



## ENTERPRISE SERVICE AGREEMENT

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

SPREEDLY		CUSTOMER	
Name:	Spreedly, Inc.	Name:	Oracle America, Inc.
Address:	300 Morris Street, Suite 400	Address:	
City/State:	Durham, NC 27701	City/Country:	
<b>PRIMARY SPREEDLY CONTACT</b>		<b>PRIMARY CUSTOMER CONTACT</b>	
Name:	Helen Kruskamp	Name:	Oliver Auerbach
Title:	Enterprise Account Executive	Title:	
Phone:	1-888-727-7750	Phone:	
Email:	hmkruskamp@spreedly.com	Email:	oliver.auerbach@oracle.com
<b>SPREEDLY FINANCE CONTACT</b>		<b>CUSTOMER BILLING CONTACT</b>	
Name:	Spreedly Accounting Department	Name:	
Phone:	888-727-7750	Phone:	
Email:	accounting@spreedly.com	Email:	

### Background

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

### Agreement

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

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

1.1. "**Affiliate(s)**" means any entity that is now or in the future directly or indirectly controlled by, controlling or under common control with a Party.

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

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

1.4. "**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.

1.5. "**Claim**" means any claim, suit, action, proceeding, or investigation by a governmental body.



1.6. “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.

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

1.8. “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.

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

1.10. “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.

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

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

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

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

1.15. “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.

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

2.1.1. Customer may enter into an Order Form for any Spreedly services to be performed on behalf of a Customer Affiliate or share all or any part of this Agreement and any Confidential Information disclosed hereunder with a Customer Affiliate provided that Customer remains ultimately responsible for any obligation, financial or otherwise, of any such Customer Affiliate.

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. 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 not authorized under this Agreement 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 Spreedly's competitors, for any purpose, otherwise non-public information about the Platform.

2.4. Changes to the Platform. Spreedly may make any changes to the Platform (including, without limitation, the design, look and feel, functionality, content, material, information and/or services provided via the Platform) that Spreedly deems necessary or useful to improve the Platform or for any other reason, from time-to-time in Spreedly's sole discretion, and without notice to Customer; provided, however, that Spreedly will not make any such changes that will materially adversely affect its features or functionality available to Customer during the Term. Such changes may include upgrades, bug fixes, patches and other error corrections and/or new features (collectively, including related Documentation changes, "Updates"). All Updates will be deemed a part of the Platform governed by all the provisions of this Agreement pertaining thereto. Notwithstanding the foregoing, if the features and functionality of the Platform available to Customer are materially adversely affected by a change, Customer shall have the right to terminate this Agreement without penalty and shall be entitled to a pro-rated refund of any pre-paid fees remaining under any existing Order Form(s).

2.5. Subcontractors. Spreedly may, in Spreedly's discretion, engage subcontractors to aid Spreedly in providing the Platform and performing Spreedly's obligations under this Agreement, but Spreedly will remain liable to Customer for any act or omission by such subcontractors that would be a breach or violation of this Agreement. Spreedly may use Amazon Web Services, Microsoft Azure, Google Cloud Platform and/or such other reputable hosting provider that implements and maintains commercially reasonable security programs, policies, procedures, controls and technologies (each a "Reputable Hosting Services Provider") for cloud-based infrastructure and hosting and storage services for the Platform, and such Reputable Hosting Services Provider will host and store certain portions of Customer Data that is processed through the Platform. Customer hereby specifically approves and consents to Spreedly's use of a Reputable Hosting Services Provider in the manner described provided Spreedly can produce a copy of a current Attestation of Compliance with PCI-DSS standards and SOC 2 certificate to confirm the Reputable Hosting Services Provider is operating in a manner consistent with industry best practices and complies with the requirements for the Data Security Policy.

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

2.7. Suspension of Services and Platform Access. Spreedly may suspend or deny Customer's access to or use of all or any part of the Platform and Support Services, without any liability to Customer or others, if (i) Spreedly is required to do so by Law or court order; or (ii) Customer has (A) failed to comply with Section 2.2 or 2.3), or (B) otherwise breached a material term of this Agreement and have failed to cure such breach within thirty (30) days after Spreedly



provides written notice thereof to Customer. Spreedly's remedies in this Section are in addition to, and not in lieu of, Spreedly's termination rights in Section 10.

2.8. Customer Data Export; Customer Data Retention. Customer may elect at any time to perform an automatic export of any Card Data and/or other Customer Data to a third-party endpoint for which Spreedly supports third-party vaulting as set forth at Spreedly's website (currently: <https://docs.spreedly.com/guides/third-party-vaulting>). For any endpoint for which automatic export is not supported, Customer may request that Spreedly perform one (1) free-of-charge manual export during the Term, of any Card Data or other credit card or user information associated with Customer's account to a recipient designated by Customer, provided that the recipient has proven that it is PCI-DSS compliant, and the transfer is not in violation of any applicable Laws. If Customer requires additional manual exports during the Term, each additional manual export will incur an export charge at Spreedly'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 Availability.

3.1. Support Services. During the Term, so long as Customer complies with this Agreement, Spreedly will provide customer support services (the "Support Services") to Customer in accordance with Spreedly's Support Service Terms posted at Spreedly's website (currently: <https://www.spreedly.com/support-services-terms>) at the support level specified on the Order Form.

