunder will be in writing and will be delivered by one of the following means, with notice deemed given as indicated in parentheses: (i) by personal delivery (when actually delivered); (ii) by overnight courier (upon written verification of receipt); (iii) by email (upon confirmation of receipt); or (iv) by certified or registered mail, return receipt requested (upon verification of receipt). In each case, such notices will be addressed to a Party at such Party's address set forth in the Initial Order Form (or such other address as updated by such Party from time-to-time by giving notice to the other Party in the manner set forth in this Section 14.4).

14.5. Assignment. Neither Party may assign, delegate or otherwise transfer its rights or obligations under this Agreement without the prior written consent of the other Party; provided that either Party may assign this Agreement in its entirety without the other Party's consent to an entity that acquires all or substantially all of the business or assets of such Party to which this Agreement pertains, whether by merger, reorganization, acquisition, sale or otherwise. This Agreement will be binding upon, and inure to the benefit of, the successors and permitted assigns of the Parties.

14.6. 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 will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Agreement.

14.7. Relationship of the Parties. The relationship between the Parties is that of independent contractors. Nothing contained in this Agreement will 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 will have authority to contract for or bind the other Party in any manner whatsoever.

14.8. Force Majeure. Neither Party will be liable for any delays or non-performance of its obligations arising out of actions or decrees of governmental authorities, criminal acts of third parties, epidemics and/or pandemics as designated by governing authorities, earthquakes, flood, and other natural disasters, war, terrorism, acts of God, or fire, or other similar causes not within such Party's reasonable control (each, a "Force Majeure Event"). In the event of any failure or delay caused by a Force Majeure Event, the affected Party will give prompt written notice to the other Party stating the period of time the occurrence is expected to continue and use commercially reasonable efforts to end the failure or delay and minimize the effects of such Force Majeure Event. Either Party may terminate this Agreement if a Force Majeure Event affecting the other Party continues substantially uninterrupted for a period of thirty (30) days or more.

14.9. Equitable Remedies. Each Party acknowledges and agrees that a breach or threatened breach by such Party of any of its obligations under Section 2.c (Limitations and Restrictions), Section 5 (Confidentiality) or Section 8 (Intellectual Property Rights) of this Agreement would cause the other Party irreparable harm for which monetary damages would not be an adequate remedy and that, in the event of such breach or threatened breach, the other Party will be entitled to equitable relief, including in a restraining order, an injunction, specific performance and any other relief that may be available from any court of competent jurisdiction, 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.

14.10. Conflict in Terms. If there is a conflict between this Agreement and any Order Form or Statement of Work, the terms of such Order Form or Statement of Work will govern the provision of the Platform or the Professional Services involved; provided, however, that nothing in an Order Form or Statement of Work may modify or supersede anything in Sections 2.3 (Limitations and Restrictions), 4.5 (Ownership of Work Product), 8 (Ownership and Intellectual Property Rights), 10 (Representations and Warranties), 11 (Indemnification), 13 (Limitation of Liability), or 14 (Miscellaneous) of this Agreement unless an express cross-reference is made to the relevant provision of this Agreement in the applicable Order Form or Statement of Work and the Parties have expressly agreed in such Order Form or Statement of Work to modify or alter the relevant provision of this Agreement.

14.11. Counterparts. This Agreement may be executed in two or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument. Counterparts may be delivered via facsimile, electronic mail (including pdf or any electronic signature complying with the U.S. federal ESIGN Act of 2000, *e.g.*, www.docusign.com) or other transmission method and any counterpart so delivered will be deemed to have been duly and validly delivered and be valid and effective for all purposes.

The Parties have executed this Agreement by their duly authorized representatives in one or more counterparts, each of which will be deemed an original.

Spreedly, Inc.	Lemonade, Inc.
(“**Spreedly**”)	(“**Customer**”)
Justin Benson 391744E614CFD0F21AF830DF74E3408B contractworks	Tim Bixby EB45D2083341155EC9DFE362FEC3A48A contractworks
Authorized Signature	Authorized Signature
Justin Benson	**Tim Bixby**
Print Name	Print Name
CEO	**CFO**
Title	Title
09/29/2023	**09/29/2023**
Date	Date

SCHEDULE A

ORDER FORM [#]

Spreedly, Inc.
300 Morris Street
Suite 400
Durham, NC 27701

Order Form

Issued: Offer Valid

Until:

To:
Customer Legal
Name: 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.

SCHEDULE B

Data Security Policy

This Data Security Policy describes Spreedly's standard information security controls and is hereby incorporated into and made a part of the Enterprise Service Agreement between the Parties. Any capitalized terms used but not defined herein will have the meaning described in the Agreement. In the event of any conflict between the terms of the Agreement and this Data Security Policy, this Data Security Policy will govern with respect to the security measures in place for Customer Data.

A. Definitions.

A.1. "Data Incident" means a breach of Spreedly's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on the Platform. "Data Incidents" exclude unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

A.2. "Security" means Spreedly's technological, physical, administrative and procedural safeguards, including without limitation, policies, procedures, guidelines, practices standards, controls, hardware, software, firmware and physical security measures, the function or purpose of which is, in whole or part, to: (a) protect the confidentiality, integrity or availability of Customer Data and the Platform; (b) prevent the unauthorized use of or unauthorized access to the Platform; or (c) prevent a breach or malicious infection of Customer Data.

B. Data Security.

B.1. Security Controls. Spreedly uses industry-accepted technological, physical, administrative, procedural safeguards, methods and products, including without limitation, policies, procedures, guidelines, practices standards, controls, hardware, software, firmware and physical security measures, the function or purpose of which is to: (a) protect the confidentiality, integrity or availability of Customer Data and the Platform; and (b) prevent the unauthorized use of or unauthorized access to the Platform. Spreedly agrees that beginning on the Effective Date of the Agreement, Spreedly will employ and maintain, at a minimum, the reasonable and appropriate security controls listed in Attachment 1 attached hereto and incorporated by reference.

B.2. Data Ownership and Use Limitations. As between Spreedly and Customer, Customer is the owner of any and all Customer Data, including information provided by Customer's clients, customers or users, and Spreedly will have no ownership rights or interest in the Customer Data. Spreedly will use, process and handle Customer Data solely for the purpose of providing services under the Agreement and only per the instructions of Customer.

B.3. Data Deletion. Upon termination of the Agreement for which Spreedly is processing Customer Data, Spreedly will, upon Customer's request and subject to the limitations described in the Agreement, delete Customer Data in accordance with the procedures and timeframes specified in the Agreement.

B.4. Data Tokenization. Tokenization is a process by which the primary account number (PAN) is replaced with a surrogate value called a token. Tokenization promotes security and efficiency between the Platform and connected payment gateways. When available, Spreedly may at its sole discretion tokenize applicable Customer Data for use within the Platform.

B.5. Third-Party Audit and Compliance. Spreedly undergoes annual PCI-DSS assessments by a Qualified Security Assessor and annual SOC 2 Type 2 audits performed by an external third-party. The copy of the most recent Attestation of Compliance with PCI-DSS is available at www.spreedly.com/pci and Spreedly will provide a copy of its most recent SOC 2 Type 2 upon Customer's request.

B.6. Use of Subcontractors. Prior to utilizing any subcontractor, vendor, or other third party, Spreedly will conduct a reasonable, documented investigation of such third party to ensure the third party can comply with the privacy, confidentiality and security requirements of Customer Data that are at least as protective of Customer Data as the requirements imposed on Spreedly under this Data Security Policy. Spreedly will ensure that its Subcontractors comply with the terms of this Policy.

