



ORDER FORM #1

Spreedly, Inc.

300 Morris Street
Suite 400
Durham, NC 27701

To: DQ Accounts Payable

Customer Legal Name: American Dairy Queen Corporation

Tax ID: 41-0853275

Offer Valid Until: 16 February 2022

Billing Address:

8331 Norman Center Drive
Suite 700
Bloomington, MN 55437

Sales Rep: Lauren Wilson

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, or, in the absence of an ESA, the Spreedly Terms of Service located at <https://www.spreedly.com/terms-of-service>.

In the event of any conflict between the terms of the Agreement and this Order Form, this Order Form shall 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

The Initial Term of this Order Form is 12 months. Thereafter, this Order Form shall automatically renew for successive one-year periods (each, a "**Renewal Term**" and, together with the Initial Term, the "**Term**") unless either party has provided written notice of its intent to not renew this Agreement not less than sixty (60) days prior to the expiration of the then-current Initial or Renewal Term.

2) Annual Platform Fees:

Annual platform fees and API usage fees will be billed to the Customer in accordance with Table 1.

- Customer will start the Initial Term at the Tier 1 level platform.
- Customer may elect to upgrade to a higher platform tier at any time during the Term by executing a new Order Form subject to this Agreement.
- Upon upgrading to a higher tier, Customer will be billed a prorated Annual Platform Fee corresponding to the number of days left until the next anniversary of the Order Form Effective Date, and Customer will immediately be advanced to the API call rate corresponding with the new platform fee, in accordance with Table 1.
- Customer must provide 30 days written notice to Spreedly to upgrade tiers. Customer may not move down to a lower tier except at the start of a Renewal Term.

Table 1: Approved Enterprise Pricing for Dairy Queen		
	Annual Platform Fee	Cost per API call
Tier 1	\$75,000	\$0.0050
Tier 2	\$150,000	\$0.0025
Tier 3	\$225,000	\$0.0010

3) API Usage Fees:

In addition to the annual Enterprise Platform Fee, Spreadly will bill Customer monthly in arrears at the then current Cost per API call rate in accordance with Table 1 for the term of the contract. Customer will pay within thirty (30) days following receipt of invoice by any of the methods accepted by both parties.

- Customer will start the Initial Term at the Tier 1 level and be billed \$0.0050 per API call.

4) Account Updater Service Fees:

Customer may elect to participate in Spreadly's Account Updater program at a cost of \$0.18 per successfully updated card when making a minimum bulk purchase of \$18,000, equivalent to 100,000 successful updates. Customer shall prepay a minimum of \$18,000 for use of the service (equivalent to 100,000 successful updates), and that fee shall be debited each time the account updater service is performed and fees are accrued. Customer shall be invoiced an additional \$18,000 only when the remaining balance falls below \$1,800.

Customer may elect to pre-purchase more than \$18,000 updates at the same rate. Bulk purchases of updates will be made by executing a new Order Form subject to the terms of this Agreement. Credit for pre-purchased updates will not expire as long as the Agreement remains in force between the Parties.

If Customer elects not to pre-purchase Account Updater updates at the minimum bulk purchase rate of \$18,000, Customer will be billed monthly in arrears at a cost of \$0.20 per successfully updated card.

5) Fee increases:

The Annual Platform Fee and all API usage fees will increase by 6% annually in each successive Renewal Term. For example, in the first Renewal Term following the Initial Term, the Tier 1 Annual Platform Fee will increase to \$159,000 and the cost per API call will increase to \$0.00265 per API call.

6) Payments:

All payments are subject to the terms prescribed in Section 7 of the Agreement. Customer will pay the Annual Platform Fee for the first year of the Initial Term in full within 15 days of the Order Form Effective Date. Each subsequent annual payment shall be invoiced 30 days prior to the anniversary of the Effective Date ("**Annual Renewal Date**") and shall be due and payable prior to the Annual Renewal Date.

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

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

Receiver: Silicon Valley Bank
 ABA/Routing #: 121140399
 SWIFT Code: SVBKUS6S
 Beneficiary: 3301451580
 Spreadly, Inc.
 300 Morris Street, Suite 400
 Durham, NC 27701
 USA

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


By signing below, Customer indicates its acceptance of the terms of the Agreement and represents and warrants 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 the Agreement; (iii) the execution of this Order Form by its representative has been duly authorized by all necessary corporate or organizational action of Customer; and (iv) when executed and delivered by both Parties, the Agreement will constitute the legal, valid and binding obligation of Customer, enforceable against Customer in accordance with its terms.

[SIGNATURES ON FOLLOWING 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.

