ENTERPRISE SERVICE AGREEMENT

This Enterprise Services Agreement ("Agreement") is entered by and between Spreedly, Inc., a Delaware corporation, ("Spreedly") and Factor Systems LLC dba Billtrust, a Delaware Limited Liability Company, ("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:	Factor Systems LLC dba Billtrust
Address:	1009 Lenox Drive, Suite 101
City/Country:	Lawenceville, NJ 08648

PRIMARY SPREEDLY CONTACT

Name:	Helen Kruskamp
Title:	Enterprise Account Executive
Phone:	888-727-7750
Email:	hmkruskamp@spreedly.com

PRIMARY CUSTOMER CONTACT

Name:	Justin Main
Title:	VP, Integrated Payments & BPN
Phone:	
Email:	jmain@billtrust.com

SPREEDLY FINANCE CONTACT

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

CUSTOMER BILLING CONTACT

Name:	Accounts Payable
Phone:	AccountsPayable@Billtrust.com
Email:	Invoices@Billtrust.Coupahost.com

Background

Spreedly develops, markets and provides to its customers a web-based payments orchestration and tokenization platform, 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.

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 and costs).

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 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 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 reasonably suspects that Customer's use of the Platform has been for an unauthorized, illegal, or criminal purpose. 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.

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 the Platform or any features or functionality of the Platform except as permitted to provide the Permitted Uses as set forth above, to Customer's customers, 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 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, (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. At Customer's request and available at https://www.spreedly.com/gdpr-subprocessors, Spreedly will disclose their subcontractors utilized in providing the Platform and a description of the services each provides. Billtrust can object to the use of a subcontractor, including a Reputable Hosting Services Provider, on the basis that such would violate (i) applicable Laws; (ii) cause Billtrust to violate its contractual obligations with a third party; or (iii) other reasonable cause. Billtrust's objection must be in writing and include any specific reasons for its objection and options to mitigate. If Billtrust reasonably objects to the use of a subcontractor, the Parties will, for a period of no more than 30 days from the date of Billtrust's written objection, work together in good faith to attempt to find a commercially reasonable solution that avoids the use of the objected-to subcontractor. If no solution can be found which is satisfactory to both Parties, Billtrust, upon written notice to Spreedly, may terminate this Agreement immediately (or upon such date as Billtrust selects), with no further fees due, other than what has been accrued up to and including the date of termination.

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 materially comply with Section 2.2 or 2.3), or (B) otherwise breached a material term of this Agreement and have failed to cure or make good faith efforts to commence to cure such breach within thirty(30) 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. Spreedly reserves the right to delete all of Customer's Card Data and any other Customer Data thirty (30) days after the effective date of termination of this Agreement (the "Data Transfer Window"). If Customer requires additional time to arrange the 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 posted at Spreedly's website (currently: https://www.spreedly.com/support-services-terms) at the support level specified on the Order Form.

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 posted at Spreedly's website (currently: https://www.spreedly.com/support-services-terms) 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 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.

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. 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 necessary 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.

4.5. 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.

4.6. 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; (iv) was or is independently developed by the Receiving Party without reliance upon any Confidential Information; or (v) to the extent it was or is independently developed by the Receiving Party with use of or reliance upon Residual Information (as defined below).

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, so long as Customer complies with this Agreement, Spreedly will implement safeguards to protect against 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").

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 (collectively "Personal Information"), Spreedly will store, use and otherwise process such Personal Information in all material respects in accordance with all applicable laws relating to the privacy and protection of the Personal Information involved ("Data Privacy Laws"), including but not limited to the California Consumer Privacy Act of 2018 and its implementing regulations (as amended, restated or supplemented from time to time, "CCPA") where applicable. Spreedly will not access, use, handle, maintain, process, dispose of, or disclose Personal Information other than as permitted or required under this Agreement or Data Privacy Laws. Spreedly will limit dissemination of Personal Information to its employees and subcontractors who (i) need to know the information to enable Spreedly to perform its obligations or exercise its rights under this Agreement, and (ii) are bound by confidentiality obligations substantially equivalent to those provided for in this Agreement. Upon Customer's written request Spreedly will cooperate with Customer as may be reasonably required to enable Customer to comply with Data Privacy Laws, including by reasonably assisting Customer in complying with individuals' rights in regards to their Personal Information under Data Privacy Laws. In furtherance of the foregoing, based on the Customer Data that Customer will process using the Platform or otherwise provide to Spreedly, if and to the extent Data Privacy Laws require additional clauses to be executed by Spreedly beyond those set forth in this Agreement, then Customer will notify Spreedly in writing of such requirement and Spreedly will in good faith review, negotiate and consider adding such clauses as an addendum to this Agreement. In the absence of such notice Customer represents and warrants that no additional clauses are required.

6.3. CCPA Service Provider Compliance. Spreedly and Customer both agree that Customer is a business and Spreedly is a service provider under CCPA. Spreedly will: (i) not retain, use or disclose personal information for any purpose (including any commercial purpose) other than for the specific purpose of providing the Platform and performing the Support Services and Professional Services contemplated by this Agreement; (ii) not retain, use or disclose personal information outside of the direct business relationship between Customer and Spreedly; and (iii) not sell the personal information to any third parties. Spreedly certifies that it understands and will comply with the restrictions, duties and obligations set forth in this Section 6.3. In the event that any consumer makes a request directly to Spreedly with respect to exercising its privacy rights under CCPA, Spreedly will promptly notify Customer and provide Customer with a copy of the consumer request, inform the consumer that the consumer's request cannot be acted upon because the request has been sent to a service provider, provide Customer with a copy of such response, and reasonably cooperate with Customer in its efforts to respond and act on the consumer's request in accordance with the requirements of CCPA, in each case unless legally prohibited from doing so. As permitted and provided by CCPA, nothing in this Section 6.3 will prohibit Spreedly from retaining, using or disclosing the personal information in connection with: (z) retaining or employing another service provider as a subcontractor, provided the subcontractor meets the requirements for a service provider under CCPA; (y) Spreedly's internal use to build or improve the quality of its Platform or services, provided that the data used is anonymized data only and 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; (x) detecting data security incidents, or protecting against fraudulent or illegal activity; (w) complying with applicable laws; (v) complying with a civil, criminal or regulatory inquiry, investigation, subpoena, or summons by governmental authorities; (u) cooperating with law enforcement agencies concerning conduct or activity that Spreedly, Customer or a third party reasonably and in good faith believes may violate applicable law; or (t) exercising or defending legal claims. For purposes of this Section 6.3, the terms "business," "commercial purpose," "consumer," "personal information," "processing," "sell" and "service provider" will have the meanings given to such terms in CCPA.

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. Provided Spreedly is in compliance with the terms of this Agreement, all purchases are final and (except as otherwise expressly provided in this Agreement or in the applicable Order Form or Statement of Work) all undisputed Fees for services rendered 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 undisputed 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"), the parties will cooperate with each other to minimize 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 within thirty (30) days of receipt of the invoice. Customer is responsible for providing complete and accurate billing and contact information and notifying Spreedly of any changes to that information.

7.4. Late Payment. If Customer fails to make any payment when due and has been notified and given 5 days to remedy, 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 the rights and permissions only to the Customer Data 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 written consent from Customer in each instance, 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. Within 30 days of the Effective Date, the parties will cooperate to draft a press release or other public announcement related to the subject matter of this Agreement and the relationship between the parties. The parties will not unreasonably withhold or delay their consent to press releases or public announcements.

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 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 thirty (30) days after the non-breaching Party provides the breaching Party with written notice regarding such breach.

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) Spreedly will immediately discontinue Customer's access to the Platform subject to the Transition Period set forth below; (ii) Customer will complete all pending transactions and stop accepting new transactions through the Platform; (iii) each Party will discontinue use of any of the other Party's trademarks and immediately remove any references and logos from its website; and (iv) each Party will promptly return to the other or, if so directed by the other Party, destroy all originals and copies of any Confidential Information of the other Party (including all notes, records and materials developed therefrom).

9.4. Transition Assistance. Upon termination or expiration of this Agreement or an Order Form for any reason, then upon request by Customer made prior to the expiration date, Spreedly will continue to provide access and use of the Platform for a minimum of 18 months 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.

9.5. Surviving Terms. Sections 1 (Definitions), 5 (Confidentiality), 7 (Fees and Payment), 8 (Ownership and Intellectual Property Rights), 9.3 (Effect of Termination), 9.4 (Transition Assistance), 10.c (Disclaimer of Warranties), 11 (Indemnification), 13 (Limitations of Liability), 14 (Miscellaneous) and this Section 9.5 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 the Parties, enforceable against the other 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 manner. 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.