B.7. Additional Controls. Spreedly may update the security controls in Exhibit A from time to time upon notice to Customer and implement and maintain additional security controls in the event of any material changes to the Platform, available technology or systems, provided that such changes or additional controls will not materially reduce Spreedly's obligations under this Data Security Policy. In the event of any material change (including changes due to a change in applicable Law) which requires a change to all or a significant part of the security controls, services or the Platform, the parties agree to make appropriate adjustments to the terms of the Agreement utilizing the amendment process.

B.8. Spreedly's Obligations.

Spreedly shall collect, retain, use, disclose, and/or otherwise process Customer Data only for the purpose of providing the Platform under the Agreement and this Addendum. Without limiting Spreedly's obligations as set forth above, Spreedly shall not:

a. share, sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, Customer Data to another person or entity: (i) for monetary or other valuable consideration; or (ii) for cross-context behavioural advertising, whether or not for monetary or other valuable consideration;

b. retain, use, or disclose Customer Data for any purpose other than to perform its obligations under the Agreement, which for the avoidance of doubt prohibits Spreedly from retaining, using, or disclosing Customer Data outside of the direct business relationship with Customer, or for any purpose other than the business purpose specified in the Agreement. For the avoidance of doubt, Spreedly shall be prohibited from retaining, using, or disclosing Customer Data for any commercial purpose; or

c. combine Customer Data with personal data Spreedly receives from or on behalf of another person or entity.

Upon Customer's request, Spreedly shall provide such assistance as Customer reasonably requires in ensuring compliance with Customer's obligations under applicable data protection laws, including but not limited to responding to requests by data subjects to exercise rights afforded them under data protection laws. At a minimum, Spreedly shall maintain the ability to access, modify, remove from processing, or irrevocably delete or destroy the personal information of an individual data subject when requested by Customer. If Spreedly receives a request from a data subject to exercise a right under applicable data protection laws, Spreedly shall promptly notify Customer, and shall await instructions from Customer concerning whether, and how, to respond to such a request.

C. Data Incident Response.

C.1. Response Actions. In the event of a Data Incident, Spreedly will:

C.1.1. promptly conduct a reasonable investigation of the reasons for and circumstances of such Data Incident;

C.1.2. take all reasonably necessary actions to prevent, contain, and mitigate the impact of, such Data Incident, and remediate such Data Incident;

C.1.3. provide notice to Customer using the contact information identified in the most recent Order Form and security@lemonade.com without undue delay and in any event within twenty-four (24) hours after the
Spreedly confirms such Data Incident;

C.1.4. promptly, and in no event more than two (2) Business Days after the Spreedly provides notice of a Data Incident provide a written report to Customer providing all relevant details concerning such Data Incident;

C.1.5. collect and preserve all evidence concerning the discovery, cause, vulnerability, remedial actions and impact related to such Data Incident; and

C.1.6. document the incident response and remedial actions taken in detail.

C.2. Data Incident Notice. Spreedly hereby authorizes Customer, in Customer's sole and absolute discretion, to provide notice of, and reasonably required information and documents concerning, any Data Incident, to third parties, including without limitations individuals or entities that may have been impacted by the breach.

C.3. Security Contacts. The following individuals will be the primary contacts for purposes of any coordination, communications or notices with respect to this Schedule, or any Data Incident:

Spreedly Security Contact:

Name: Name: Jennifer Rosario

Telephone: Telephone: 888-727-7750

Email: Email: security@spreedly.com

Each party will promptly notify the other if any of the foregoing contact information changes.

D. Monitoring and Reporting.

D.1. Records; Maintenance. Spreedly will, consistent with PCI-DSS and its security obligations in this Schedule and the Agreement, collect and record information, and maintain logs, planning documents, audit trails, records and reports, concerning its security, its compliance with this Schedule, Laws, Data Incidents, its storage, processing and transmission of Customer Data and the accessing and use of Customer Data on the Platform.

D.2. Customer Assessments. Upon reasonable notice to Spreedly, once per year during the Term, Customer (or any vendor selected by Customer subject to the conditions in this Schedule), may at Customer’s sole cost, undertake an assessment and audit of security and Spreedly’s compliance with this Schedule. The scope of such assessments and audits will be as mutually agreed between Spreedly and Customer but will not include penetration testing or any assessment that may adversely affect Spreedly’s production environment.

D.3. Security Coordinator. Spreedly will assign a dedicated account manager that will act as the liaison between Customer and Spreedly to communicate compliance with this Schedule, coordinate Data Incident response and remedial action, and provide notice, reporting and other actions and duties as set forth in the Agreement. Spreedly will ensure that such individual is sufficiently trained, qualified and experienced to be able to fulfill these functions and any other related functions that might reasonably be expected to be carried out under this Schedule.

D.4. Information Requests.

D.4.1. Spreedly will cooperate with Customer in responding to any party, non-party, or government or public authority request or demand made to Customer for information related to the services under the Agreement (including metadata). In the event that such requests are served on Customer, Spreedly will provide Customer with access to such information in the format in which it is maintained in the ordinary course of business (or, on Customer's request, in any format necessary to satisfy such request).

D.4.2. In the event a request or demand by any party, non-party, or government or public authority (in the form of a subpoena, court order or otherwise) is provided to or served on Spreedly for information related to the services under the Agreement (including Customer Data and metadata), Spreedly will, to the extent it may legally do so, promptly notify Customer's security contact (as specified in subsection 3.3) in writing by electronic mail.

E. Cooperation and Coordination. Spreedly agrees to reasonably cooperate and coordinate with Customer concerning: (a) Customer's investigation, enforcement, monitoring, document preparation, notification requirements and reporting concerning Data Incidents and Spreedly's and Customer's compliance with Privacy Laws; and (b) any other activities or duties set forth under this Schedule for which cooperation between Customer and Spreedly may be reasonably required.

F. Survival. Spreedly's obligations and Customer's rights in this Schedule will continue as long as Spreedly, or a third party for or on Spreedly's behalf, controls, possesses, stores, transmits or processes Customer Data, including after expiration or termination of the Agreement.

G. Data Processing Agreement. At the request of the Customer, Spreedly will enter into a data processing agreement that incorporates the European Commission Standard Contractual Clauses between Controllers and Processors, in accordance with the Agreement (or any similar agreement with respect to non-European Union countries) with Customer and its Affiliates in order to allow Customer to be transferred to Spreedly and any Spreedly Affiliate.

Attachment 1: Specific Security Controls

Security Controls	
Information Security Governance	A comprehensive information security program including a policy written in one or more readily accessible parts that: (1) contains technical, physical, administrative and procedural controls to provide for the security, confidentiality, integrity and availability of Personal Information and supplier systems; (2) protect against hazards or threats and unauthorized access or use of Personal Information; (3) controls identified risks; (4) addresses access, retention and transport of Personal Information, and (5) acceptable use. Designate an individual to manage and coordinate its written security policy and who is sufficiently trained, qualified and experienced to be able to fulfill those functions and any other functions that might reasonably be expected to be carried out by the individual as a security manager or officer.
Asset Management	Mechanisms exist to inventory system components that: (1) Accurately reflects the current system; (2) Is at the level of granularity deemed necessary for tracking and reporting; and (3) Includes organization-defined information deemed necessary to achieve effective property accountability. All corporate laptops are full disk encrypted and wiped per industry standards when decommissioned. All infrastructure equipment housing Customer Data resides within certified third-party data centers within AWS. AWS currently uses the techniques detailed in NIST 800-88 (“Guidelines for Media Sanitization”) as part of the decommissioning process.
Business Continuity and Disaster Recovery	Plans and regular exercises to address business continuity of key people and processes along with disaster recovery plans for critical technology resiliency.
Change Management	Mechanisms exist to govern the technical configuration change control processes. Prior to implementing changes to the Platform Spreedly will assess the potential impact of such changes on Security and determine whether such changes are consistent with existing Security. No changes to the Platform or Security should be made which increase the risk of a Security Incident or which would cause a breach of the Schedule.
Cloud Security	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.
Compliance	Mechanisms exist to facilitate the identification and implementation of relevant legislative statutory, regulatory, and contractual controls.
Configuration Management	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.
Continuous logging and monitoring	Mechanisms exist to ensure that all systems used to store Customer Data are logged, monitored, and reviewed regularly.
Cryptographic Protections	Spreedly will encrypt all sensitive cardholder data using appropriate encryption technology wherever it is stored or transmitted. Spreedly will use only strong, public encryption algorithms and reputable cryptographic implementations and will not employ any proprietary cryptography.