DocuSigned by:

By: 
Name: Justin Benson
Title: CEO

American Dairy Queen Corporation

DocuSigned by:

By: 
Name: Kevin Baartman
Title: EVP of Information Technology

Notice Address:

Spreedly, Inc.
300 Morris Street, Suite 400
Durham, NC 27701
Attn: Accounts Receivable
E-mail: ar@spreedly.com

Notice Address:

American Dairy Queen Corporation
8331 Norman Center Drive, Suite 700
Bloomington, MN 55437
Attn: DQ Accounts Payable
E-mail: Marketing.Invoices@idq.com



ENTERPRISE SERVICE AGREEMENT

This Enterprise Services Agreement ("**Agreement**") is entered by and between Spreadly, Inc., a Delaware corporation, ("**Spreadly**") and American Dairy Queen Corporation, a Delaware Corporation, ("**Customer**"). Spreadly 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		CUSTOMER	
Name:	Spreadly, Inc.	Name:	American Dairy Queen Corporation
Address:	300 Morris Street, Suite 400	Address:	8331 Norman Center Drive, Suite 700
City/State:	Durham, NC 27701	City/Country:	Bloomington, MN 55437
PRIMARY SPREEDLY CONTACT		PRIMARY CUSTOMER CONTACT	
Name:	Lauren Wilson	Name:	Dan Amundsen
Title:	Enterprise Account Executive	Title:	IT Program Manager
Phone:	315-447-8366	Phone:	952-830-0222
Email:	lwilson@spreadly.com	Email:	dan.amundsen@idq.com
SPREEDLY FINANCE CONTACT		CUSTOMER BILLING CONTACT	
Name:	Spreadly Accounting Department	Name:	Crissy McCluney
Phone:	888-727-7750	Phone:	952-830-0353
Email:	accounting@spreadly.com	Email:	Marketing.Invoices@idq.com

Background

Spreadly develops, markets and provides to its customers a web-based payments orchestration and tokenization platform, which includes Spreadly's proprietary API integration (collectively, the "**Platform**"), which enables its customers to validate, tokenize and vault credit cards (and other payment types) and then process charges against one or more of the payment gateways that are integrated to the Platform and/or third-party payment method receivers that Spreadly supports, and, where applicable, automatically update expired or lost credit cards (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, the SLA 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 Spreadly 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 make available to Customer at: <https://docs.spreedly.com/>, which describe the functionality, components, features or requirements of the Platform, as Spreedly may update from time-to-time in Spreedly’s discretion.

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

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

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

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

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

1.12. “Order Form” means each order form 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.

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. “Spreedly Agents” means Spreedly’s and Spreedly’s affiliates’ employees, consultants, subcontractors, agents and representatives that are performing services on behalf of Spreedly under this Agreement.

1.16. “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 our Service. If Customer purchases the Account Updater program in connection with any Order Form submitted hereunder, Customer’s use thereof will be subject to the supplemental Account Updater terms and conditions described in the Order Form.

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 or otherwise make available the Platform or any features or functionality of the Platform to any other person or entity for any reason, including as part of any time-sharing, service bureau or software as a service arrangement;
- 2.3.3. reverse engineer, disassemble, decompile, decode, adapt or otherwise attempt to derive, gain access to or discover the source code of the Platform or the underlying structure, ideas, know-how, algorithms or methodology relevant to the Platform;
- 2.3.4. input, upload, transmit or otherwise provide to or through the Platform any information or materials that are unlawful or injurious, or contain, transmit or activate any Malicious Code;
- 2.3.5. attempt to gain unauthorized access to, damage, destroy, disrupt, disable, impair, interfere with or otherwise impede or harm in any manner the Platform;
- 2.3.6. access or use the Platform in any way that 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 Spreadly's competitors, for any purpose, otherwise non-public information about the Platform.

2.4. Changes to the Platform. Spreadly 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 Spreadly deems necessary or useful to improve the Platform or for any other reason, from time-to-time in Spreadly's sole discretion, and without notice to Customer; provided, however, that Spreadly 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. Spreadly may, in Spreadly's discretion, engage subcontractors to aid Spreadly in providing the Platform and performing Spreadly's obligations under this Agreement, but Spreadly will remain liable to Customer for any act or omission by such subcontractors that would be a breach or violation of this Agreement. Spreadly 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. Spreadly will provide Customer with thirty (30) days advance notice of any changes of the hosting provider. Customer hereby specifically approves and consents to Spreadly'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. Spreadly will remain liable to Customer for any act or omission of any Reputable Hosting Services Provider.

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

2.8. Customer Data Export; Customer Data Retention. Customer may elect at any time to perform an automatic export of any Card Data and/or other Customer Data to a third-party endpoint for which Spreedly supports third-party vaulting as set forth at: <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's 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 SLA.

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 Policy described at in Schedule A (as amended from time-to-time, the "Support Services Terms").

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 Service Level Agreement described in Schedule B (as amended from time-to-time, the "SLA"). THE REMEDIES SPECIFIED IN THE SLA ARE CUSTOMER'S EXCLUSIVE REMEDIES, AND SPREEDLY'S SOLE OBLIGATION AND LIABILITY TO CUSTOMER, FOR ANY FAILURE TO MEET THE SLA REQUIREMENTS.

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 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’s being disclosed or made available to the Receiving Party in connection with this Agreement; (ii) was or becomes generally known by the public other than by the Receiving Party’s 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, or the level of care required by any Law; 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. Notwithstanding the foregoing, Customer will not be liable for sharing Confidential Information with third parties who, at the time of disclosure and as informed by Spredly, have a separate written agreement including confidentiality and non-disclosure restrictions of Spredly's 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, Spredly will implement safeguards to ensure Customer Data against destruction, loss, alteration, unauthorized access by or disclosure to third parties while in the possession or under the control of Spredly and Spredly Agents in accordance with Spredly's Data Security Policy described in Schedule C, as amended from time-to-time (the "Data Security Policy"). Such precautions will (i) ensure the security, integrity and confidentiality of Customer Data, (ii) protect against any anticipated threats or hazards to the security or integrity of Customer Data, (iii) protect against unauthorized access to or use of Customer Data that could result in substantial harm to Customer, and (iv) ensure the proper disposal of Customer Data.