10.4. 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" to the extent caused by Spreedly; (iii) Spreedly's failure to remain compliant with PCI-DSS or (iv) material breach of the Agreement or violations of any applicable 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 material 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 shall have sole 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. Subject to the above, 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 THE AMOUNT OF FEES PAID TO SPREEDLY BY CUSTOMER DURING THE TWELVE-MONTH PERIOD IMMEDIATELY PRECEDING SUCH CLAIM, PROVIDED HOWEVER, IN THE EVENT OF A) DATA INCIDENT OR B) FOR CLAIMS RELATED TO A PARTY'S INDEMNITY OBLIGATIONS, A PARTY'S TOTAL AND CUMULATIVE LIABILITY WILL NOT EXCEED THE AMOUNT OF FEES PAID TO SPREEDLY DURING THE THIRTY SIX (36) MONTH PERIOD PRIOR TO THE INCIDENT GIVING RISE TO THE CLAIM. NOTWITHSTANDING THE FOREGOING THESE LIMITS 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 Delaware, without regard to its conflicts of law provisions.

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 ("Assignment") however in the event of a Spreedly Assignment Spreedly shall give Customer 90 days' written notice. 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. Compliance with Export Controls Laws. Each Party shall comply with all applicable U.S.A. export and re-export control Laws, including the Export Administration Regulations ("**EAR**") maintained by the U.S.A. Department of Commerce. Each Party shall not directly or indirectly export, re-export, transfer, divert, or otherwise dispose of any export regulated items or technology to any destination or person prohibited by the Laws of the U.S.A., without obtaining prior authorization from the competent government authorities as required by those Laws. Any such authorized exportation shall only be done in coordination and with the consent of the other Party.

14.12. Equal Opportunity/Affirmative Action. Customer is an equal opportunity employer and federal contractor. To the extent applicable to Spreedly's performance or obligations under this Agreement, Spreedly shall comply with Executive Order 11246, Section 503 of the Rehabilitation Act of 1973, the Vietnam Era Veterans' Readjustment Assistance Act of 1974, and the implementing regulations for each found at 41 CFR Part 60, all as in effect at any time, and Spreedly shall comply with, and this Agreement incorporates, as if they were contained in this Agreement, the "equal opportunity clauses" stated at 41 CFR sections 60-1.4(a), 60-741.5(a), and 60-300.5(a), and Spreedly shall incorporate those equal opportunity clauses in all applicable subcontracts subsequently executed to the extent required by 41 CFR section 60-1.4(d).

14.13. Notice of Employee Rights Under Federal Labor Laws. To the extent applicable to Spreedly's performance or obligations under this Agreement, Spreedly shall comply with, and this Agreement incorporates, as if they were contained in this Agreement, the language stated in 29 CFR Part 471, Appendix A to Subpart A (Text of Employee Notice Clause).

14.14. 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.

[Signatures on Next Page]

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. (“**Spreedly**”)	Factor Systems LLC dba Billtrust (“**Customer**”)
DocuSigned by: Justin Benson C9132818B2F844A...	DocuSigned by: Andrew Herning 51AF8FB38ADD405...
Authorized Signature	Authorized Signature
Justin Benson	Andrew Herning
Print Name	Print Name
CEO	Senior VP, Finance
Title	Title
2/15/2023	2/15/2023
Date	Date

SCHEDULE A

ORDER FORM [#]

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

To:
Customer Legal Name: Factor Systems LLC dba Billtrust
Tax ID:
Billing Address: 1009 Lenox Drive, Lawrenceville, NJ 08648
Sales Rep:

Order Form Issued:

Offer Valid Until:

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

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

1) Order Form Term

2) Platform Fees:

3) API Usage Fees:

4) Account Updater:

5) Payments:

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

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

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

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

SAMPLE ONLY DO NOT SIGN

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.

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.

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 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:

Customer Security Contact:	**Spreedly Security Contact:**
Name: Ken Hehl	Name: Jennifer Rosario
Telephone:	Telephone: 888-727-7750
Email: Security@billtrust.com	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. The provisions of the Billtrust Data Processing Addendum attached hereto as Schedule C and as updated from time to time at https://www.billtrust.com/privacy-terms/ are hereby incorporated by reference and will be deemed to have the same force and effect as if set forth in full herein;.

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 Data Incidents 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 Data Incidents, and encouraging reporting actual or reasonably suspected Data Incidents, including: (1) training Supplier's personnel with access to Customer Data to recognize actual or potential Data 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

BILLTRUST
DATA PROCESSING ADDENDUM

VENDORS

This Billtrust Data Processing Addendum (this "**Addendum**"), including its exhibits, is entered into by and between Factor Systems, LLC d/b/a Billtrust, acting on its own and as agent for the Billtrust Affiliates (collectively referred to as "**Billtrust**"), and Spreedly, Inc. (the "**Vendor**") (each, a "**Party**" and, collectively, the "**Parties**"). This Addendum (including its exhibits) form part of any written or electronic agreement(s) between Billtrust or a Billtrust Affiliate and Vendor or a Vendor affiliate for the purchase of services pursuant to which the Vendor or a Vendor affiliate processes Personal Data for which Billtrust or a Billtrust Affiliate qualifies as a Controller or Processor (the **"Agreement"**).

This Addendum sets out obligations of the Parties with respect to data protection in relation to the Agreement. The Addendum will become effective when the last Party signs it, as indicated by the date below that Party's signature (the "**Effective Date**"). For the purposes of this Addendum only, and except where indicated otherwise, the term "Vendor" shall include Vendor and Vendor affiliates and the term "Billtrust" shall include Billtrust and/or where applicable Billtrust Affiliates.

To the extent of any conflict or inconsistency between the provisions of this Addendum and any provision of the Agreement, the provisions of this Addendum shall prevail and take precedence over such conflicting or inconsistent provisions in the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended or supplemented by, and including, this Addendum and its exhibits.

RECITALS

WHEREAS, the Parties entered into the Agreement and have retained the power to alter, amend, revoke, or terminate the Agreement as provided in the Agreement; and

WHEREAS, the Parties now wish to amend the Agreement to ensure that Personal Data (as defined below) transferred between the Parties is Processed in compliance with Applicable Data Protection Laws and legal requirements.

NOW, THEREFORE, in consideration of the mutual agreements set forth in this Addendum, the Parties agree as follows:

1. Definitions

1.1 Capitalized definitions not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified or supplemented below, the definitions of the Agreement shall remain in full force and effect.

1.2 For the purpose of interpreting this Addendum, the following terms shall have the meanings set out below:

(a) "**Applicable Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including laws of the European

Union (or any member state thereof) and the laws of any other country, province, or state to which the Processing of the Personal Data is subject;

(b) "**Billtrust Affiliates**" means any companies which are controlled by BTRS Holdings Inc, which control Billtrust or which are under common control with Billtrust and either: (i) are Controllers of any Personal Data; and/or (ii) on whose behalf Vendor and/or any Sub-Processor otherwise processes any Personal Data. For these purposes "control" and its derivatives means to hold, directly or indirectly, more than 50% of the respective shares with voting rights.

(c) "**Billtrust Personal Data**" means any Personal Data Processed by or on behalf of Vendor on behalf of Billtrust and/or any Billtrust Affiliate pursuant to or in connection with the Agreement. This definition is used when Billtrust acts as a Controller and may include Billtrust human resources data, business contact information, and/or vendor relationship data, among other data types.

(d) "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;

(e) "**Customer**" means a natural person or entity that receives products or services from Billtrust and/or any of Billtrust Affiliates.

(f) "**Customer Personal Data**" means any Personal Data originating from the Customer and Processed by or on behalf of Vendor, on behalf of Billtrust and/or any Billtrust Affiliate pursuant to or in connection with the Agreement. This definition is used when Billtrust acts as a Processor.

(g) "**GDPR**" or "**General Data Protection Regulation**" means, as appropriate and as amended from time to time, 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, and Repealing Directive 95/46/EC,";

(h) "**Processor**" means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller;

(i) "**Processing**" (or any cognate terms) means any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(j) "**Personal Data**" means any information relating to an identified or identifiable* natural person (a "**Data Subject**") pertaining to Billtrust (and the Data Subjects, respectively) Processed by Vendor on behalf of Billtrust pursuant to or in connection with the Agreement

**an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*;

(k) “**Personal Data Breach**” means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data which Vendor Processes on behalf of Billtrust and/ or in connection with the Agreement;

(l) “**Personal Data Recipient**” means Vendor, a Sub-Processor, or both collectively;

(m) “**Restricted Transfer**” means any transfer of Personal Data to a third country or an international organization that would be prohibited by Applicable Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Applicable Data Protection Laws);

(n) “**Vendor**” means the party, as indicated in the opening paragraph of this Addendum, that has entered into the Agreement with Billtrust, including all affiliates of that entity that are also bound by the Agreement, if any;

(o) “**Services**” means the services and other activities carried out by or on behalf of Vendor for Billtrust and/or any Billtrust Affiliate pursuant to the Agreement;

(p) **“Standard Contractual Clauses”** means the Standard Contractual Clauses approved by the European Commission in decision 2021/914 (as updated from time to time if required by law or at the choice of Billtrust to reflect the latest version adopted by the European Commission);

(q) "**Sub-Processor**” means any third party appointed by or on behalf of Vendor to Process Personal Data on behalf of Billtrust in connection with the Agreement;

(r) “**Supervisory Authority**” in the context of the GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR; in the context of the UK GDPR, means the UK Information Commissioner’s Office; and in the context of the FADP, the FDPIC. (see definitions in **Exhibit D**)

2. Applicability

2.1 This Addendum will apply to the Processing of all Personal Data, regardless of country of origin, place of Processing, location of Data Subjects, or any other factor.