Data Classification and Handling	Mechanisms exist to facilitate the implementation of data protection controls to ensure data and assets are categorized in accordance with applicable statutory, regulatory, and contractual requirements.
Endpoint Security	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices including but not limited to (1) utilization of anti-malware technologies to detect and eradicate malicious code; (2) automatic updates of anti-malware technologies, including signature definitions; (3) ensuring that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period; and (4) utilization of host-based firewall software, or a similar technology, on all information systems, where technically feasible.
HR Security	As permitted by applicable Law, conduct reasonable background checks of any Spreedly personnel that will have access to Customer Data, including Criminal Record Bureau checks. Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.
Identification and Authentication	Mechanisms exist to (1) provide physical access controls, secure user authentication protocols, secure access control methods, and firewall protection; and (2) prevent terminated Supplier Personnel from accessing Personal Information and supplier systems by promptly terminating their physical and electronic access to such Personal Information. With respect to supplier systems and Personal Information: (1) maintain secure control over user IDs, passwords and other authentication identifiers; (2) maintain a secure method for selecting and assigning passwords and using authentication technologies such as token devices; (3) Restrict access to only active users/accounts; (4) block user access after multiple unsuccessful attempts to login or otherwise gain access; (5) assign unique user identifications plus passwords, which are not vendor supplied default passwords; and (6) require personnel to change passwords at regular intervals and whenever there is any indication of possible system or password compromise, and avoid re-using or cycling old passwords. Duties and areas of responsibility of Supplier Personnel are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of supplier system or Personal Information.
Incident Response	Maintain policies and procedures for detecting, monitoring and responding to actual or reasonably suspected intrusions and Security Incidents, and encouraging reporting actual or reasonably suspected Security Incidents, including: (1) training Supplier's personnel with access to Customer Data to recognize actual or potential Security Incidents and to escalate and notify the senior management of the foregoing; (2) mandatory post-incident review of events and actions taken concerning security of Customer Data.
Malicious Code Mitigation Software	Mechanisms exist to (1) implement and maintain software for Spreedly systems that detects, protects against, removes and remedies software or computer code designed to perform an unauthorized function on, or permit unauthorized access to, an information system, including without limitation, computer viruses, Trojan horses, worms, and time or logic bombs; (2) run mitigation software on at least a weekly basis; (3) update mitigation software automatically, including without limitation, obtaining and implementing the most currently available virus signatures.
Network Security	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network including but not limited to (1) up-to-date firewalls between supplier system, the Internet (including internal networks connected to the Internet) and other public networks, and internal networks operated by Supplier that are not necessary for providing the Services to Customer, which are reasonably designed to maintain the security of Personal Information and supplier system; (2) implementation and management of a secure guest network.

Physical and Environmental Security	Mechanisms exist to provide (1) reasonable restrictions on physical access to Customer Data and the Platform; and (2) physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied. Policies concerning security for the storage, access, transportation and destruction of records and media containing Personal Information outside of business premises.
Privacy	Mechanisms exist to comply with applicable privacy laws, regulations, and notices.
Risk Management	Periodic and regular information security risk assessment and monitoring of Spreedly's information security program, Security and the Platform, at least annually, including: (1) identifying and assessing reasonably foreseeable internal and external threats and risks to the security, confidentiality, integrity and availability of Personal Information; (2) assessing the likelihood of, and potential damage that can be caused by, identified threats and risks; (3) regularly testing, monitoring and evaluating the sufficiency and effectiveness of Security and Data Incident response actions, and documenting same; (4) assessing adequacy of Spreedly personnel training concerning, and compliance with, Spreedly's information security program; (5) designing, implementing, adjusting and upgrading Security in order to limit identified threats and risks, and address material changes in technology, business and sensitivity of Customer Data; and (6) assessing whether such information security program is operating in a manner reasonably calculated to prevent unauthorized access or use of Customer Data; and (6) detecting, preventing and responding to attacks, intrusions and other system failures.
Secure Engineering and Architecture	Mechanisms exist to facilitate the implementation of industry-recognized security and privacy practices in the specification, design, development, implementation and modification of systems and services.
Security Awareness and Training	Regular and periodic training of Spreedly personnel concerning: (1) Security; (2) implementing Spreedly 's information security program; and (3) the importance of personal information security.
Technology Development and Acquisition	Spreedly will adhere to industry best practices and standards for Secure Software Development Lifecycle (SSDLC), including all of, but not limited to, the following techniques: (1) Leveraging security guidelines from one or all the following industry best practices and standards – OWASP Top 10, SANS Top 25 and Cloud Security Alliance; (2) Consistently executed secure code reviews and testing either through manual peer review or via a code scanning solution; (3) Protection of test data and content and removal of test data and content before deployment to production; (4) System acceptance testing; and (5) System change control and approvals before deployment to production.
Third Party Management	Mechanisms exist to facilitate the implementation of third-party management controls including but not limited to: (1) reasonable steps and due diligence to select and retain third party suppliers that are capable of maintaining security consistent with the Schedule and complying with applicable legal requirements; (2) contractually requiring such suppliers to maintain such security; and (3) regularly assessing and monitoring third party suppliers to confirm their compliance with the applicable security required in the Schedule and by law.
Threat Management	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.
Vulnerability and Patch Management	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information including but not limited to (1) software and firmware patching; (2) vulnerability scanning on a recurring basis; and (3) penetration testing conducted by an independent third party twice per year.

SCHEDULE C

SUPPORT OPTIONS

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

Every Spreedly 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. Customer has access to the Spreedly Help Center and Knowledge Base and to product Documentation; and can enroll for status notifications at the Spreedly API Status Page. Spreedly 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.

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

CONTACTING SUPPORT

Contact Spreedly's technical support by emailing support@spreedly.com or by submitting a request via our intake form at support.spreedly.com.

Please include the following information in all support requests:

- The organization name associated with the Spreedly 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 Spreedly 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

Spreedly'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

Spreedly 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
Spreedly is committed to rapid response of each request for support. All requests can be logged with Spreedly 24 hours-per-day, 7 days-per-week, 365 days-per-year via email at support@spreedly.com or via our request intake form at support.spreedly.com.

Spreedly will use commercially reasonable efforts to promptly respond to each support request. Spreedly 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 Spreedly. 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 Spreedly 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 Spreedly’s core API responsible for processing customer’s payment transaction requests and does not include any beta features or non-payment transaction Spreedly services such as dashboard reporting.

Table 1							
Severity	**Definition**	**Spreedly 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 Spreedly 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 Spreedly issue	Up to 2 hours	Up to 1 hours	Up to 30 minutes	Within 2 days	Within 2 days	Within 8 hours

Severity Level Definitions
Customer should indicate a priority when submitting a support ticket based on the severity level of their issue, however, Spreedly may adjust the priority if the request no longer fits the original severity level definition. Spreedly 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 Spreedly’s control and no work around exists.