6.2. Data Privacy. In the event that the Parties enter into an Order Form and/or SOW whereby Spredly 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"), Spredly 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. Spredly 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. Spredly will limit dissemination of Personal Information to its employees and subcontractors who (i) need to know the information to enable Spredly 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 Spredly 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 regard 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 provided to Spredly, if and to the extent Data Privacy Laws require additional clauses to be executed by Spredly beyond those set forth in this Agreement, then Customer shall notify Spredly in writing of such requirement and Customer and Spredly will in good faith negotiate 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. With regard to the processing of Customer Data governed by the European General Data Protection Regulation the Data Processing Addendum attached hereto as Schedule D will apply.

6.3. CCPA Service Provider Compliance. Spredly and Customer both agree that Customer is a business and Spredly is a service provider under CCPA. Spredly 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 Spreadly; and (iii) not sell the personal information to any third parties. Spreadly 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 Spreadly with respect to exercising its privacy rights under CCPA, Spreadly 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 Spreadly 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, and provided Spreadly is fully liable for the subcontractor's actions and omissions as if they were Spreadly's own; (y) Spreadly's internal use to build or improve the quality of its Platform or services for a use compatible with the context in which the personal information was collected, provided that the use does not include building or modifying household or consumer profiles for use in providing services to another business, or correcting or augmenting data acquired from another source; (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 Spreadly, 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" shall have the meanings given to such terms in CCPA.

7. Fees and Payment.

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

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

7.3. Payment. Customer will make all payments in US dollars. Unless otherwise set forth in an applicable Order Form or Statement of Work, all invoiced amounts are due net thirty (30) days from the invoice date. Customer is responsible for providing complete and accurate billing and contact information and notifying Spreadly of any changes to that information.

7.4. Late Payment. If Customer fails to make any payment when due then, in addition to all other remedies that may be available to Spreadly (including Spreadly's rights under Section 2.7 and Section 9.3), Spreadly may charge interest on the past due amount at the rate of 1.5% per month calculated daily and compounded monthly or, if lower, the highest rate permitted under applicable law.

8. Ownership and Intellectual Property Rights.

8.1. Platform and Documentation. Customer acknowledges and agrees that Spreadly 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. Spreadly 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). Spreadly reserves all rights not expressly granted to Customer in this Agreement.

8.2. Customer Data. As between Customer and Spreadly, 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 Spreadly in this Section 8. During the Term, Customer hereby grants to Spreadly and its subcontractors all such rights and permissions in or relating to Customer Data as are necessary to: (i) provide the Platform to Customer; and (ii) enforce this Agreement and exercise Spreadly's rights and perform Spreadly's obligations under this Agreement.

8.3. Improvements. During the Term, Customer hereby grants to Spreadly all such rights and permissions in or relating to Customer Data that are necessary for Spreadly to process Customer Data internally for the purpose of improving the quality of the Platform. To the extent Spreadly makes any improvements to the Platform ("Improvements") based upon the Platform's processing of Customer Data, Customer agrees that Spreadly exclusively owns all right, title and interest in and to the Improvements, including all related Intellectual Property Rights.

8.4. Usage Data. Customer acknowledges and agrees that Spreadly 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 Spreadly may use Usage Data in connection with providing Support Services to Customer and for Spreadly's internal business purposes (such as monitoring, enhancing and improving the Platform), and that Spreadly 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, with the prior written approval of Customer, Customer may allow include Customer's name, trademarks and logos on Spreadly's website and in other sales and marketing materials in order to factually identify Customer as a current customer.

9. Term and Termination.

9.1. Term. Unless otherwise terminated in accordance with this Agreement, the initial term of this Agreement will be for the duration specified in the Initial Order Form (the "Initial Term"). Thereafter, this Agreement 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; and (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) Spreadly will immediately discontinue Customer's access to the Platform; (ii) Customer will complete all pending transactions and stop accepting new transactions through the Platform; (iii) Customer will discontinue use of any Spreadly trademarks and immediately remove any Spreadly references and logos from Customer's 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. Surviving Terms. Sections 1 (Definitions), 5 (Confidentiality), 6 (Data Protection), 7 (Fees and Payment), 8 (Ownership and Intellectual Property Rights), 9.3 (Effect of Termination), 10.c (Disclaimer of Warranties), 11 (Indemnification), 13 (Limitations of Liability), 14 (Miscellaneous) and this Section 9.4 will survive any expiration or termination of this Agreement.