3. Processing of Personal Data

3.1 In the context of this Addendum and its exhibits, with regard to the Processing of Personal Data, 1) Billtrust may act as a Controller, and Vendor may act as a Processor; or 2) Billtrust may act as a Processor, and Vendor may act as a Sub-Processor. For the avoidance of doubt, the aforementioned situations fall within the scope of and are covered by this Addendum. The respective roles of the Parties for the Processing of Personal Data in the context of the Agreement is set out in **Exhibit A (Details of processing)**, Section A.

(a) The Parties acknowledge and agree that in relation to any Billtrust Personal Data provided or made available to Vendor for Processing in connection with the Services, Billtrust is the Controller and Vendor is a Processor, depending on the Services described in the relevant Agreement;

(b) in relation to any Customer Personal Data, Customer is the Controller, Billtrust is a Processor, and Vendor is a Sub-Processor.

3.2 Vendor warrants:

(a) to comply with all Applicable Data Protection Laws in the Processing of Personal Data; and

When Vendor is acting as a Processor or Sub-Processor:

(b) Process Personal Data pursuant to the Agreement (including with regard to international transfers of Personal Data), unless such Processing is required by Applicable Data Protection Laws to which the relevant Personal Data Recipient is subject, in which case Vendor, shall to the extent permitted by Applicable Data Protection Laws, inform Billtrust of that legal requirement before the respective act of Processing of that Personal Data;

(c) only conduct transfers of Personal Data in compliance with all applicable conditions, as laid down in Applicable Data Protection Laws; and

(d) promptly update, when necessary, all information, as provided in **Exhibit A (Details of processing)**, attached hereto and incorporated by reference, and keep all such information complete and up to date.

3.3 Where Vendor is acting as a Processor or Sub-Processor, Billtrust instructs Vendor (and authorizes Vendor to instruct each Processor or Sub-Processor it engages) to Process Personal Data and, in particular, transfer Personal Data to any country or territory, only as reasonably necessary for the provision of the Services and consistent with the Agreement, this Addendum and the relevant Exhibits. In the event that, in Vendor's opinion, a Processing instruction given by Billtrust may infringe Applicable Data Protection Laws, Vendor shall immediately inform Billtrust.

3.4 **Exhibit A** sets forth certain information regarding Vendor's Processing of Personal Data. The Parties may from time to time amend Exhibit A by mutual agreement or pursuant to 3.2(d) above.

3.5 Where Billtrust is acting as a Processor, it warrants that it:

(a) Processes Personal Data only on behalf of its Customers' relevant documented instructions and, in turn, instructs Vendor to carry out such Processing activities on behalf of Billtrust in accordance with said instructions of Billtrust's Customers; and

(b) has obtained the prior authorization from its respective immediate Customer, who is typically acting as a Controller regarding the processing of Personal Data, for subcontracting its activities to Vendor.

4. Vendor Personnel

4.1 Vendor shall take reasonable steps to ensure the reliability of any of its employees, agents, or contractors who may have access to Personal Data.

4.2 Vendor shall ensure that access to Personal Data is strictly limited to those individuals who need to know or access it, as strictly necessary to fulfill the documented Processing instructions given to Vendor by Billtrust or to comply with Applicable Data Protection Laws.

4.3 Vendor shall ensure that all such individuals are subject to formal confidentiality undertakings, professional obligations of confidentiality, or statutory obligations of confidentiality.

5. Security of Processing

5.1 Taking into account the state of the art and the high sensitivity of the Personal Data, Vendor shall, with regard to Personal Data, implement and maintain appropriate technical and organizational security measures to ensure a level of security appropriate to that risk (including, as appropriate, the measures referred to in Article 32(1) of the GDPR) as well as assist Billtrust with regard to ensuring Billtrust's compliance with its own obligations related to its security measures (including, without limitation, as required by Article 32 of the GDPR). In particular, the Vendor shall take the Minimum Security Measures as listed under **Exhibit B** to this Addendum.

5.2 In assessing the appropriate level of security, Vendor shall take account, in particular, of the risks that are presented by the nature of such Processing activities, and particularly those related to possible Personal Data Breaches.

5.3 Without limiting clauses 5.1 and 5.2, Vendor shall, and shall cause each Processor or Sub-Processor to, comply with the security obligations set out in the Addendum including **Exhibit B**.

6. Sub-processing

***When Vendor is acting as a Processor or Sub-Processor*:**

6.1 Billtrust authorizes Vendor to appoint (and permit each Sub-Processor appointed in accordance with this Section 6 to appoint) Sub-Processors in accordance with this Section 6 and any possible further restrictions, as set out in the Agreement, as the case may be.

6.2 Vendor may continue to use those Sub-Processors already engaged by Vendor as of the date of this Addendum, subject to Vendor meeting the obligations set out in Section 6.5. The list of Vendor's Sub-Processors as of the Effective Date is provided in **Exhibit C** to this Addendum.

6.3 Subject to Section 6.2, Vendor shall notify Billtrust in advance of appointing any new Sub-Processors no less than 90 days of their proposed first use for Processing under the Agreement. Within 30 days after Vendor's notification of the intended change, Billtrust can object to the addition of a Sub-Processor on the basis that such addition would violate (i) Applicable Data Protection Laws; (ii) cause Billtrust to violate its contractual obligations with a third party; or (iii) other reasonable cause. Billtrust's objection must be in writing and include any specific reasons for its objection and options to mitigate. If Billtrust does not object within such period, the Sub-Processor may be engaged by Vendor without further notice.

6.4 If Billtrust reasonably objects to a proposed appointment as set out in Section 6.3, the Parties will, for a period of no more than 30 days from the date of Billtrust's refusal, work together in good faith to attempt to find a commercially reasonable solution for Billtrust that avoids the use of the objected-to Sub-Processor. If no solution can be found which is satisfactory to both parties, Billtrust, upon written notice to Vendor, may terminate the Agreement immediately (or upon such date as Billtrust selects), with no further fees due, other than what has been accrued up to and including the date of termination.

6.5 With respect to each Sub-Processor, Vendor shall:

(a) before the Sub-Processor first Processes Personal Data (or, where relevant, in accordance with Section 6.2), carry out adequate due diligence to ensure that the Sub-Processor is capable of providing the level of protection and security for Personal Data required by this Addendum, the Agreement, and Applicable Data Protection

Laws; and must disclose the result of the conducted due diligence procedure to Billtrust and provide Billtrust with the documents used in the due diligence procedure upon request of Billtrust; and

(b) ensure that the arrangement between Vendor and the prospective Sub-Processor is governed by a written contract that includes terms which offer at least the same level of protection for Personal Data as those set out in this Addendum, and that such terms meet the requirements of Applicable Data Protection Laws.

6.6 Where any Sub-Processor fails to fulfil its data protection obligations under such written contract (or in the absence thereof, as the case may be), Vendor shall remain fully liable to Billtrust for the performance of the respective Sub-Processors' obligations under such contract or in connection with this Addendum.

7. Rights of the Data Subjects

7.1 When acting as Processor or Sub-Processor, taking into account the nature of the Processing, Vendor shall assist Billtrust (and for Customer Personal Data: the Customer) by implementing appropriate technical and organizational measures, insofar as this is possible, to respond to requests to exercise rights of the Data Subjects under Applicable Data Protection Laws.

7.2 With regard to the rights of the Data Subjects within the scope of this Section 7, Vendor shall:

(a) promptly notify Billtrust if any Personal Data Recipient receives a request from a Data Subject under any Applicable Law with respect to Personal Data;

(b) ensure that the Personal Data Recipient does not respond to that request, except on the documented instructions of Billtrust, or as required by Applicable Data Protection Laws to which the Personal Data Recipient is subject, in which case Vendor shall, to the extent permitted by Applicable Data Protection Laws, inform Billtrust of that legal requirement before the Personal Data Recipient responds to the request; and

(c) promptly comply with any documented instructions from Billtrust regarding response to a request to exercise rights of the Data Subjects under Applicable Data Protection Laws.

8. Personal Data Breach

***When Vendor is acting as a Processor or Sub-Processor*:**

8.1 If Vendor discovers, is notified of, or has reason to suspect a Personal Data Breach affecting Personal Data, Vendor will provide notice to Billtrust within 24 hours of becoming aware of a confirmed or suspected Personal Data Breach.

8.2 Vendor shall provide Billtrust with sufficient information to assist Billtrust, or to allow Billtrust to assist its clients, so that each affected entity can meet its respective obligations pursuant to Applicable Data Protection Laws, including any obligations to report the Personal Data Breach to the competent supervisory authorities, and/or inform the Data Subjects.