Level 2 (Serious): Transaction Processing Service is severely impaired due to an issue under Spreedly’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 Spreedly.

Before submitting a support request, please first check the Spreedly **API Status Page** to see if the outage has already been reported or if your issue is due to scheduled maintenance.

Support Escalation
Spreedly'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 Spreedly 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 Customer, without interruption or undue delay. Any downtime resulting from outages of third-party connections or utilities or other reasons beyond Spreedly'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 Customer and continues until the Transaction Processing Service is restored.

Spreedly will give no less than 5 business days' prior written notice to Customer of all scheduled maintenance. Spreedly 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 Spreedly fails to meet or exceed the applicable service levels for Customer's given Subscription Support Services Plan, Spreedly will issue a credit to Customer in the following amounts based on the actual Availability during the applicable calendar month and the Customer'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 the Platform Fees
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 Baes 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 Customer's next applicable payment. The issuance of Service Credits is Spreedly's sole obligation and liability and Customer's sole remedy for any Service Level Failure.

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

CUSTOMER RESPONSIBILITIES

Internal Help Desk

Customer 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 Spreedly, please contact Spreedly for technical support by email at support@spreedly.com or via our request intake form at support.spreedly.com

TECHNICAL LEADS

Customer will establish a technical lead to manage troubleshooting and establish best practices. Your technical leader will be the liaison between Customer and Spreedly for technical support. These persons must have sufficient knowledge of the Spreedly product and your own environment in order to work with Spreedly to analyze and resolve Support Requests. They are responsible for engaging Spreedly 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 Spreedly 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 Spreedly’s online resources (e.g. website product Documentation, technical Documentation and Knowledge Base) and the Spreedly Status Page before submitting a Support Request.

PROTECTION OF API KEYS AND CREDENTIALS

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

PRODUCT AND SUPPORT UPDATES

Updates to Spreedly Services

Spreedly may release Updates to its products and services pursuant to Spreedly's standard release cycle. Spreedly will provide Updates at no additional charge. Spreedly may make changes to its products and services (including, without limitation, the design, look and feel, functionality, content, material, information) that Spreedly deems necessary or useful to improve the products or services or for any other reason and at any time, provided however Spreedly 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, Spreedly will schedule such Updates during non-business hours. Notice to Customer will be sent via email or posted at the Spreedly API Status Page.

Updates to these Support Policies

Customer understands that these Support Services terms are subject to change at Spreedly’s reasonable discretion upon posting to Spreedly’s website at www.spreedly.com/support-services-terms and advance notice to Customer; provided that Spreedly will not materially degrade the performance of the Platform or Support Services provided to Customer during the Term.

SCHEDULE D

DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "DPA") forms part of the Enterprise Service Agreement (the "Agreement") between Lemonade, Inc. (the "Controller") and Spreedly, Inc., a Delaware corporation ("Processor"). This DPA applies where, and to the extent that, Processor processes personal data of data subjects on behalf of the Controller when providing the Platform, Support Services and/or Professional Services (collectively for the purposes of this DPA, the "Services") under the Agreement. This DPA may be supplemented with additional jurisdiction-specific clauses as described in Section 14(f) below. All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement.

In consideration of the mutual obligations set forth herein, the parties agree to the terms and conditions of this DPA, effective as of the effective date of the Agreement.

1. **Defined Terms**. For the purposes of this DPA only, the following terms have the meanings given to such terms below:

(a) "Controller Personal Data" means any personal data processed by Processor on behalf of the Controller pursuant to the Agreement. For the avoidance of doubt, all Customer Data that constitutes personal data is Controller Personal Data.

(b) "EEA" means the European Economic Area.

(c) "Data Privacy Laws" means applicable laws relating to the privacy and protection of personal data, including without limitation (but only where applicable) GDPR and U.S. state laws (only where applicable).

(d) "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, including the recitals. Where personal data of data subjects in the United Kingdom is involved, "GDPR" more specifically means and refers to Regulation (EU) 2016/679, the General Data Protection Regulation together with and as implemented by the UK Data Protection Act of 2018 and the implementing rules or regulations that are issued by the UK Information Commissioner's Office ("ICO").

(e) "personal data" means and includes "personal information" and "personal data" as defined under Data Privacy Laws.

(f) "Restricted Transfer" means a transfer of Controller Personal Data from the Controller to Processor or any onward transfer of Controller Personal Data from Processor to a Subprocessor, in each case where such transfer would be prohibited by Data Privacy Laws in the absence of the parties' agreement to the Standard Contractual Clauses or another data transfer mechanism permitted by Data Privacy laws.

(g) "Standard Contractual Clauses" means, collectively, (i) where personal data of data subjects in the EEA is involved, the standard contractual clauses set out in Commission Implementing Decision (EU)2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to GDPR (referred to herein more particularly as the "EU SCCs"), and (ii) where personal data of data subjects in the United Kingdom is involved, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018 (referred to herein more particularly as the "UK SCCs").

(h) "Subprocessor" means any person or entity (excluding employees of Processor) appointed by or on behalf of Processor to Process Controller Personal Data on behalf of the Controller in connection with the Agreement.

(i) Additionally, the terms "controller," "data subject," "personal data," "personal data breach," "process," "processor," and "supervisory authorities" (or their respective substantially corresponding equivalents under Data Privacy Laws) will have the meanings given to such terms under Data Privacy Laws.

2. **Nature of Relationship**. The parties acknowledge and agree that the Controller is a controller and Processor is a processor under Data Privacy Laws.

3. **Controller Representations and Warranties**. The Controller represents and warrants to Processor that, prior to transferring any Controller Personal Data to Processor for processing, asking Processor to collect Controller Personal Data on the Controller's behalf in connection with the Services, or otherwise providing or making available any personal data to Processor in connection with Processor's performance of the Services, the Controller has provided

to the applicable data subjects every type of notice and obtained from the applicable data subjects every type of consent in each case as required by Data Privacy Laws pertaining to such disclosures of personal data to or collection of personal data on the Controller's behalf by Processor. The Controller will indemnify and hold harmless Processor from and against all claims, liabilities, fines, penalties, costs or other expenses, of any kind or nature whatsoever, arising out of the Controller's breach of this Section 3.

4. **Description of Processing**.

(a) Data Subjects: Personnel and customers of the Controller.

(b) Categories of Data: With respect to personnel of the Controller, 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 the Controller, name, address, e-mail, telephone number, location, and billing and payment details such as bank account and credit or debit card numbers.

(c) Special Categories of Data: None.

(d) Nature and Purpose of Processing: All processing operations required to facilitate provision of Services to the Controller in accordance with the Agreement.

(e) Frequency of Transfer (per Section 12 of this DPA): Continuously throughout the term of the Agreement.

(f) Period of Retention of Personal Data: Except as otherwise provided in the Agreement or this DPA, in accordance with the retention policy of the Processor, provided that to the extent that any personal data is retained beyond the termination of the Agreement for back up or legal reasons, the Processor will continue to protect such personal data in accordance with the Agreement and this DPA.

(g) For transfers to Subprocessors, the subject matter, nature and duration of the Processing: As described in Section 10 of this DPA.