10. Representations and Warranties.

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



10.2. Customer Representations. Customer represents and warrants that: (i) it will not use the Platform, directly or indirectly, for any fraudulent undertaking or in any manner so as to interfere with the use of the Platform; (ii) Customer's use of the Platform and its collection and use of all of Customer Data (including Customer's processing of Customer Data and/or any card authorization, credit, ticket only, capture or settlement request, decline transaction, or other related transaction, completed or submitted under Customer's account) will comply with (A) all applicable Laws, (B) the terms of service of the payment gateways, merchant service providers and/or API endpoints Customer connects with on the Platform; (C) the operating rules, bylaws, schedules, supplements and addenda, manuals, instructions, releases, specifications and other requirements, as may be amended from time-to-time, of any of the payment networks including Visa, MasterCard, American Express, Discover Financial Services, and any affiliates thereof or any other payment network applicable to this Agreement; (D) PCI-DSS and PA-DSS, as applicable; and (E) any regulatory body or agency having jurisdiction over the subject matter thereof; (iii) Customer either owns, or has all rights, permissions and consents that are necessary to process, and to permit Spreedly, its subcontractors and the Platform to process as contemplated in this Agreement, all Customer Data and the credit card transaction related thereto; (iv) Spreedly's and its subcontractors' access to and use of Customer Data (including, for the avoidance of doubt, the Card Data and all personal data included with Customer Data) as contemplated by this Agreement does not and will not violate any applicable Law or infringe, misappropriate or otherwise violate any Intellectual Property Right, privacy right or other right of any third party; (iv) 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.

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.
- 10.3.5. the Platform and all Professional Services will be compliant with all Laws applicable to the provision of the services.
- 10.3.6. no programs containing malicious or detrimental hidden files, illicit code, viruses, malware or any other malicious computer program, such as containing any hardware-limiting, software-limiting or services-limiting function not part of standard configuration or containing any automatically replicating, transmitting or activating computer program that is not planned or expected by one of the Parties has been or will be coded or introduced into Customers systems, software, hardware, tools, equipment or any similar item.

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 COMPAY 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. Spredly Indemnification. Spredly will indemnify, defend and hold harmless Customer, and its directors, officers, affiliates and agents and their respective successors and assigns from all damages, losses, costs, expenses (including reasonable attorney's fees), liabilities, fines and penalties suffered or otherwise incurred by any of them arising from, or otherwise relating to: (i) an allegation that the Platform and/or any Deliverables (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" (as defined in Schedule C attached hereto); (iii) Spredly's failure to remain compliant with PCI-DSS; (iv) the failure of any of Spredly's representations or warranties in this Agreement; and (v) any violation of Law by Spredly or any Spredly Agent or their respective employees, officers, directors, agents or representatives under this Agreement.

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

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

11.4. Additional Terms for Infringement Claims.

11.4.1. Spredly 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 Spredly 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 Spredly'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, Spredly may, at Spredly's option and Spredly'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 Spredly determine the remedies in clauses (A) and (B) are not commercially reasonable, then Spredly may terminate the applicable Order Form upon written notice and without any liability to Customer and Spredly 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 SPREDLY'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, Spredly will maintain (i) commercial general liability insurance with at least \$1,000,000 per occurrence and \$2,000,000 aggregate limit (ii) "errors and omission" (tech and cyber coverage)



insurance in an amount not less than \$20,000,000. Customer will be named as an additional insured. Upon Customer's request, Spredly will provide Customer with a certificate of insurance evidencing the same. Spredly will not self-insure any of its obligations under this Agreement.

13. Limitation of Liability.

13.1. Exclusions. IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY LOST PROFITS, 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.

13.2. Direct Damages. THE TOTAL AND CUMULATIVE LIABILITY OF A PARTY ARISING UNDER OR IN CONNECTION WITH THIS AGREEMENT WILL NOT EXCEED TWO (2) TIMES THE AMOUNT OF FEES PAID TO SPREDLY BY CUSTOMER DURING THE TWELVE-MONTH PERIOD IMMEDIATELY PRECEDING SUCH CLAIM.

13.3. Exclusions. NOTWITHSTANDING THE FOREGOING, THE LIMITATIONS ON LIABILITY WILL NOT APPLY TO SPREDLY'S INDEMNIFICATION OBLIGATIONS FOR INFRINGEMENT CLAIMS UNDER SECTION 11.1(I) (EXCEPT AS LIMITED BY SECTION 11.4) AND TO THE EXTENT THE LIABILITY OF A PARTY IS A DIRECT RESULT OF THE FRAUDULENT, CRIMINAL OR GROSSLY NEGLIGENT OR MORE CULPABLE ACTS OR OMISSIONS OF THAT PARTY.

13.4. Applicability. 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. THE PARTIES AGREE THAT THE FOLLOWING LIABILITIES CONSTITUTE DIRECT DAMAGES UNDER SECTION 13.2: (i) ANY AMOUNTS ARISING FROM SPREDLY'S INDEMNIFICATION AND DEFENSE OBLIGATIONS INCLUDING ANY COSTS AND/OR EXPENSES ACTUALLY INCURRED BY CUSTOMER IN CONNECTION WITH FULFILLING LEGALLY REQUIRED OBLIGATIONS RESULTING FROM A SECURITY INCIDENT (E.G., SENDING NOTICES TO AFFECTED CUSTOMERS, REMEDIATION COSTS, AND THE COST OF PROVIDING LEGALLY REQUIRED MONITORING SERVICES TO AFFECTED END USERS); AND (ii) ANY FINES, PENALTIES, NON-COMPLIANCE FEES OR SIMILAR AMOUNTS ASSESSED OR IMPOSED BY A GOVERNMENTAL AUTHORITY OR CARD ASSOCIATION IN CONNECTION WITH A SECURITY INCIDENT AND/OR SPREDLY'S BREACH OF THE DATA SECURITY POLICY.