8.3 Vendor shall co-operate with Billtrust and take all reasonable commercial steps (at Vendor's own expense) to assist Billtrust in the investigation, mitigation, and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

9.1 For services that the Vendor provides as Processor or Sub-Processor, Vendor shall provide Billtrust with relevant information and documentation, and assist Billtrust in complying with its obligations, with regard to any data protection impact assessments or prior consultations with supervisory authorities, when Billtrust determines that such data protection impact assessments or prior consultations are required pursuant to Applicable Data Protection Laws (including, without limitation, Article 35 or 36 of the GDPR), but in each such case solely with regard to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the respective Personal Data Recipient.

10. Deletion or Return of Personal Data

10.1 Vendor shall provide Billtrust with the technical means, consistent with the way the Services are provided, to request the deletion of Personal Data upon the request of Billtrust, unless Applicable Data Protection Laws require storage of any such Personal Data.

10.2 Vendor shall promptly, following the date of cessation of Services involving the Processing of Personal Data, at the choice of Billtrust, delete or return all Personal Data to Billtrust, as well as delete existing copies, unless Applicable Data Protection Laws require storage of any such Personal Data. In the event that Billtrust has not specified its choice, it shall be deemed that Vendor is obliged to delete all Personal Data from Billtrust.

10.3 Vendor shall also cause all Sub-Processors that may have received any Personal Data to delete or return, as applicable, all such Personal Data without undue delay.

10.4 Upon request from Billtrust, Vendor shall provide written certification to Billtrust that it has fully complied with this Section 10.

11. Audit Rights

11.1 Billtrust may request, and Vendor will provide (subject to obligations of confidentiality), all information reasonably necessary to demonstrate compliance with the obligations set forth in this Addendum and Applicable Data Protection Laws, including but not limited to a current SOC 1/2 audit report, ISO 27001 certificate, or other substantially similar third party certification or audit of industry standard.

11.2 If Billtrust after having reviewed such audit report(s), still deems that it requires additional information (for example, Vendor’s policies and procedures regarding data protection, information from Vendor’s Sub-Processors, or any other relevant information) Vendor shall further assist and make available to Billtrust all such additional information and/or documentation (including relevant provisions of contracts with Sub-Processors) necessary to demonstrate compliance with this Addendum and/or Applicable Data Protection Laws.

When acting as a Processor or Sub-Processor:

11.3 In addition, Vendor shall reasonably allow for and contribute to audits, including remote inspections of the Services, by Billtrust (on behalf of itself or its clients) or an auditor mandated by Billtrust (on behalf of itself or its clients) with regard to the Processing of the Personal Data by the Personal Data Recipient.

11.4 Billtrust shall give reasonable notice of any audit or inspection to be conducted under section 11.3 and agree to subject such audit or inspection to the Vendor’s security policy and other confidentiality requirements, where legally permissible.

11.5 If it is established during an audit that Vendor has failed to comply with its obligations under this Addendum, Billtrust shall notify Vendor and Vendor shall take all measures necessary to ensure its compliance as soon as reasonably practicable.

11.6 Billtrust shall bear its own third party costs in connection with such inspection or audit, unless the findings of the audit show that Vendor and/or any Sub-Processor failed to comply in any material respect with the provisions of this Addendum, in which case Vendor shall reimburse all reasonable and documented costs incurred by Billtrust in connection with such inspection or audit.

12. Jurisdiction Specific Terms

12.1 To the extent Vendor processes Personal Data originating from, or protected by, Applicable Data Protection Laws in one of the jurisdictions listed in **Exhibit D**, then the terms specified in **Exhibit D** with respect to the applicable jurisdiction(s) ("**Jurisdiction Specific Terms**") shall apply in addition to the terms of this Addendum.

12.2 Billtrust may update **Exhibit D** from time to time, to reflect changes in or additions to Applicable Data Protection Laws to which Billtrust is subject. If Billtrust updates **Exhibit D**, it will provide the updated **Exhibit D** to Vendor. If Vendor does not object to the updated **Exhibit D** within 30 days of receipt, Vendor will be deemed to have consented to the updated **Exhibit D**.

12.3 In case of any conflict or ambiguity between the Jurisdiction Specific Terms and any other terms of this Addendum, the applicable Jurisdiction Specific Terms will take precedence.

13. No Selling of Personal Data

13.1 When acting as Processor or Sub-Processor, Vendor acknowledges and confirms that it does not receive any Personal Data as consideration for any services or other items that Vendor provides to Billtrust. Billtrust retains all rights and interests in Personal Data. Vendor agrees to refrain from taking any action that would cause any transfers of Personal Data to or from Vendor to qualify as selling or sharing Personal Data under Applicable Data Protection Laws.

14. General Terms

14.1 This Addendum supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between the Vendor and Billtrust.

14.2 All clauses of the Agreement, that are not explicitly amended or supplemented by the clauses of this Addendum, and as long as this does not contradict with compulsory requirements of Applicable Data Protection Laws under this Addendum, remain in full force and effect and shall apply.

14.3 In the event of any conflict between the Agreement (including any annexes and appendices thereto) and this Addendum, the provisions of this Addendum shall prevail. This is without prejudice to the order of precedence between the Jurisdiction Specific Terms and any other provision in this Addendum including Section 12.3 above.

14.4 Should any provision of this Addendum or its Exhibits be found legally invalid or unenforceable, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of the Addendum and/ or the respective Exhibit will continue in effect.

14.5 If Vendor makes a determination that it can no longer meet any of its obligations in accordance with this Addendum, it shall promptly notify Billtrust of that determination, and cease the Processing or take other reasonable and appropriate steps to remediate.

14.6 If you are accepting the terms of this Addendum on behalf of an entity, you represent and warrant to Billtrust that you have the authority to bind that entity and its affiliates, where applicable, to the terms and conditions of this Addendum.

14.7 In the event that Vendor materially breaches this Addendum, or suffers a material Personal Data Breach, Billtrust may, upon written notice to the Vendor, terminate the relevant Service Agreement immediately (or upon such date as Billtrust selects), with no further fees due, other than what has been accrued up to and including the date of termination.

14.8 This Addendum and its exhibits is governed by the laws that apply to the Agreement. Any disputes between the Vendor and Billtrust as a result of the creation, fulfillment, and/ or interpretation of the Addendum shall be exclusively submitted to the courts appointed as per the Agreement.

Exhibit A: Details of processing

A. List of Parties

DATA EXPORTER: The Billtrust entity identified in the Agreement and Addendum with an address as set forth in the Agreement.

Contact details: privacy@billtrust.com, see signature section of this Addendum for additional details.

Activities relevant for the Addendum: to receive the Services pursuant to the Agreement.

Role:

- For **Billtrust Personal Data**, Controller: see Processing Annex 1

- For **Customer Personal Data**, Processor: see Processing Annex 2:

DATA IMPORTER: The Vendor entity identified in the Agreement and this Addendum with an address as set forth in the Agreement.

Contact details: See signature section of this Addendum for additional details.

Activities relevant for the Addendum: to provide the Services set out in the Agreement.

Role:

- For **Billtrust Personal Data**, Parties have agreed that Vendor’s role for the Services set out in the Agreement is: Processor

- For **Customer Personal Data**: a Sub-Processor (the Parties acknowledge and agree that Billtrust supplies a service to its Customers, and that Billtrust has appointed Vendor in connection with such services pursuant to the Agreement).

B. Description of transfer

This section sets out the Processing Annexes concerning Personal Data transferred to a third country by the Parties pursuant to the Agreement. The Parties may agree additional Processing Annexes from time to time in accordance with the terms of the Agreement. There are two categories of data envisaged by this Agreement:

Processing Annex 1: Billtrust Personal Data, Controller to Processor

Processing Annex 2: Customer Personal Data, Processor to Sub-Processor

Processing Annex 1 – Billtrust Personal Data

This Processing Annex describes Personal Data transferred by Billtrust as Controller and Data Exporter(s) and the purposes for which that Personal Data may be Processed by the Vendor as Data Importer(s) in the role of Processor.