(h) Duration: as necessary, during the term of the Agreement

5. **Processing of Personal Data.** Processor will process Controller Personal Data only as needed to perform the Services and otherwise only on documented instructions from Controller (including, for the avoidance of doubt, as described in the Agreement), unless Processor is required to do so by applicable law to which Processor is subject, in which case Processor will inform the Controller of that legal requirement before processing (unless the applicable law prohibits providing such information to the Controller on important grounds of public interest). The Controller will ensure that its instructions comply with all laws, rules and regulations applicable in relation to the Controller Personal Data, and that the processing of Controller Personal Data in accordance with the Controller's instructions will not cause Processor to be in breach of Data Privacy Laws or any other laws, rules or regulations applicable with respect to the Controller Personal Data. Processor represents that it has implemented appropriate technical and organizational measures in such a manner that its processing of Controller Personal Data will meet the requirements of Data Privacy Laws and ensure the protection of the rights of the data subjects.

6. **Confidentiality of Personal Data**. Processor will ensure that all persons (including Subprocessors) authorized to process Controller Personal Data have committed to keeping such Controller Personal Data confidential or are under an appropriate statutory obligation of confidentiality with respect to such Controller Personal Data. Processor will take steps to ensure that any natural person acting under the authority of the Processor who has access to Controller Personal Data does not process such Controller Personal Data except as needed to perform the Services or otherwise upon instructions from the Controller, unless the Processor is required to do so by applicable law to which Processor is subject. Processor may not disclose, share or sell Controller Personal Data (other than as strictly necessary to perform its obligations pursuant hereto or in the Agreement), and it may not combine Controller Personal Data obtained pursuant to the Agreement with any other information regarding such person(s).

7. **Security of Personal Data**. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, Processor will implement appropriate technical and organizational measures to ensure a level of security for Controller Personal Data appropriate to the risk, including in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Controller Personal Data transmitted, stored or otherwise processed. Such measures will include, *inter alia* as appropriate: (a) the pseudonymization or encryption of Controller Personal Data, (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services used to process Controller Personal Data, (c) the ability to restore the availability and access to Controller 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. Additionally, such measures will include those set forth in the Processor's Data Security Policy attached as Schedule B to the Agreement.

8. **Assistance and Cooperation**.

(a) Processor will provide, at the Controller's cost, reasonable assistance to Controller in performing any data protection impact assessments and/or relevant consultations with supervisory authorities or other competent data privacy authorities, in each case to the extent required by Data Privacy Laws (such as, where applicable, GDPR Articles 35 or 36), and in each case solely in relation to Processing of Controller Personal Data by, and taking into account the nature of the Processing and information available to, Processor and its Subprocessors.

(b) Taking into account the nature of the Processing and the information available to Processor, Processor will, at the Controller's cost, assist Controller as Controller may reasonably require, including by appropriate technical and organizational measures, insofar as this is possible, in ensuring compliance with the Controller's obligations under Data Privacy Laws to appropriately secure and safeguard Controller Personal Data (such as, where applicable, pursuant to GDPR Article 32).

(c) Taking into account the nature of the Processing, Processor will, at the Controller's cost, assist Controller as Controller may reasonably require, including by appropriate technical and organizational measures, insofar as this is possible, to enable the Controller to comply with requests by data subjects to exercise their rights under Data Privacy Laws. Processor will: (i) promptly notify the Controller if Processor receives a request from a data subject under Data Privacy Laws with respect to Controller Personal Data, and (ii) not respond to that request except on the written instructions of the Controller or as required by applicable law to which Processor is subject, in which case Processor will (to the extent permitted by applicable law) inform Controller of that legal requirement before Processor responds to the request.

9. **Recordkeeping; Information and Audit Rights**. Processor will maintain all records pertinent to its processing of Controller Personal Data that are required by Data Privacy Laws, such as, where applicable, Article 30(2) of the GDPR, and (to the extent they are applicable to Processor's activities for the Controller) Processor will make such records available to the Controller upon the Controller's reasonable written request. Processor will make available to the Controller on the Controller's reasonable request all information necessary to demonstrate compliance with this DPA, and will, at the Controller's cost, allow for and cooperate with audits, including inspections, by the Controller or an auditor appointed by Controller in relation to the Processing of the Controller Personal Data by Processor, subject to the following:

(a) Information disclosed to the Controller or its auditor or that is otherwise revealed in such records, inspections or audits will be the Confidential Information of Processor under the confidentiality provisions of the Agreement.

(b) The Controller may request an audit by emailing success@spreedly.com.

(c) Audits may not be conducted more than once per year or more frequently: (i) to the extent required by a supervisory authority, or (ii) in the event of and in connection with a particular personal data breach.

(d) Audits will be conducted only during Processor's normal business hours and only with reasonable advance written notice of not less than 15 business days (except in the event of a personal data breach or if the Controller has a reasonable basis to believe (supported by substantial evidence) that Processor is in material non-compliance with this DPA, in which case advance notice will be not less than 72 hours).

(e) Following the Processor's receipt of the Controller' written request to conduct an audit and/or inspection, the Processor and Controller will discuss and agree in advance on the reasonable scope, start date and duration of this audit, as well as any applicable security and confidentiality controls that may be required.

(f) No such audit will include access to Processor's (or any Subprocessors') facilities or systems (e.g., computing infrastructure, servers, data storage mechanisms and infrastructure, audit logs, activity reports, system configuration, etc.) without Processor's prior written consent, except to the extent required by a supervisory authority.

(g) The Processor may charge a fee (based on the Processor's reasonable costs) for any such audit. The Processor will provide the Controller with additional details of this fee including the basis of its calculation, in advance of the audit. Additionally, the Controller will be responsible for any fees charged by any third-party auditor appointed by the Controller for this audit.

In lieu of an audit, upon reasonable request by the Controller, but no more than once per year, Processor agrees to complete, within thirty (30) days of receipt, an audit questionnaire provided by the Controller regarding Processor's compliance with this DPA, of reasonable length and required detail (not to exceed a reasonably-estimated three person-hours to complete unless otherwise agreed to and subject to the payment of additional fees set forth in a separate written agreement by the parties), provided that any such questionnaire responses will be the Processor's Confidential Information under the confidentiality provisions of the Agreement.

10. **Subprocessors**.

(a) Processor will not engage any Subprocessor to process Controller Personal Data under the Agreement without written authorization from the Controller. Processor reserves the right to maintain its Subprocessor list through means such as publication of its Subprocessor list online, and the Controller hereby provides written authorization for Processor to engage the Subprocessors listed online at https://www.spreedly.com/gdpr-subprocessors. Controller may receive notifications of new Subprocessors by emailing subprocessor@spreedly.com with the subject "Subscribe," and once subscribed in this manner Controller will receive notification of new Subprocessors before those Subprocessors are authorized to process Controller Personal Data on behalf of the Processor. Processor will send notice to Controller by email of any additional or replacement Subprocessors at least 10 days in advance of engaging any such additional or replacement Subprocessors to process Controller Personal Data under the Agreement. Controller may object to any such additional or replacement Subprocessor within 10 days of receiving such notice, provided that such objections are reasonable and on grounds relating to the protection or privacy of the Controller Personal Data involved in accordance with Data Privacy Laws or this DPA. Processor will use commercially reasonable efforts to resolve any such objection by the Controller, and the Controller will reasonably and in good faith cooperate with Processor in such efforts. If Processor cannot resolve the Controller's objection within a reasonable period of time following receipt of Controller's objection (such period of time not to exceed 60 days), and if Processor is unable to provide some or all of the Services without the use of the objected-to Subprocessor, then the Controller may terminate the applicable Services which cannot be provided by Processor without the use of the objected-to Subprocessor by providing written notice to Processor.

(b) Where Processor engages a Subprocessor for carrying out specific processing activities on behalf of the Controller with respect to Controller Personal Data, Processor will by contract impose on the Subprocessor substantially the same data protection obligations as set forth in this DPA. Where the Subprocessor fails to fulfil such data protection obligations, Processor will remain fully liable to the Controller for the performance of that Subprocessor's obligations.