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 e-mail (upon confirmation of receipt); or (iv) by certified or registered mail, return receipt requested (upon verification of receipt). In each case, such notices will be addressed to a Party at such Party's address set forth in the Initial Order Form (or such other address as updated by such Party from time-to-time by giving notice to the other Party in the manner set forth in this Section 14.4).

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



14.6. No Third-Party Beneficiaries. This Agreement is for the sole benefit of the Parties hereto and their respective successors and permitted assigns and nothing herein, express or implied, is intended to or will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Agreement.

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

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

14.9. Equitable Remedies. Each Party acknowledges and agrees that a breach or threatened breach by such Party of any of its obligations under Section 2.c (Limitations and Restrictions), Section 5 (Confidentiality) or Section 8 (Intellectual Property Rights) of this Agreement would cause the other Party irreparable harm for which monetary damages would not be an adequate remedy and that, in the event of such breach or threatened breach, the other Party will be entitled to equitable relief, including in a restraining order, an injunction, specific performance and any other relief that may be available from any court of competent jurisdiction, without any requirement to post a bond or other security, or to prove actual damages or that monetary damages are not an adequate remedy. Such remedies are not exclusive and are in addition to all other remedies that may be available at law, in equity or otherwise.

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

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

[Signatures on Next Page]



CONFIDENTIAL

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

Speedly, Inc.

("Speedly")

DocuSigned by:

Authorized Signature

Justin Benson

Print Name

CEO

Title

2/16/2022

Date

American Dairy Queen Corporation

("Customer")

DocuSigned by:

Authorized Signature

Kevin Baartman

Print Name

EVP of Information Technology

Title

2/16/2022

Date



SCHEDULE A

Support Services Terms

Spreedly will provide email support Monday through Friday between 3:00 am and 9:00 pm (US Eastern time zone). Customer and its employees and consultants can contact Spreedly at support@spreedly.com with questions about the Platform, to report errors or other problems with the Platform, or to otherwise request support or assistance with respect to the Platform. Spreedly will maintain a sufficient number of Spreedly support staff to ensure timely responses to emails from Customer and to otherwise satisfy Spreedly's obligations under this Schedule.

Spreedly shall make Updates to the Platform available to Customer on a regular basis. In addition, Spreedly shall troubleshoot and resolve errors related to the Platform in accordance with the following table:

Category	Definition	Spreedly Acknowledgement Time	Resolution
Low	End-user or Customer complaint that requires investigation by Spreedly (including bugs not impacting Transaction Processing Service Availability)	Up to 48 hours	Next update
Serious	Customer's use of Transaction Processing Service is severely impaired due to Spreedly-side issue	Up to 4 hours	Within 3 days
Critical	Transaction Processing Service is unavailable due to Spreedly-side issue	Up to 60 minutes	Within 1 day

Spreedly has internal systems and procedures in place to notify support personnel of critical issues with the Transaction Processing Service 24 hours a day, 7 days a week.



SCHEDULE B

Service Level Agreement

The Transaction Processing Service (as defined below) shall be available 99.95%, measured monthly, excluding scheduled maintenance. For purposes hereof, “**Transaction Processing Service**” means Spreadly’s core API responsible for processing Customer’s payment transaction requests and does not include any beta features or non-payment transaction Spreadly services such as dashboard reporting. For purposes of calculations, the following shall apply:

- “Availability” means that the services are up and running, accessible by Customer and its end users, without interruption or undue delay.
- Any downtime resulting from outages of third-party connections or utilities or other reasons beyond Spreadly’s control will be excluded from any such calculation.
- Any unavailability resulting from Spreadly’s right to suspend the Service in accordance with the terms of the Agreement shall be excluded from any such calculation.
- Downtime shall begin to accrue as soon as the Transaction Processing Service is unavailable to Customer and/or its end users and continues until the availability of the Transaction Processing Service is restored.
- Spreadly shall give no less than 5 business days prior written notice to Customer of all scheduled maintenance. Spreadly shall perform scheduled maintenance in such a way that any interruption of the Transaction Processing Service is kept to a minimum and will provide a maintenance window during which the scheduled maintenance will be carried out (which shall not exceed 60 minutes individually or 24 hours in the aggregate in any month).

In the event of a failure to comply with foregoing service level for a given calendar month (a “Service Level Failure”), Spreadly shall issue a credit to Customer (each, a “Service Credit”) in the following amounts based on the availability for the applicable calendar month (as follows):

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

Service Credits may not be redeemed for cash and shall be applied to Customer’s next applicable payment of Base Annual Fee. In the event of three (3) Service Level Failure events in any consecutive twelve (12) month period, then notwithstanding that Spreadly has cured the failure, Customer may terminate this Agreement upon notice to Spreadly within 30 days following the event triggering the terminate right. The issuance of Service Credits and the terminate right set forth in this Schedule will be Spreadly’s sole obligation and liability and Spreadly’s sole remedy for any Service Level Failure.