Categories of data subjects whose personal data is transferred:	Categories of data subjects are defined in the Agreement. For the avoidance of doubt, categories include: Billtrust Employees - Past, present and future staff of the Data Exporter (including volunteers, agents, independent contractors, interns, temporary and casual workers). For Agreements related to our human resources recruitment, also included is the category of Job candidates and applicants of the Data Exporter. For Agreements related to our marketing and events also included is staff of past, present and potential users of Billtrust Services (including those that attend or sign up for Billtrust events or conferences).
Categories of personal data transferred:	Categories of personal data transferred are defined in the Agreement. For the avoidance of doubt, categories include: *Billtrust Employees* Identification data: e.g. civil/marital status, photograph, nationality, corporate and national identifier, IP address; personal and business contact details: e.g. address, telephone number, email address, fax number, emergency contact information. *For Agreements related to our human resources*, also included is personal details and identification data; employment details: e.g job title, company name, grade, occupation code, geographic location; national identifiers; e.g. national ID/passport number, visa or immigration status; academic and professional qualifications; financial data. *For Agreements related to our marketing and events, also included is p*ersonal detail and business contact information: name; e-mail address; phone number; office address; Name of employer; job title; IT-related data: IP addresses of visitors to the Data Exporter's websites; correspondence data and other communications.
Sensitive data transferred (if applicable) and applied restrictions or safeguards, or additional security measures:	Billtrust does not anticipate the collection of any sensitive data as a Controller from any individuals other than Billtrust employees in connection with valid employment purposes. Such collection will only concern limited sensitive data, for example, health-related information for the purpose of managing employee absences, or disabilities in order to provide access to our premises. Race and ethnicity may appear indirectly on photos and other information available on passports and national IDs, which are necessary to comply with local immigration laws and for employee travel management. However, race/ethnicity are not Processed purposefully in Europe. Trade union membership may be collected but only where permitted and for the purposes defined under Applicable Data Protection Laws.

	The Parties will only export sensitive data where such export is not otherwise restricted by Applicable Data Protection Laws. The safeguards are set out in Exhibit B.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous
Nature of the processing:	Vendor will process the Personal Data to deliver the Services pursuant to the Agreement.
Purpose(s) of the data transfer and further processing:	The Data Importer will provide assistance to Data Exporter in undertaking that Processing.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	For the duration of the Agreement between Data Exporter and Data Importer and in accordance with the Addendum section 10.Deletion or Return of Personal Data.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Where the Data Importer engages Processors (or sub-Processors) it will do so in compliance with the terms of the Standard Contractual Clauses. The subject matter, nature and duration of the Processing activities carried out by the Processor (or Sub-Processor) will not exceed the Processing activities as described in the Agreement.

Processing Annex 2 - Billtrust Customer Personal Data

This Annex describes the types of Customer Personal Data transferred to a Vendor when Billtrust and/or Billtrust Affiliates act as a Processor and Vendor acts as Sub-Processor. This Annex also describes the purposes for which such Customer Data may be Processed..

Categories of data subjects whose personal data is transferred:	Data subjects of which a Billtrust Customer is the Controller, which includes users of the Billtrust products and services e.g. Customer's employees, employees of the customer of the Billtrust Customer, and other Customers' users of the services (whether current, past or potential).
Categories of personal data transferred:	The categories of Personal Data to be Processed are personal identifiers and business contact information, including business address and email address, first and last name, login credentials; financial information such as credit card company, credit card number and expiration date, credit card billing address, bank account information; invoicing information and order data; IT information such as user log-in and information from the products and services.
Sensitive data transferred (if applicable) and applied restrictions or safeguards, or additional security measures:	Billtrust does not anticipate the processing of any sensitive data with respect to Customer data. The safeguards are set out in Exhibit B.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous.
Nature of the processing:	Vendor will process the Personal Data to deliver the Services pursuant to the Agreement.
Purpose(s) of the data transfer and further processing:	The purpose of processing of Customer Personal Data pertains to the provision of specified products and services implementation under the Agreement.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	For as long as (i) the Data Exporter (Billtrust) and Data Importer (Vendor) have an Agreement for Services and (ii) the Data Exporter (Billtrust) provides services to its Customer which require the Processing of Billtrust Customer Data.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Where the Data Importer engages Processors or Sub-Processors it will do so in compliance with the terms of the Standard Contractual Clauses and this Addendum. The subject matter, nature and duration of the Processing activities carried out by the Processor or Sub-Processor will not exceed the Processing activities as described in the Agreement.

C. Competent Supervisory Authority

The competent Supervisory Authority shall be determined as follows:

Where Billtrust is established in an EU Member State: the competent Supervisory Authority shall be the Supervisory Authority of that EU Member State in which Billtrust is established.

Where Billtrust is not established in an EU Member State: the competent Supervisory Authority shall be the Supervisory Authority of the Netherlands.

Exhibit B: Minimum Security Measures

Vendor Information Security Requirements

A. INTRODUCTION

These Vendor Information Security Requirements ("Requirements") describe Vendor's obligations with respect to information security and data protection in relation to the Services provided by Vendor to Billtrust under the Agreement between Billtrust or Billtrust's affiliate(s) and Vendor. For the purpose of these Requirements, the term "Vendor" shall mean a third-party providing Software or Services to Billtrust or a Billtrust Customer and who is identified by either their entity name or the defined terms "Vendor", "Service Provider", "Supplier", "Provider", or "Consultant" in the Agreement. Terms capitalized and used in these Requirements will have the meanings ascribed to them under the Addendum unless specifically provided for in these Requirements otherwise. In the event an entity other than Vendor does so under a contract with Vendor or otherwise for or on behalf of Vendor, Vendor will ensure by contract or otherwise that the following provisions apply correspondingly to the other entity for the benefit of Billtrust.

For the avoidance of doubt, to the extent of any conflict or inconsistency between the provisions of this Addendum and any of the Requirements listed below, the Requirements shall prevail and take precedence over such conflicting or inconsistent provisions in this Addendum, subject to Exhibit D, clause 1.3(e).

B. SECURITY MEASURES

1. Billtrust acknowledges and agrees that Vendor may change its security policies and related security measures, provided that Vendor maintains, at all times, an overall level of security as least as stringent as the one set forth in this Addendum.

2. The Vendor Processes Personal Data in accordance with applicable law to which Processor is subject and in accordance with the data security requirements of the controls defined by latest available SSAE 18 SOC 2 or ISO 27001 implemented controls (or equivalent standard).

3. Comprehensive security policies, standards and procedures are developed and maintained by a designated person responsible for privacy and data protection, such as a Chief Security Officer, and reviews of the information security policy are completed at least annually.

4. The Vendor must provide its personnel, third party consultants, and contractors with annual information security awareness training including, but not limited to, education on general safety awareness, relevant security policies and procedures, and Personal Data Processing.

C. ACCESS CONTROL

1. Vendor shall maintain suitable measures in order to prevent unauthorized persons from gaining access to the data Processing equipment (namely database and application servers and related hardware) where the Personal Data is Processed or used. This is accomplished by measures like:

- establishing security areas and establishing procedures for working in such areas;

- protection and restriction of access paths;

- securing the data Processing equipment and personal computers;
- establishing access authorizations and appropriate restrictions to authorized personnel;
- all access to the data centre where Personal Data is hosted is logged, monitored, and tracked;
- the data centre where Personal Data is hosted is secured by a security alarm system; and
- other appropriate security measures.

2. The Vendor manages information system accounts by implementing centralized control of user access and administrator functions; access is assigned and periodically reviewed to ensure least privilege access is granted.

3. Where the Vendor (a) stores, processes, or transmits Payment Card Data in connection with the Services under the Agreement, or (b) is otherwise subject to PCI DSS, computing systems processing credit card (PAN) and ACH information must be physically and/or logically isolated to reduce the risk of unauthorized access.

4. The Vendor maintains suitable measure to prevent its systems from being used by unauthorized persons, such as:

- annual review and certification of logical access accounts;
- log file of events (monitoring of break-in-attempts);
- issuing and safeguarding of identification codes;
- employee policies and training with respect to each employee's access rights to Personal Data (if any), including informing employees about their obligations and the consequences of any violations of such obligations, to ensure that employees will only access Personal Data and resources required to perform their job duties;
- all access to data content is logged and monitored;
- users with access to Vendor's information resources must utilize User IDs that are specifically assigned to them;
- controls minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts;
- -processes and procedures for password strength requirements are in line with applicable regulatory or industry guidelines;
- -effective and measured disciplinary action against individuals who access Personal Data without authorization;
- release of Personal Data only to authorized persons;
- control of files, controlled and documented destruction of Personal Data; and

- policies controlling the retention of back-up copies.

D. AVAILABILITY CONTROL

1. Vendor shall maintain suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This is accomplished by:

- infrastructure redundancy;
- tape backup is stored off-site and available for restore in case of failure of SAN infrastructure for database server;
- complying with Processor's business continuity policy; and
- any detected security incident is recorded.

E. INPUT CONTROL

Vendor implements suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data has been input into Personal Data Processing systems or removed. This is accomplished by:

- an authorization policy for the input of data into memory, as well as for the reading, alteration and disposal of stored Personal Data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and disposal of stored Personal Data;
- utilization of user codes (passwords);
- following a policy according to which all employees of Vendor who have access to Personal Data Processed for Billtrust shall reset their passwords at a minimum once in a 180 day period, or as defined in Processor's IT Security Policy and in line with potential multi-factors of authentication;
- providing that entries to Processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
- automatic log-off of user IDs that have not been used for a substantial period of time;
- proof established Vendor's organization of the input authorization; and
- electronic recording of entries.

F. OPERATIONS MANAGEMENT

1. Vendor information resources are established and maintained in accordance with information technology standard builds and the applicable platform-specific security baseline.