(c) The Controller understands, acknowledges and agrees that the Processor is (and its Subprocessors may be) based in the United States and that the Processor provides (and the Subprocessors may provide) services under the Agreement from the United States, and the Controller hereby consents to the transfer of Controller Personal Data to the United States for Processing by the Processor and its Subprocessors in accordance with Section 12 below.

(d) Controller and Processor acknowledge that the Controller 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. Any such third parties engaged by the Controller will not be deemed a Subprocessor of the Processor for purposes of this DPA. Accordingly, nothing in this DPA obligates the Processor to enter into a data protection agreement with any such third party or to be responsible or liable for such third party's acts or omissions.

(e) Processor remains fully liable to the Controller with respect to its Subprocessors.

11. **Return or Deletion of Controller Personal Data**.

(a) Subject to Sections 11(b), 11(c) and 11(d) below, Processor will at Controller's request within thirty (30) days after the date of cessation of Services involving the Processing of Controller Personal Data, either; (i) return to the Controller the Controller Personal Data in a mutually-agreeable format; or (ii) delete and ensure the deletion of all copies of Controller Personal Data.

(b) Processor (and Processor's Subprocessors) may retain Controller Personal Data to the extent and for such period as is required by applicable law, rule or regulation, provided that Processor will ensure the continued confidentiality of all such Controller Personal Data, and will ensure that the Controller Personal Data are only accessed and used for the purpose(s) specified in the applicable law, rule or regulation requiring its retention. Additionally, solely to the extent not prohibited by Data Privacy Laws, Processor (and Processor's Subprocessors) may retain Controller Personal Data stored in electronic archived or backup systems until such copies are deleted in the ordinary course in accordance with Processor's data retention policies, provided that any such retained Controller Personal Data will remain protected to the standards of this DPA for so long as it is retained.

(c) Processor may retain and use for its business purposes any aggregated or de-identified data (i.e., data that is no longer personal data) created from or using Controller Personal Data, during and after termination of the Agreement, but only pursuant to and in accordance with Data Privacy Laws.

(d) The Processor's obligations under this Section 11 will be subject to any agreed-upon post-termination data retrieval provisions in the Agreement.

12. **Restricted Transfers**. Subject to the remainder of this Section 12, the Controller (as "Data Exporter") and Processor (as "Data Importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from Controller to Processor. Processor will ensure that before it commences any Restricted Transfer to a Subprocessor, the Subprocessor will enter into the Standard Contractual Clauses (or variations of those Standard Contractual Clauses made under Section 14(e) or as otherwise proposed by the Subprocessor or Processor as long as such variations are compliant with Data Privacy Laws).

(a) With respect to the EU SCCs, the same are incorporated by reference into this DPA on an unchanged basis save for the following:

(i) Only "Module 2" of the EU SCCs applies;

(ii) For the purposes of clause 9(a) of the EU SCCs, option 2 ("General Prior Authorisation") is selected and the specified time period is 10 days in advance;

(iii) For the purposes of clause 11(a) of the E.U. Standard Contractual Clauses, the optional language is deleted;

(iv) For the purposes of clause 13 of the EU SCCs: (i) if Controller is established in an EU Member State, the relevant supervisory authority acting as the competent supervisory authority is the supervisory authority of the EU Member State in which Controller is established, (ii) if Controller is not established in an EU Member State but has appointed a representative pursuant to GDPR Article 27(1), the relevant supervisory authority acting as the competent supervisory authority is the supervisory authority of the EU Member State in which Controller's representative is established, and (iii) if Controller is not established in an EU Member State and has not appointed a representative pursuant to GDPR Article 27(1), then the supervisory authority of one of the EU Member States in which the data subjects whose Controller Personal Data is transferred under the EU SCCs in relation to the offering of goods or services to them are located will act as competent supervisory authority. This paragraph will constitute "Annex I.C" for purposes of the EU SCCs;

(v) For the purposes of clause 14(a) of the EU SCCs, the Assessment attached hereto as Appendix 1 is incorporated herein by reference.

(vi) For the purposes of clause 17 of the EU SCCs, the governing law is the Netherlands;

(vii) For purposes of clause 18(b) of the EU SCCs, the selection is the Netherlands; and

(viii) The relevant party identification information from the Agreement and the description of processing in Section 4 of this DPA together will constitute "Annex 1" for the purposes of the EU SCCs. Sections 6 and 7 of this DPA will constitute "Annex 2" for the purposes of the EU SCCs.

(b) With respect to the UK SCCs, the same are incorporated by reference into this DPA on an unchanged basis save for the following:

(i) In Table 2, the selections made are those that match the EU SCCs as described and detailed in clause (a) of this Section 12;

(ii) In Table 4, both "importer" and "exporter" are selected; and

(iii) The relevant party identification information from the Agreement, the description of processing in Section 4 of this DPA, and Sections 6 and 7 of this DPA will be incorporated into (and will constitute) Tables 1 and 3 of the UK SCCs, as applicable.

13. **Personal Data Breach**. Taking into account the nature of processing and the information available to the Processor, Processor will reasonably assist the Controller in the Controller's efforts to comply with its obligations regarding personal data breaches as set forth in Data Privacy Laws, such as, where applicable, GDPR Articles 33 and 34. If any Controller Personal Data is subject to any personal data breach Processor will, upon becoming aware of the personal data breach, without undue delay notify the Controller, take reasonable steps to contain and counteract the personal data breach and minimize any damage resulting from the personal data breach, and provide Controller with sufficient information to allow the Controller to meet any obligations to report to supervising authorities or inform the applicable data subjects of the personal data breach to the extent required under Data Privacy Laws. Processor will cooperate, at the Controller's cost, to assist Controller in the investigation, mitigation and remediation of each such personal data breach.

14. **Miscellaneous**.

(a) Subject to the following sentence of this Section 14(a), in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA will prevail. In any event, Processor's liability under this DPA, including for breach or other failure under this DPA by Processor or its Subprocessors, will be (to the maximum extent permitted under Data Privacy Laws, the Standard Contractual Clauses and other applicable law) subject to the exclusion and limitation of liability provided for I the Agreement as if this DPA were a part of the Agreement, *ab initio*..

(b) To the extent this DPA is not governed exclusively by Data Privacy Laws, it will be governed by and construed in accordance with the laws selected pursuant to the governing law provision set forth in the Agreement.

(c) This DPA constitutes the entire understanding of the parties with respect to the subject matter hereof and supersedes all prior agreements, oral or written.

(d) Except as expressly stated in Data Privacy Laws or the Standard Contractual Clauses attached hereto, the parties to this DPA do not intend to create any rights in any third parties.

(e) The parties agree that, to the extent required under Data Privacy Laws, such as due to legislative changes, court decisions, and/or to reflect measures or guidance from supervisory authorities, including, without limitation and only where applicable, the adoption of standards for contracts with processors according to GDPR Article 28(7) or (8) or the invalidation, amendment, replacement or repeal of a decision adopted by the EU Commission or ICO in relation to international data transfers on the basis of GDPR Article 45(3) or Article 46(2) GDPR or on the basis of Article 25(6) or 26(4) of EU Directive 95/46/EC, such as, in particular, with respect to the Standard Contractual Clauses or similar transfer mechanisms, the Controller may request reasonable changes or additions to this DPA to reflect applicable requirements. If the Controller makes a request to change or supplement this DPA pursuant to this Section 14(e), the Controller and Processor will in good faith negotiate such changes and additions (including, where applicable, providing for Controller's reimbursement of Processor's costs and expenses for undertaking additional obligations) and the Processor will not unreasonably withhold or delay agreement to any variations to this DPA.