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



SCHEDULE C

Data Security Policy

This Data Security Policy describes Spreadly'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 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 Spreadly'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. Spreadly 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. Spreadly agrees that beginning on the Effective Date of the Agreement, Spreadly will employ and maintain, at a minimum, the reasonable and appropriate security controls listed in Attachment A attached hereto and incorporated by reference.

B.2. Data Ownership and Use Limitations. As between Spreadly and Customer, Customer is the owner of any and all Customer Data, including information provided by Customer's clients, customers or users, and Spreadly will have no ownership rights or interest in the Customer Data. Spreadly 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 Spreadly is processing Customer Data, Spreadly 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, Spreadly may at its sole discretion tokenize applicable Customer Data for use within the Platform.

B.5. Third-Party Audit and Compliance. Spreadly 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.spreadly.com/pci and Spreadly 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, Spreadly 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 Spreadly under this Data Security Policy.

B.7. Additional Controls. Spreadly 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 Spreadly'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: Greg Lindseth	Name: Jennifer Rosario
Telephone: (952) 830-0309	Telephone: 888-727-7750
Email: Greg.Lindseth@idq.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 mutually agreed between the Spreedly and the Customer, but may include Spreedly's security practices and procedures.

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. The 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, Spreadly 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 Spreadly for information related to the services under the Agreement (including Customer Data and metadata), Spreadly 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. Spreadly 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 Spreadly'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 Spreadly may be reasonably required.

F. Survival. Spreadly's obligations and Customer's rights in this Schedule will continue as long as Spreadly, or a third party for or on Spreadly'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, Spreadly 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 Spreadly and any Spreadly Affiliate.



Attachment A: Specific Security Controls

Security Controls	
Information Security Governance	<p>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 Information and Supplier Systems; (2) protect against hazards or threats and unauthorized access or use of Information; (3) controls identified risks; (4) addresses access, retention and transport of Information, and (5) acceptable use.</p> <p>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.</p>
Asset Management	<p>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.</p> <p>All corporate laptops are full disk encrypted and wiped per industry standards when decommissioned.</p> <p>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.</p>
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 Spreadly will assess the potential impact of such changes on Security and determine whether such changes are consistent with existing Security. No changes to the Platform or Security should be made which increase the risk of a Security Incident or which would cause a breach of the Schedule.
Cloud Security	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.
Compliance	Mechanisms exist to facilitate the identification and implementation of relevant legislative statutory, regulatory, and contractual controls.
Configuration Management	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.
Continuous logging and monitoring	Mechanisms exist to ensure that all systems used to store Customer Data are logged, monitored, and reviewed regularly.
Cryptographic Protections	Spreadly will encrypt all sensitive cardholder data using appropriate encryption technology wherever it is stored or transmitted. Spreadly 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 Spredly 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	<p>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 Information and Supplier Systems by promptly terminating their physical and electronic access to such Information.</p> <p>With respect to Supplier Systems and 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.</p> <p>Duties and areas of responsibility of Supplier Personnel are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Supplier System or Information.</p>
Incident Response	Maintain policies and procedures for detecting, monitoring and responding to actual or reasonably suspected intrusions and Security Incidents, and encouraging reporting actual or reasonably suspected Security Incidents, including: (1) training Supplier's personnel with access to Customer Data to recognize actual or potential Security Incidents and to escalate and notify the senior management of the foregoing; (2) mandatory post-incident review of events and actions taken concerning security of Customer Data.
Malicious Code Mitigation Software	Mechanisms exist to (1) implement and maintain software for Spredly 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 Information and Supplier System; (2) implementation and management of a secure guest network.
Physical and Environmental Security	<p>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.</p> <p>Policies concerning security for the storage, access, transportation and destruction of records and media containing Information outside of business premises.</p>
Privacy	Mechanisms exist to comply with applicable privacy laws, regulations, and notices.



Risk Management	Periodic and regular information security risk assessment and monitoring of Spredly'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 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 Spredly personnel training concerning, and compliance with, Spredly'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 Spredly personnel concerning: (1) Security; (2) implementing Spredly 's information security program; and (3) the importance of personal information security.
Technology Development and Acquisition	Spredly 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 D

Data Processing Addendum

Compliance with the General Data Protection Regulation in the EU and UK

Spreadly, Inc. (the "Processor") and the company to whom this GDPR Annex has been sent (the "Controller") have one or more written agreements (collectively, "the Agreements") pursuant to which the Processor provides services to the Controller (collectively, the "Services") that may entail the Processing of Personal Data (as defined below).

The European General Data Protection Regulation (GDPR) imposes specific obligations on controllers with regard to their vendor relationships. The GDPR requires controllers to conduct appropriate due diligence and to have contracts with processors containing specific provisions relating to data protection.

Each of the Agreements contains provisions requiring each party to comply with applicable laws pertaining to the privacy and protection of Personal Data. This GDPR Annex documents the data protection requirements agreed to by the parties in furtherance of the Controller's efforts to comply with the GDPR. To the extent applicable, this GDPR Annex is hereby incorporated by reference into each Agreement in order to demonstrate compliance with the GDPR.