2. Vendor is responsible for installing available patches on the information resources under their control in a timely fashion after the release. Critical security patches relevant to the protection of sensitive information (including Personal Data) must be installed as soon as reasonably possible after release.

3. Vendor will perform vulnerability scans and penetration tests on a periodic basis and no less than annually.

4. Vulnerability remediation efforts, including patch implementations, must be coordinated and processed according to the Vendor's change management process, including meeting all testing and/or documentation requirements.

5. System lifecycle and change management processes and controls are established.

6. Development, test and production environments must be separated physically, or at a minimum logically, to reduce the risk of accidental change or unauthorized access to production software and data.

7. The Vendor must establish processes and procedures for separation of duties between development/test and production environments.

8. Vendor maintains a change control process for the change of backup and restore documentation and deploys appropriate technologies to manage backup and restore tasks.

9. The Vendor must establish processes and procedures for virus detection software configuration.

10. Information resources are backed up and can be recovered in a timely manner.

11. The Vendor must establish a record retention schedule that supports regulatory requirements.

12. The Vendor employees, third party contractors and vendors must adhere to all copyright laws and packaged software license agreements.

13. Configuration management and software standards are established.

G. SECURITY DEFENSE, MONITORING, AND RESPONSE

1. The Vendor is responsible for developing, implementing, maintaining and communicating a security incident reporting process and related procedures to include, without limitation, all security and privacy related incidents involving a 'breach of security' to Personal Data.

H. SECURING DATA IN TRANSIT AND AT REST

1. Encryption use standards are established to protect sensitive information (including Personal Data) when being transmitted and/or stored on Vendor information resources. Where applicable, Primary Account Number (PAN) must be encrypted both at rest and in transit.

2. Connections to wireless access points must be authenticated over an industry best practice, strong encrypted channel.

3. Sensitive information, including Personal Data, such as cardholder information, must not be sent over the Internet, via Remote Access or transmitted over public or external networks unless the transition utilizes a strong encryption method or protocol as designated by NIST.

I. SERVER AND NETWORK SECURITY

This section is only applicable if Vendor is (a) storing or processing Billtrust Customer data, on its network, or (b) remotely accessing Billtrust Customer data or network access credentials in connection with the Services under the Agreement.

1. Vendor will harden its operating systems in accordance with leading information security industry standards (e.g., NIST) and adhere to the concept of "least-privileged" access.

2. Requirements are established for ensuring users only have direct access to the network services for which they have been specifically authorized to use and only authorized devices are permitted to connect to the network.

3. Vendor will have mechanisms to prevent the unauthorized removal of Billtrust Customer Data from the Vendor's networks.

4. Vendor will employ a defensive model when building networks (including firewalls) in a multi-tiered approach and use separate layers of presentation, business logic and data when considered necessary in accordance with information security best practices. Connection between networks shall be limited to those ports and services required for Vendor to support, secure, monitor and perform the Services under the Agreement.

5. Where the Services are provided using online services, the Vendor must establish and implement a firewall rule base to prohibit traffic which is not specifically permitted for valid business purposes and ensure that adequate protection is in place.

J. THIRD PARTY SERVICES

1. The Vendor must establish processes and procedures for analysis of services to be outsourced.

2. The Vendor must evaluate and perform thorough due diligence before engaging a Vendor.

3. Depending on the sensitivity and criticality of the services provided, the Vendor requests or commissions a review of the service provider's security control structure.

4. The Vendor employs safeguards to ensure that the interests of Vendors are consistent with and reflect Vendor interests.

5. A written agreement containing the appropriate terms and conditions must be executed for all third party service provider relationships.

K. APPLICATION MANAGEMENT

For all applications supported by the Vendor in connection with the Services under the Agreement., the following controls will be implemented:

1. The Vendor requires the integration of security requirements in system design that are consistent and supportive of the Vendor security architecture.

2. Suitable measures are in place to prevent the disclosure of (i) application configuration information that could be exploited; and (ii) Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof.

3. The Vendor implements processes and procedures for testing of security features and controls as part of application testing.

4. Significant modifications, major enhancements, and new systems must be integration tested prior to deployment in production environments.

L. ENTERPRISE RESILIENCE (BUSINESS CONTINUITY)

This section is only applicable if Vendor is (a) storing or processing Billtrust Customer Data on its network, or (b) providing Billtrust with a Service or Software that Billtrust relies upon to deliver services to its Customers.

1. Vendor will establish and maintain disaster recovery and business continuity plans, including offsite data storage and recovery infrastructure, designed to minimize the risks associated with a disaster affecting Vendor’s ability to provide the Services.

2. Vendor will maintain adequate backup procedures in order to recover data it processes in connection with the Services; test its disaster recovery and business continuity plans, not less frequently than annually, and will provide to Billtrust its annual disaster recovery and business continuity plans test results upon request.

M. COMPLIANCE

1. The Vendor must establish processes and procedures for documentation of legal and compliance obligations including privacy and data protection.

3. Personal Data must only be obtained by Vendor for specified and lawful purposes and must not be further processed or disclosed if prohibited by law.

4. The Vendor must have procedures for the data subjects to exercise their rights relating to their Personal Information held by Vendor, although with respect to this Agreement, Billtrust or the Billtrust Customer has primary responsibility for responding to data subjects.

5. When outsourcing to a third party, the protection of Personal Data is considered.

6. The Vendor conducts independent and/or self-administered audits, assessments and penetration tests on an annual basis, or as otherwise necessary (i.e. segmentation controls, significant infrastructure or application upgrade or modification).

Exhibit C: List of Sub-Processors

Below is a list of the Sub-Processors of Vendor as at the Effective Date of the Addendum:

Sub-Processor (full legal entity name)	Processing Activities	Categories of Billtrust Personal Data	Location (country)
Auth0	Spreedly direct customer portal login		USA
AWS	Cloud data processing		USA
FiveTran	SaaS data integration service		USA
FIS/Global/Vantiv	Account updater service		UK
Looker	Business intelligence and visualization for analytics		USA
Slack	Private customer communication		USA
Snowflake	Data warehousing		USA
Zendesk	Inbound customer support and help center/community		USA

Exhibit D: Jurisdiction-Specific Terms

1. **Transfers of EEA Personal Data**

14.9 Definitions:

For the purpose of interpreting the current Section 1 (Transfers of EEA Personal Data) of **Exhibit D**, the following terms shall have the meanings set out below:

(a) "**EEA**" means the European Economic Area.

(b) "**EEA Restricted Transfer**" includes any transfer of Personal Data subject to the GDPR (including data storage on foreign servers) which is undergoing Processing or is intended for Processing after transfer, to a Third Country (as defined below) or to an international organization.

(c) "**Supervisory Authority**" in the context of the GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR.

(d) "**Third Country**" (as used in this Section) means a country or territory outside of the EEA.

14.10 Transfer Mechanisms:

With regard to any EEA Restricted Transfer from Billtrust to Vendor within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) a valid adequacy decision pursuant to the requirements under the GDPR that provides that the third country, a territory or one or more specified sectors within that third country, or the international organization in question to which Personal Data is to be transferred ensures an adequate level of data protection;

(b) Certification to any successor to the Privacy Shield Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the GDPR, as the case may be), provided that the Services are covered by the self-certification, if applicable;

(c) the Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under the GDPR, as the case may be); or

(d) any other lawful basis, as laid down in the GDPR, as the case may be.

14.11 Standard Contractual Clauses:

(a) To the extent that Billtrust acts as Controller and Vendor acts as Controller, Vendor (which will take on the obligations of "data importer" for the purposes of the Standard Contractual Clauses) and Billtrust (which will take on the obligations of "data exporter" for the purposes of the Standard Contractual Clauses) hereby enter into the Standard Contractual Clauses, which are incorporated by this reference and constitute part of this Addendum (and where Annexes 1 and 2 of the Standard Contractual Clauses would reflect the information as contained **Exhibit A** to this Addendum) as follows:

(i) Module One of the Standard Contractual Clauses will apply;

(ii) in Clause 7, the optional docking Clause will not apply;

(iii) Clause 9, shall be deemed inapplicable;

(iv) Clause 13, all square brackets removed, and all text therein is retained;

(v) Clause 17, the parties agree that the SCCs will be governed by the laws indicated under Section 14.8 of the Addendum;

(vi) in Clause 18(b), disputes shall be resolved before the competent courts pursuant to Section 14.8 of the Addendum;

(vii) the certification of deletion of Personal Data described in Clause 8.5 of the SCCs shall be provided by the data importer to the data exporter only upon data exporter's written request.

(viii) the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 11 of this Addendum.