(f) Controller and Processor hereby accept and agree to, and where and as applicable will adhere to, the clauses that appear in the following attachments:

- Attachment 1 – Compliance with the Federal Act on Data Protection of the Swiss Confederation (FADP)
- Attachment 2 – Compliance with U.S. State Consumer Privacy Laws
- Attachment 3 – Compliance with the Brazilian Data Protection Law (LGPD)
- Attachment 4 – Compliance with Argentina's Pending Data Protection Law

(g) Based on the Customer Data that Controller will process using the Platform or otherwise provide to Processor, if and to the extent Data Privacy Laws require additional clauses to be executed by Processor beyond those set forth in this DPA, then Controller will notify Processor in writing of such requirement and Processor will in good faith review, negotiate and consider adding such clauses as an additional addendum to the Agreement. In the absence of such notice Controller represents and warrants that no additional clauses are required.

Attachment 1

Compliance with the Federal Act on Data Protection of the Swiss Confederation as Revised Effective September 1, 2023 ("FADP")

1. This Attachment 1 applies only to any processing of personal data that has actual or potential effects in the Swiss Confederation.

2. All provisions of the above DPA are incorporated and restated in this Attachment 1 in their entirety, except as specifically amended or modified below.

3. References to Data Privacy Laws in the DPA will mean and include (but only where applicable) FADP.

4. Section 12(a) of the DPA is supplemented and amended as follows, as and to the extent required by the FADP:

   (a) All references to the GDPR in Section 12(a) and in the EU SCCs are to be understood as references to the FADP, which governs all data transfers from the Swiss Confederation, and which permits the use of the EU SCCs. This provision will constitute the Annex required by the Federal Data Protection and Information Commissioner ("FDPIC") in its guidance issued August 27, 2021.

   (b) The term "Member State" must not be interpreted in such a way as to exclude data subjects in the Swiss Confederation from the possibility of suing for their rights in their place of habitual residence, in accordance with Clause 18(c) of the EU SCCs. This provision will constitute the Annex required by the FDPIC in its guidance issued August 27, 2021.

   (c) Section 12(a)(iv) is amended to state: "For the purposes of clause 13 of the EU SCCs, the FDPIC of the Swiss Confederation is the competent supervisory authority. This paragraph will constitute 'Annex I.C' for purposes of the EU SCCs."

   (d) In Sections 12(a)(vi) and 12(a)(vii), "Ireland" is replaced by "Swiss Confederation."

5. Section 12(b) of the DPA is deleted.

Attachment 2

Compliance with U.S. State Consumer Privacy Law

This Attachment 2 applies where, and to the extent that, Processor processes personal information of consumers within one or more U.S. States that have enacted consumer privacy laws applicable to the Services.

Notwithstanding anything to the contrary elsewhere in the DPA, where the California Consumer Privacy Act of 2018 and its implementing regulations, as amended effective January 1, 2023 by the California Privacy Rights Act and its implementing regulations (the two laws collectively, as amended, restated or supplemented from time-to-time, the "CCPA/CPRA") applies, the terms "business," "combine," "commercial purpose," "consumer," "contractor," "personal information," "processing," "sell," "share," and "service provider" will have the meanings given to such terms in CCPA/CPRA; and where any of the state privacy laws listed below and their respective implementing regulations (each, an "Other State Law," and, collectively, the "Other State Laws") apply, the terms "consumer," "controller," "processing," "processor," "sell" (and its corresponding "sale") and "targeted advertising" will have the meanings given to such terms in the applicable Other State Law, and the term "personal information" will have the same meaning as the term "personal data" as such term is defined in the applicable Other State Law. The Other State Laws are:

- The Virginia Consumer Data Protection Act, effective January 1, 2023 (as amended, restated or supplemented from time-to-time, the "VCDPA");
- The Colorado Privacy Act, effective July 1, 2023 (as amended, restated or supplemented from time-to-time, the "CPA");
- The Connecticut Personal Data Privacy and Online Monitoring Act, effective July 1, 2023 (as amended, restated or supplemented from time-to-time, the "CPDPOMA"); and
- The Utah Consumer Privacy Act, effective December 31, 2023 (as amended, restated or supplemented from time-to-time, the "UCPA").

In consideration of the mutual obligations set forth herein, the parties agree to the terms and conditions of this Addendum.

1. The parties acknowledge and agree that the Controller is a business and Processor is a service provider or contractor to the Controller under the CCPA/CPRA, and Controller is a controller and Processor is a processor under the Other State Laws. Controller represents, warrants and covenants that it has complied and it will comply with the CCPA with respect to all personal information of consumers that Controller has transferred or made available to Processor and its Subprocessors, or that Controller has asked Processor or its Subprocessors to collect on Controller's behalf for processing in connection with the Services. The Controller will indemnify and hold harmless Processor from and against all claims, liabilities, fines, penalties, costs or other expenses, of any kind or nature whatsoever, arising out of the Controller's breach of this Section 1.

2. In its processing of personal information of consumers that the Controller has transferred to Processor for processing, that Processor may have access to, or that Processor has collected on the Controller's behalf, in each case in connection with the Services, Processor will comply with all requirements of the CCPA/CPRA that are applicable to service providers and contractors and all requirements of the applicable Other State Laws that are applicable to processors. Without limiting the foregoing, during the term of the Agreement and thereafter, Processor will: (i) not retain, use or disclose the personal information for any purpose (including any commercial purpose) other than for the specific purpose of performing the Services contemplated by the Agreement; (ii) not retain, use or disclose the personal information outside of the direct business relationship between Processor and the Controller; (iii) not sell or (where CCPA/CPRA applies) share the personal information to any third parties; and (iv) not combine the personal information that Processor receives from, or on behalf of, Controller with personal information that Processor receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that Processor may combine such personal information (1) for the specific purpose of providing the Services contemplated by the Agreement or (2) to perform any other permitted business purpose under CCPA/CPRA and/or the Other State Laws, as applicable. Processor certifies that it understands and will comply with the restrictions, duties and obligations set forth in this Section 2.

3. Where not prohibited by applicable law, nothing in this Addendum will prohibit Processor from retaining, using or disclosing the personal information in connection with: (i) retaining or employing another service provider, contractor or subcontractor (as applicable), provided the service provider, contractor or subcontractor meets the requirements for a service provider, contractor or subcontractor under the CCPA/CPRA or Other State Law, as applicable; (ii) internal use by Processor to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles for use in providing services to another business, or correcting or augmenting data acquired from another source; (iii) detecting data security incidents, or protecting against fraudulent or illegal activity; (iv) complying with federal, state or local laws; (v) complying with a civil, criminal or regulatory inquiry, investigation, subpoena, or summons by federal, state or local authorities; (vi) cooperating with law enforcement agencies concerning conduct or activity that the Controller, Processor or a third party reasonably and in good faith believes may violate federal, state or local law; or (vii) exercising or defending legal claims.

4. If Processor authorizes any Subprocessor to process, retain or use any personal information received from the Controller, accessed in connection with the Services or collected on the Controller's behalf in connection with the Services, then prior to any disclosure of such personal information to such Subprocessor, Processor will enter into a written agreement with such Subprocessor that includes all required or necessary terms to ensure that such Subprocessor is deemed a service provider or contractor within the meaning of the CCPA/CPRA or a subcontractor within the meaning of any applicable State Law.

5. To the extent this Addendum is not governed exclusively by CCPA/CPRA or an Other State Law (as applicable), it will be governed by and construed in accordance with the laws set forth in the governing law section of the Agreement. If there is any conflict between this Addendum and the DPA, the Agreement or any other data protection agreement(s) between the parties, this Addendum will prevail to the extent of that conflict with respect to the personal information of consumers only.