1. For purposes of this Annex, "GDPR" means Regulation (EU) 2016/679, the General Data Protection Regulation, together with any additional implementing legislation, rules or regulations that are issued by applicable supervisory authorities. Where Personal Data of data subjects in the United Kingdom is involved, "GDPR" more specifically means and refers to Regulation (EU) 2016/679, the General Data Protection Regulation together with and as implemented by the U.K. Data Protection Act of 2018 and the implementing rules or regulations that are issued by the U.K. Information Commissioner's Office ("ICO"). Words and phrases in this Annex shall, to the greatest extent possible, have the meanings given to them in Article 4 of the GDPR. In particular:
 - (a) "Controller" has the meaning given to it in Article 4(7) of the GDPR: "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."
 - (b) "Personal Data" has the meaning given to it in Article 4(1) of the GDPR: "any information relating to an identified or identifiable natural person; 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," but only to the extent such personal data pertains to persons located in the European Economic Area (EEA) or the United Kingdom (U.K.) (as applicable) or are otherwise subject to the GDPR.
 - (c) "Personal Data Breach" has the meaning given to it in Article 4(12) of the GDPR: "[any] breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."
 - (d) "Processing" has the meaning given to it in Article 4(2) of the GDPR: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."
 - (e) "Subprocessor" means any processor as defined in Article 4(8) of the GDPR: "[any] natural or legal person, public authority, agency or other body which processes personal data" on behalf of the Processor (including any affiliate of the Processor).
 - (f) "Transfer" means to disclose or otherwise make Personal Data available to a third party (including to any affiliate or Subprocessor), either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means. Transfer also includes moving the Personal Data within a single party from the U.K. or an EU member State (as applicable) to a country not within the U.K. or EU (as applicable), or otherwise making such data accessible outside the U.K. or EU (as applicable).



2. The following description of Processing is provided in accordance with GDPR Article 28(3):
 - (a) Nature and Purpose of Processing: All processing operations required to facilitate provision of software and services to the Controller in accordance with the Agreements.
 - (b) Data Subjects: Personnel and customers of the Controller.
 - (c) Categories of Data: With respect to personnel of the Controller, personal details, including information that identifies the data subject such as name, employer, address, e-mail, telephone number, location and other contact details. With respect to customers of the Controller, name, address, e-mail, telephone number, location, and billing and payment details such as bank account and credit or debit card numbers.
 - (d) Special Categories of Data: None.
 - (e) Frequency of Transfer (per Section 6 of this GDPR Annex): Continuously throughout the term of the Agreements.
 - (f) Period of Retention of Personal Data: Except as otherwise provided in the Agreements or this GDPR Annex, in accordance with the retention policy of the Processor, provided that to the extent that any Personal Data is retained beyond the termination of the Agreements for back up or legal reasons, the Processor will continue to protect such personal data in accordance with the Agreements and this GDPR Annex.
 - (g) For Transfers to Subprocessors, the subject matter, nature and duration of the Processing: As described in Sections 4 and 6 of this GDPR Annex.
3. In accordance with GDPR Article 28(1), Processor represents that it has implemented appropriate technical and organizational measures in such a manner that its Processing of Personal Data will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects.
4. The Processor will maintain a current list of Subprocessors used throughout the service, including the Subprocessor's name and purpose of their processing. This list will be accessible via <http://www.spreadly.com/gdpr/subprocessors>. Controllers may receive notifications of new Subprocessors by emailing subprocessor@spreadly.com with the subject "Subscribe" and once subscribed in this manner that Controller will receive notification of new Subprocessors before those Subprocessors are authorized to process Personal Data on behalf of the Processor.

The controller may reasonably object to the Processor's use of new a Subprocessor by notifying the Processor in writing within ten business days of receiving the notice of intent to authorize via the mechanism specified in Section 3 above. This notice shall explain the reasonable grounds for objection (e.g., if the use of this Subprocessor would violate applicable laws or weaken protections for the applicable Personal Data). The Processor will make commercially reasonable efforts to resolve the objection by the Controller. If the Processor is unable to resolve the objection within a reasonable period of time, not to exceed 30 days, then either party may terminate the Agreements without penalty.

5. In accordance with GDPR Article 28(3), the following terms are incorporated by reference into the Agreements:
 - (a) The Processor shall only process the Personal Data (i) as needed to provide the Services, (ii) in accordance with the specific instructions that it has received from the Controller, including with regard to any Transfers, and (iii) as needed to comply with law (in which case, the Processor shall provide prior notice to the Controller of such legal requirement, unless that law prohibits this disclosure);
 - (b) Processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 - (c) Processor shall take all security measures required by GDPR Article 32, namely:
 - i. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures to



- ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- ii. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
 - iii. The Processor shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not process such Personal Data except upon instructions from the Controller, unless the Processor is required to do so by U.K. or EEA Member State law (as applicable).
- (d) Taking into account the nature of the processing, Processor shall reasonably assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights;
 - (e) Taking into account the nature of processing and the information available to the Processor, Processor shall reasonably assist the Controller in the Controller's efforts to comply with its obligations regarding Personal Data Breaches (as set forth in GDPR Articles 33 and 34), data protection impact assessments (as set forth in GDPR Article 35), and prior consultation (as set forth in GDPR Article 36);
 - (f) At the Controller's discretion, the Processor shall delete or return all the Personal Data to the Controller after the end of the provision of services relating to Processing, and delete existing copies unless applicable U.K. or EEA member state law requires storage of the Personal Data;
 - (g) The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations laid down in the GDPR, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller; and
 - (h) The Processor shall immediately inform The Controller if, in its opinion, an instruction infringes the GDPR or other U.K. or EU Member State data protection provisions.
6. The Processor shall not Transfer any Personal Data (and shall not permit its Subprocessors to Transfer any Personal Data) without the prior consent of the Controller. The Processor understands that the Controller must approve and document that adequate protection for the Personal Data will exist after the Transfer, using contracts that provide sufficient guarantees (such as standard contractual clauses) unless another legal basis for the Transfer exists. The Controller hereby consents to the Processor's Transfer of Personal Data to the Subprocessors described in Section 3 above. Additionally, the Controller understands, acknowledges and agrees that the Processor is (and its Subprocessors may be) based in the United States and that the Processor provides (and the Subprocessors may provide) services under the Agreement from the United States, and the Controller hereby consents to the Transfer of Personal Data to the United States for Processing by the Processor and its Subprocessors in accordance with Section 7 (EEA) or Section 8 (U.K.), as applicable, below.
7. The Processor and the Controller hereby agree to enter into the Standard Contractual Clauses issued by the European Commission on June 4, 2021 ("SCCs"), which are incorporated by reference into this GDPR Annex on an unchanged basis save for the following:
- (a) Only "Module 2" of the SCCs (Controller to Processor) applies.
 - (b) For the purposes of clause 9(a) of the SCCs, option 1 ("Specific Prior Authorisation") is deleted and the specified time period is 10 days in advance.
 - (c) For the purposes of clause 11(a) of the SCCs, the optional language is deleted.



- (d) For the purposes of clause 13 of the SCCs: (i) if the Controller is established in an EU Member State, the relevant supervisory authority acting as the competent supervisory authority is the supervisory authority of the EU Member State in which the Controller is established, (ii) if the Controller is not established in an EU Member State but has appointed a representative pursuant to GDPR Article 27(1), the relevant supervisory authority acting as the competent supervisory authority is the supervisory authority of the EU Member State in which the Controller's representative is established, and (iii) if the Controller is not established in an EU Member State and has not appointed a representative pursuant to GDPR Article 27(1), then the supervisory authority of one of the EU Member States in which the data subjects whose Personal Data is Transferred under these Clauses in relation to the offering of goods or services to them are located shall act as competent supervisory authority. This paragraph shall constitute "Annex I.C" for purposes of the SCCs.
 - (e) For the purposes of clause 17 of the SCCs, the governing law is Ireland.
 - (f) For purposes of clause 18(b) of the SCCs, the selection is Ireland.
 - (g) The Recitals above, the relevant party identification information from the Agreements and the description of processing in Section 2 of this GDPR Annex together shall constitute "Annex 1" for the purposes of the SCCs. Schedule C – Spredly's Data Security Policy attached to the Agreements shall be attached to the SCCs and constitute "Annex 2" for the purposes of the SCCs.
8. The Processor and the Controller hereby agree to enter into the Standard Contractual Clauses for Controller to Processor Transfers issued by ICO and made available online at <https://ico.org.uk/media/for-organisations/documents/2620100/uk-sccs-c-p-202107.docx> (the "U.K. SCCs"), which are incorporated by reference into this GDPR Annex on an unchanged basis save for the following:
- (a) The Recitals above, the relevant party identification information from the Agreements and the description of processing in Section 2 of this GDPR Annex together shall constitute the Parties section and "Appendix 1" for the purposes of the U.K. SCCs. Schedule C – Spredly's Data Security Policy attached to the Agreements shall constitute the description of the technical and organizational security measures for "Appendix 2" for the purposes of the U.K. SCCs.
 - (b) For the purposes of clause 9 of the U.K. SCCs, the governing law shall be deemed to be that of England & Wales.
 - (c) No optional additional clauses are adopted.
9. The Processor will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Data. Processor will notify the Controller without undue delay in the event of any Personal Data Breach.
10. The Processor shall maintain all records required by Article 30(2) of the GDPR, and (to the extent they are applicable to Processor's activities for the Controller) Processor shall make them available to the Controller upon request.
11. The Processor will allow the Controller, or a third-party appointed by the Controller, to conduct audits (including inspections) to verify the Processor's compliance with the Agreements described in this document.
- (a) The Controller may request an audit by emailing succcess@spredly.com.
 - (b) Following receipt of this request, the Processor and Controller will discuss and agree in advance on the reasonable scope, start date and duration of this audit, as well as any applicable security and confidentiality controls that may be required.
 - (c) The Processor may charge a fee (based on the Processor's reasonable costs) for any such audit. The Processor will provide the Controller with additional details of this fee including the basis of its calculation, in advance of the audit. Additionally, the Controller will be responsible for any fees charged by any third-party auditor appointed by the Controller for this audit.
12. In Accordance with GDPR Article 24(1), the following terms are incorporated by reference into the Agreements:



CONFIDENTIAL

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