(b) To the extent that Billtrust acts as Controller and Vendor acts as Processor, Vendor (which will take on the obligations of "data importer" for the purposes of the Standard Contractual Clauses) and Billtrust (which will take on the obligations of "data exporter" for the purposes of the Standard Contractual Clauses) hereby enter into the Standard Contractual Clauses, which are incorporated by this reference and constitute part of this Addendum (and where Annexes 1 and 2 of the Standard Contractual Clauses would reflect the information as contained **Exhibit A** to this Addendum) as follows:

(i) **Module Two** of the Standard Contractual Clauses will apply;

(ii) in Clause 7, the optional docking Clause will not apply;

(iii) in Clause 9, Option 1 Specific Prior Authorisation applies;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws indicated under Section 14.8 of the Addendum;

(vi) in Clause 18(b), disputes shall be resolved before the competent courts pursuant to Section 14.8 of the Addendum;

(vii) the certification of deletion of Personal Data described in Clause 8.5 of the SCCs shall be provided by the data importer to the data exporter only upon data exporter's written request.

(viii) the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 11 of this Addendum.

(ix) in Annex I:

(A) Part A: with the information set out in the Exhibit A to this Addendum;

(B) Part B: with the relevant Processing Annex(ures) set out in Exhibit A to this Addendum; and

(C) Part C: in accordance with the criteria set out in Clause 13(a) of the EU SCC's;

(x) Annex II: with the Minimum Security Measures of Exhibit B.

(c) To the extent that Billtrust acts as Processor and Vendor acts as Sub-Processor, Vendor (which will take on the obligations of "data importer" for the purposes of the Standard Contractual Clauses) and Billtrust (which will take on the obligations of "data exporter" for the purposes of the Standard Contractual Clauses) hereby enter into the Standard Contractual Clauses, which are incorporated by this reference and constitute part of this Addendum (and where Annexes 1 and 2 of the Standard Contractual Clauses would reflect the information as contained **Exhibit A** to this Addendum) as follows:

(i) **Module Three** will apply;

(ii) in Clause 7, the optional docking Clause will not apply;

(iii) in Clause 9, Option 1 Specific Authorisation applies;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 13, all square brackets removed, and all text therein is retained;

(vi) in Clause 17, Option 1 will apply, and the SCC's will be governed by the laws indicated under Section 14.8 of the Addendum;

(vii) in Clause 18(b), disputes shall be resolved before the competent courts pursuant to Section 14.8 of the Addendum;

(viii) the certification of deletion of Personal Data described in Clause 8.5 of the SCCs shall be provided by the data importer to the data exporter only upon data exporter's written request.

(ix) the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 11 of this Addendum.

(x) in Annex I:

(A) Part A: with the information set out in Exhibit A to this Addendum;

(B) Part B: with the relevant Processing Annex(ures) set out in Exhibit A to this Addendum; and

(C) Part C: in accordance with the criteria set out in Clause 13(a) of the EU Standard Contractual Clauses;

(xi) Annex II: with the Minimum Security Measures of Exhibit B

(d) The Parties are deemed to have signed, accepted, and executed the Standard Contractual Clauses in their entirety, including the appendices as of the Effective Date. The text contained in **Exhibit E** to this Addendum serves to supplement the Standard Contractual Clauses.

(e) In cases where the Standard Contractual Clauses apply, and there is a conflict between the terms of the Addendum, the Supplemental Clauses to the Standard Contractual Clauses contained in Exhibit E and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.

15. California

15.1 Definitions:

For the purpose of interpreting the current Section 2 (California) of Exhibit D, the following terms shall have the meanings set out below:

(a) "**Applicable Data Protection Laws**" includes the CA Privacy Laws (as defined below) as may be amended from time to time.

(b) "**CA Privacy Laws**" means, collectively, the California Consumer Privacy Act of 2018 (CCPA, codified at Civil Code section 1798.100 et seq.), the California Privacy Rights Act (CPRA), and all applicable regulations issued by the California Attorney General and/or the California Privacy Protection Agency implementing CCPA and CPRA.

(c) The terms "**Business Purpose**", "**Commercial Purpose**", "**Sale**", "**Sell**", along with their cognates whether capitalized or not, shall have the same meaning as in the CA Privacy Laws, and their related terms shall be construed accordingly.

For the purpose of interpreting the current Section 2 (California) of Exhibit D, the following terms shall be interpreted as follows:

(a) "**Contractor**" has the meaning given to it in Section 1798.140(j) of the California Civil Code.

(b) "**Personal Data Breach**" includes "Breach of the Security of the System" as defined in Section 1798.8 of the California Civil Code;

(c) "**Personal Data**" includes "Personal Information" as defined in Section 1798.140(o) of the California Civil Code.

(d) "**Service Provider**" in Section 1798.140(ag) of the California Civil Code.

Where Vendor acts as a Service Provider or Contractor on behalf of Billtrust in accordance with Section 3 of the Addendum:

(a) Billtrust discloses Personal Data to Vendor solely for: (i) valid Business Purposes; and (ii) to enable Vendor to perform the Processor Services under the Agreement(s).

(b) Vendor shall not:

(i) sell or share Personal Data it collects from Billtrust pursuant to the Agreement(s);

(ii) retain, use or disclose Personal Data it collects from Billtrust pursuant to the Agreement(s) for any purpose other than providing the Processor Services specified in the Agreement(s) or as otherwise permitted by the CA Privacy Laws;

(iii) retain, use or disclose Personal Data it collects from Billtrust pursuant to the Agreement(s) for any commercial purpose other than the business purpose(s) specified in the Agreements (or in any applicable statement of work or similar document), unless expressly permitted by the CA Privacy Laws;

(iv) retain, use or disclose Personal Data it collects from Billtrust pursuant to the Agreement(s) outside the direct business relationship between it and Billtrust unless expressly permitted by the CA Privacy Laws. For example, Vendor may not combine or update Personal Data collected pursuant to the Agreement(s) with personal information that it received from another source or collected from its own interaction with a consumer, unless expressly permitted by the CA Privacy Laws.

(c) Vendor shall comply with all applicable sections of the CA Privacy Laws, including with respect to the Personal Data collected pursuant to the Agreement(s), providing the same level of privacy protection as required of Billtrust by the CA Privacy Laws.

(d) Vendor grants Billtrust the right to take reasonable and appropriate steps to ensure that it uses the Personal Data collected pursuant to the Agreement(s) in a manner consistent with Billtrust's obligations under the CA Privacy Laws.

(e) Vendor shall notify Billtrust after it makes a determination that it can no longer meet its obligations under the CA Privacy Laws.

(f) Vendor grants Billtrust the right, upon notice, to take reasonable and appropriate steps to stop and remediate its unauthorized use of Personal Data.

(g) Vendor shall enable Billtrust to comply with consumer requests made pursuant to CA Privacy Laws or Billtrust shall inform Vendor of any consumer request made pursuant to the CA Privacy Laws that it must comply with and provide the information necessary for Vendor to comply with the request.

(h) To the extent Vendor subcontracts with another person in providing services to Billtrust, Vendor shall have a contract with the subcontractor that complies with the CA Privacy Laws.

(i) Vendor certifies that it understands these restrictions and will comply with them.

16. Canada

16.1 Definitions:

For the purpose of interpreting the current Section 3 (Canada) of Exhibit D, the following terms shall have the meanings set out below:

(a) "**Applicable Data Protection Laws**" includes PIPEDA (as defined below).

(b) "**Personal Data**" includes "**Personal Information**" as defined under PIPEDA (as defined below).

(c) "**Personal Data Breach**" includes "**Breach of Security Safeguards**" as defined under PIPEDA (as defined below).

(d) "**PIPEDA**" means the Federal Personal Information Protection and Electronic Documents Act.

(e) "Sub-Processor" and "Sub-processor" include "Third Party Organization" as defined under PIPEDA.

16.2 **Necessary Consent.** When acting as Controller, Billtrust confirms that is has obtained a valid consent (as defined under PIPEDA), where necessary to Process Personal Data of each Data Subject.

17. Switzerland

17.1 Definitions:

For the purpose of interpreting the current Section 4 (Switzerland) of Exhibit D, the following terms shall have the meanings set out below:

(a) "**Applicable Data Protection Laws**" includes the FADP (as defined below) and the OFADP (as defined below), as may be amended from time to time.

(b) "**Controller"** includes "Controller of the Data File" as defined under the FADP (as defined below).

(c) "**Data Subject**" includes the natural persons whose Personal Data is Processed.

(d) "**FADP**" means the Swiss Federal Act on Data Protection of 19 June 1992.

(e) "**OFADP**" means the Ordinance to the Federal Act on Data Protection ("OFADP")

(f) "**Personal Data**" includes "**Personal Data**" as defined under the FADP.

(g) "**Processing**" includes "**Processing**" as defined under the FADP.

(h) "**Swiss Restricted Transfer**" includes any transfer of Personal Data (including data storage in foreign servers) subject to the FADP to a Third Country (as defined below) or an international organization.

17.2 **Swiss Restricted Transfers.** With regard to any Swiss Restricted Transfer from Billtrust to Vendor within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) the inclusion of the Third Country, a territory or one or more specified sectors within that Third Country, or the international organization in question to which Personal Data is to be transferred in the list published by the Swiss Federal Data Protection and Information Commissioner of States that provide an adequate level of protection for Personal Data within the meaning of the FADP;

(b) Vendor's certification to any successor to the Privacy Shield Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the FADP and the OFADP, as the case may be), provided that the Services are covered by the self-certification, if applicable;

(c) the Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under the FADP and the OFADP, as the case may be); or

(d) any other lawful basis, as laid down in FADP and the OFADP, as the case may be.