Attachment 3

Compliance with the Brazilian Data Protection Law ("LGPD"), Retroactively Effective as of September 2020

1. This Attachment 3 applies only to processing of personal data that is carried out in Brazil, that has the purpose of offering goods or services to people in Brazil, or is done on data that was collected in Brazil.

2. Controller and Processor acknowledge that, while the text of the LGPD is available, the full details of the interpretation and enforcement of the LGDP are still being developed. In particular, regulations to be promulgated by the Brazil National Data Protection Authority (ANDP) are not final as of the date of execution of this Brazil Addendum. Controller and Processor therefore agree to attempt in good faith to comply with the LGPD in its current state and amend their respective practices and this Brazil Addendum (in accordance with the procedures set forth in Section 14(e) of the DPA) if and when required by legal developments in Brazil. Because the majority of legal obligations under the LGPD devolve upon data controllers, Controller agrees to monitor LGPD and ANDP developments and to instruct Processor whenever such developments require changes in Processor's practices or any Controller-Processor agreements.

3. Because most legal duties and obligations under the LGPD closely track those under the GDPR, all provisions of the above DPA are incorporated and restated in this Brazil Addendum in their entirety, except as specifically amended or modified below. Without limiting the generality of this Section 3, Controller further agrees to comply with current provisions of the LGPD that may impose duties that exceed those imposed by the GDPR, including without limitation those concerning the definition of personal data and the right of data subjects to anonymization of their personal data.

4. References to Data Privacy Laws in the DPA will mean and include (but only where applicable) LGPD.

5. Controller and Processor acknowledge that the LGPD permits data transfers out of Brazil pursuant to Standard Contractual Clauses, but Brazil has not yet promulgated its own Standard Contractual Clause. Therefore, Controller and Processor will use the EU SCCs as specified in the DPA for such transfers, subject to the amendments and modifications stated below, until such time as Brazil promulgates Standard Contractual Clauses.

6. Section 12 of the DPA is supplemented and amended as follows:

   (a) Section 12(a)(iv) is amended to state: "For the purposes of clause 13 of the EU SCCs, the ANDP is the competent supervisory authority. This paragraph will constitute 'Annex I.C' for purposes of the EU SCCs."

   (b) In Sections 12(a)(vi) and 12(a)(vii), "Ireland" is replaced by "Brazil."

   (c) Section 12(b) of the DPA is deleted.

Attachment 4

Compliance with Argentina's Pending Data Protection Law

1. This Attachment 4 applies only to processing of personal data of data subjects who are in Argentina that is related to the offering of goods or services to such subjects or the monitoring of their behavior within Argentina.

2. Controller and Processor acknowledge that, as of the date of execution of this DPA, the protection of personal data in Argentina is governed by Personal Data Protection Law No. 25,326 (2000) as complemented by Regulatory Decree No. 1558/2001 and several resolutions, rules and guidelines. Controller and Processor further acknowledge that a new Data Protection Law has been introduced and is in the process of public consultation and legislative enactment (the current draft has been released as DPA Resolution 119/2022 of Sep. 12, 2022) ("ARG Pending Law")), and that its enactment is expected in 2023. Because the majority of the legal obligations under the ARG Pending Law are expected to devolve upon data controllers, Controller agrees to monitor Argentina privacy law developments and to instruct Processor whenever such developments require changes in Processor's practices or any Controller-Processor agreements.

3. Because most legal duties and obligations under the ARG Pending Law are expected to closely track those under the GDPR, all provisions of the above DPA are incorporated and restated in this ARG Addendum in their entirety, except as specifically amended or modified below. Without limiting the generality of this Section 3, Controller further agrees to comply with any provisions of the current Personal Data Protection Law No. 25,326 (2000), as complemented, that may impose duties that exceed those imposed by the GDPR.

4. References to Data Privacy Laws in the DPA will mean and include (but only where applicable) the current Personal Data Protection Law No. 25,326 (2000), as complemented, and (when in force) the ARG Pending Law.

5. Controller and Processor acknowledge that the ARG Pending Law is expected to permit data transfers out of Argentina pursuant to Standard Contractual Clauses, but the specific form of such Clauses is not yet known. Therefore, Controller and Processor will use the EU SCCs as specified in the DPA for such transfers, subject to the amendments and modifications stated below, until such time as Argentina promulgates Standard Contractual Clauses.

6. Section 12 of the DPA is supplemented and amended as follows:

   (a) Section 12(a)(iv) is amended to state: "For the purposes of clause 13 of the EU SCCs, the Argentina Agency of Access to Public Information, or any successor thereto, is the competent supervisory authority. This paragraph will constitute 'Annex I.C' for purposes of the EU SCCs."

   (b) In Sections 12(a)(vi) and 12(a)(vii), "Ireland" is replaced by "Argentina."

   (c) Section 12(b) of the DPA is deleted.

Appendix 1

CLAUSE 14(a) WARRANTY ASSESSMENT
Under Standard Contractual Clauses

Spreedly, Inc. (the "processor" or "data importer") and Lemonade, Inc. (the "controller" or "data exporter") together provide the following assessment pursuant to Clause 14(d) of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as adopted by the European Commission on June 4, 2021 (the "EU SCCs"). The data importer and data exporter are each a "Party" and collectively the "Parties." Defined terms used but not otherwise defined in this assessment have the meanings given to such terms in the EU SCCs.

Background

Clause 14(a) of the EU SCCs requires that the Parties "warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses." Clauses 14(b)-(d) require that, in providing this warranty, the Parties conduct and document an assessment of the transfer in the context of the "laws and practices" of the destination country. As part of this process, "[t]he data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information." This assessment is intended to be the documentation of the Parties' compliance with their obligations under Clause 14(d) and the data importer's obligation to provide relevant information under Clause 14(b).

Summary description of data importer's processing activities

The data importer hosts a web-based payments orchestration and tokenization platform which enables the controller or 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 data importer platform, and, where applicable, to automatically update expired or lost credit cards.

Assessment

The data importer is based in the United States ("U.S.") and it and its subprocessors offer services (and process personal data) in the U.S. Therefore, personal data to be processed by the data importer and its subprocessors under the Parties' agreement will be transferred to the U.S. for processing. Data importer has received legal advice on the authority of public authorities in the U.S. to access or compel disclosure of the personal data to be transferred pursuant to the Parties' agreement, with particular attention to Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 (EO 1233), as limited by President Obama's Presidential Policy Directive 28 (PPD 28). Such advice has also dealt with the practices of U.S. public authorities, to the limited extent that they are knowable. Data importer has also taken due account of the specific circumstances of the transfer, and the applicable limitations and safeguards, including technical or organizational safeguards. Of particular relevance is the fact that the personal data to be transferred consists primarily of either (1) payment card and related payment information without context into any particular transaction, or (2) basic personal data of the data exporter's personnel accessing and using data importer's software platform and services, such as the names and business contact information of such personnel.

Based on this assessment, data importer acknowledges that U.S. laws, particularly FISA, do permit U.S. public authorities to access or compel access to personal data entering the U.S., including the personal data to be transferred pursuant to the Parties' agreement. However, given the specific circumstances of the transfer and the categories and format of the transferred personal data as described above, after due consideration the data importer cannot reasonably foresee circumstances where U.S. public authorities would be likely to take interest in the personal data to be transferred pursuant to the Parties' agreement and therefore the data importer has no reason to believe such authorities are likely to exercise their authority under FISA or other similar U.S. laws to access or compel access to such personal data.