17.3 Standard Contractual Clauses:

(a) Billtrust (which will take on the obligations of "data exporter" for the purposes of the Standard Contractual Clauses) and Vendor (which will take on the obligations of "data importer" for the purposes of the Standard Contractual Clauses) hereby enter into, the Standard Contractual Clauses (including their additional constituent elements, as set out in **Exhibit A** to this Addendum, as applicable), which are incorporated by this reference and constitute an integral part of this Addendum. The Parties are deemed to have signed, accepted, and executed the Standard Contractual Clauses in their entirety, including the appendices as of the Effective Date. The text contained in **Exhibit E** to this Addendum serves to supplement the Standard Contractual Clauses.

(b) In cases where the Standard Contractual Clauses apply, and there is a conflict between the terms of the Addendum and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.

(c) Where the Standard Contractual Clauses apply, Billtrust shall inform the Federal Data Protection and Information Commissioner about the use of the Standard Contractual Clauses before transferring the data outside the Swiss Confederation, when possible.

(d) The FDPIC shall act as the "competent supervisory authority" insofar as the relevant data transfer is governed by the FADP.

(e) The term "EU Member State" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with the SCCs.

(f) The SCCs also protect the data of legal entities until the entry into force of the revised version of the FADP of 25 September 2020, which is scheduled to come into force in 2023.

18. United Kingdom

18.1 Definitions:

For the purpose of interpreting the current Section 4 (United Kingdom) of Exhibit D, the following terms shall have the meanings set out below:

(a) "**Applicable Data Protection Laws**" includes the Data Protection Act 2018 and, when in full force and effect, the UK GDPR (as defined below).

(b) **"UK"** means the United Kingdom of Great Britain and Northern Ireland;

(c) **"UK GDPR"** means the GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019).

(d) **"UK Transfer Addendum"** means the template Addendum B.1.0 issued by the UK Information Commissioner's Office (ICO) and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the Mandatory Clauses included in Part 2 thereof (the "Mandatory Clauses").

(e) "**UK Restricted Transfer**" includes any transfer of Personal Data (including data storage in foreign servers) subject to the UK GDPR to a third country outside of the UK or an international organization.

18.2 UK Restricted Transfers:

With regard to any UK Restricted Transfer from Billtrust to Vendor within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) a valid adequacy decision pursuant to the requirements under the UK GDPR and the Data Protection Act 2018 that provides that the third country, a territory or one or more specified sectors within that third country, or the international organization in question to which Personal Data is to be transferred ensures an adequate level of data protection;

(b) Vendor's self-certifications to the E.U.-U.S. Privacy Shield Framework or any successor to the Privacy Shield Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the UK GDPR and the Data Protection Act 2018, as the case may be), provided that the Services are covered by the self-certification, if applicable;

(c) the Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under the UK GDPR and the Data Protection Act 2018) as varied by the UK Transfer Addendum in the manner described below in section 5.3 (d); or

(d) any other lawful basis, as laid down in the UK GDPR and the Data Protection Act 2018, as the case may be.

18.3 Standard Contractual Clauses:

(a) Billtrust (which will take on the obligations of “data exporter” for the purposes of the Standard Contractual Clauses) and Vendor (which will take on the obligations of “data importer” for the purposes of the Standard Contractual Clauses) hereby enter into, the Standard Contractual Clauses (including their additional constituent elements, as set out in **Exhibit A** to this Addendum, as applicable), which are incorporated by this reference and constitute an integral part of this Addendum.

(b) The Parties are deemed to have signed, accepted, and executed the Standard Contractual Clauses in their entirety, including the appendices as of the Effective Date. The text contained in **Exhibit E** to this Addendum serves to supplement the Standard Contractual Clauses.

(c) In cases where the Standard Contractual Clauses apply, and there is a conflict between the terms of the Addendum and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.

(d) PART 1 OF THE UK TRANSFER ADDENDUM. As permitted by Section 17 of the UK Transfer Addendum, the parties agree that:

(i) Tables 1, 2 and 3 of Part 1 of the UK Transfer Addendum are deemed completed with the corresponding details set out in **Exhibit A** to this Addendum and the foregoing provisions of Exhibit D, section 1.3 (subject to the variations effected by the Mandatory Clauses described in (b) below); and

(ii) Table 4 of Part 1 of the UK Transfer Addendum is completed by the box labelled ‘Data Exporter’ being deemed to have been ticked.

(e) PART 2 OF THE UK TRANSFER ADDENDUM. The Parties agree (i) to be bound by the Mandatory Clauses of the UK Transfer Addendum and (ii) In relation to any UK Restricted Transfer to which the UK Transfer Addendum applies, where the context permits and requires, any reference in this Addendum to the SCCs shall be read as a reference to those SCCs as varied in the manner set out in this section 5.3.

EXHIBIT E: Supplemental Clauses to the Standard Contractual Clauses

By this **Exhibit E** (this "Exhibit"), the Parties provide additional safeguards to and additional redress to the Data Subjects to whom transferred Personal Data pursuant to Standard Contractual Clauses. This Exhibit supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses that may be applicable to the Restricted Transfer.

1. Applicability of this Exhibit

18.4 This Exhibit only applies with respect to Restricted Transfers when the Parties have concluded the Standard Contractual Clauses pursuant to the Addendum and its Exhibits.

19. Definitions

19.1 For the purpose of interpreting this Section, the following terms shall have the meanings set out below:

(a) "**Data Importer**" and "**Data Exporter**" shall have the same meaning assigned to them in the Standard Contractual Clauses concluded by the Parties.

(b) "**FISA**" means the U.S. Foreign Intelligence Surveillance Act.

(c) "**Schrems II Judgment**" means the judgment of the European Court of Justice in Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems.

20. Back doors

20.1 Data Importer certifies that:

(a) it has not purposefully created back doors or similar programming that could be used to access Data Importer's Systems or Personal Data subject to the Standard Contractual Clauses;

(b) it has not purposefully created or changed its business processes in a manner that facilitates access to Personal Data or systems, and

(c) that national law or government policy does not require Data Importer to create or maintain back doors or to facilitate access to Personal Data or systems.

20.2 Data Exporter will be entitled to terminate the contract on short notice in those cases in which Data Importer does not reveal the existence of a back door or similar programming or manipulated business processes or any requirement to implement any of these or fails to promptly inform Data Exporter once their existence comes to its knowledge.

20.3 In circumstances where the Data Importer disclosed Personal Data transferred in violation of the commitments contained in provision 3.1 above, Data Importer shall compensate Data Subjects for any material and non-material damage suffered as a result of such violation.

21. **Other Measures to Prevent Authorities from Accessing Personal Data**

21.1 Notwithstanding the application of the Minimum Security Measures set forth in the Addendum **Exhibit B**, Data Importer will implement:

(a) Internal policies or procedures establishing that:

(i) where Data Importer is prohibited by law from notifying the Data Exporter of an order from a public authority for transferred Personal Data, the Data Importer shall take into account the laws of other jurisdictions and use best efforts to request that any confidentiality requirements be waived to enable it to notify the competent Supervisory Authorities;

(ii) the Data Importer's legal team shall scrutinize requests for legal validity and, as part of that procedure, will reject any request Data Importer considers to be invalid;

(iii) if Data Importer is legally required to comply with an order, it will respond as narrowly as possible to the specific request; and

(iv) Data Importer shall monitor any legal or policy developments (such as changes in the legislation or practice in the countries where the data is transferred) which might lead to its inability to comply with its obligations under the SCCs. In particular, Data Importer shall make reasonable efforts to inform Billtrust of legal or policy developments ahead of their implementation to enable Billtrust to recover the Personal Data from the Data Importer (either by returning the data to Billtrust or by deleting or securely encrypting the data).

22. **Termination**

22.1 This Exhibit shall automatically terminate if the European Commission, a competent Member State Supervisory Authority, or an EEA or competent Member State court approves a different lawful transfer mechanism that would be applicable to the data transfers covered by the Standard Contractual Clauses (and if such mechanism applies only to some of the data transfers, this Addendum will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Addendum.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

[SIGNATURE PAGE TO THE BILLTRUST DATA PROCESSING ADDENDUM FOLLOWS]

Each Party is signing this Addendum on the date stated below that Party's signature.

Factor Systems, LLC dba Billtrust	**Spreedly, Inc. (Vendor)**
DocuSigned by: Andrew Herning 51AF8FB38ADD405...	DocuSigned by: Justin Benson C9132818B2F844A...
Signature	**Signature**
Andrew Herning	Justin Benson
Name	**Name**
Senior VP, Finance	CEO
Title	**Title**
2/15/2023	2/15/2023
Date	**Date**