3.2. Availability. During the Term, so long as Customer complies with this Agreement, Spreedly will make the Platform available for access and use by Customer in accordance with Spreedly's Availability Commitments posted at Spreedly's website (currently: <https://www.spreedly.com/support-services-terms>) corresponding to the support level specified on the Order Form. SPREEDLY'S SOLE OBLIGATION AND LIABILITY TO CUSTOMER FOR ANY FAILURE TO MEET THE AVAILABILITY COMMITMENTS ARE THE SERVICE CREDITS SPECIFIED IN THE SUPPORT SERVICE TERMS REFERENCED ABOVE.

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

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

4.2. Personnel. Spreedly reserves the right to determine which of Spreedly's personnel and/or subcontractors will be assigned to perform Professional Services, and to replace or reassign such personnel during the Term, provided any such Spreedly personnel and/or subcontractors must have qualifications suitable for the work described in the relevant Statement of Work. Spreedly may only replace or change Spreedly personnel and/or subcontractors with other suitably qualified employees and/or subcontractors.

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 twenty (20) 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 twenty (20) 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) financial information and pricing, (B) technical information, such as research, development procedures, algorithms, data, designs, and know-how, (C) individually identifiable personal information, (D) business and operational information, such as planning, marketing interests, pricing and products, and (E) customer lists and all related information. For avoidance of doubt, all non-public information related to the Platform (including without limitation, pricing information (e.g., price quotes) and the source code for the Platform and the methods, algorithms, structure and logic, technical infrastructure, techniques and processes used by Spreedly in developing, producing, marketing and/or providing the Platform) are Spreedly’s Confidential Information, Customer Data is Customer’s Confidential Information, and the terms of this Agreement and any Order Form or Statement of Work are the Confidential Information of both Parties.

5.2. Exclusions. Confidential Information of a Disclosing Party does not include information that the Receiving Party can demonstrate by written or other documentary records: (i) was rightfully known to the Receiving Party without restriction on use or disclosure prior to such information being disclosed or made available to the Receiving Party in connection with this Agreement; (ii) was or becomes generally known by the public other than by the Receiving Party’s or any of its Representatives’ (as defined in Section 5.3 below) noncompliance with this Agreement; (iii) was or is received by the Receiving Party on a non-confidential basis from a third party that was not or is not, at the time of such receipt, under any obligation to maintain its confidentiality; (iv) was or is independently developed by the Receiving Party without reliance upon any Confidential Information; or (v) to the extent it was or is independently developed by the Receiving Party with use of or reliance upon Residual Information (as defined below).

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

5.4. Legally Required Disclosures. If a Receiving Party or one of its Representatives is required by any Law, rule or order of any governmental body or agency, or as otherwise necessary to maintain or comply with any regulatory certifications or requirements, to disclose any Confidential Information, such Receiving Party (i) will, to the extent legally permissible, give the Disclosing Party prompt notice of such request so that the Disclosing Party may (at its own





expense) seek an appropriate protective remedy, and (ii) will, and will cause its Representatives to, cooperate with the Disclosing Party (at the Disclosing Party's expense) in the Disclosing Party's efforts to obtain any such protective remedy. In the event that the Disclosing Party is unable to obtain such a protective remedy, the Receiving Party or its Representatives, as applicable, will (A) furnish only that portion of the Confidential Information that the Receiving Party or its Representatives is required to disclose in the opinion of the Receiving Party's or its Representatives' outside counsel, (B) exercise reasonable efforts to assist the Disclosing Party (at the Disclosing Party's expense) in obtaining assurances that confidential treatment will be accorded the Confidential Information so required to be disclosed, and (C) give notice to the Disclosing Party of the information to be disclosed as far in advance of disclosure of the same as is reasonably possible and legally permissible.

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

## 6. Data Protection and Privacy.

6.1. Data Security. During the Term, so long as Customer complies with this Agreement, Spreedly will implement safeguards to protect against anticipated threats or hazards to the security, confidentiality or integrity of Customer Data in accordance with the Oracle Supplier Data Protection Agreement in Schedule B, (the "Data Security Policy").

6.2. Data Privacy. In the event that the Parties enter into an Order Form and/or SOW whereby Spreedly collects, accesses, processes, stores, transfers, transmits, uses, discloses or otherwise handles any Customer Data that includes "personal information," "personal data" or "personally identifiable information" as defined under applicable law (collectively "Personal Information"), Spreedly will store, use and otherwise process such Personal Information in all material respects in accordance with all applicable laws relating to the privacy and protection of the Personal Information involved ("Data Privacy Laws"), including but not limited to the California Consumer Privacy Act of 2018 and its implementing regulations (as amended, restated or supplemented from time to time, "CCPA") where applicable. Spreedly will not access, use, handle, maintain, process, dispose of, or disclose Personal Information other than as permitted or required under this Agreement or Data Privacy Laws. Spreedly will limit dissemination of Personal Information to its employees and subcontractors who (i) need to know the information to enable Spreedly to perform its obligations or exercise its rights under this Agreement, and (ii) are bound by confidentiality obligations substantially equivalent to those provided for in this Agreement. Upon Customer's written request Spreedly will cooperate with Customer as may be reasonably required to enable Customer to comply with Data Privacy Laws, including by reasonably assisting Customer in complying with individuals' rights in regards to their Personal Information under Data Privacy Laws. In furtherance of the foregoing, based on the Customer Data that Customer will process using the Platform or otherwise provide to Spreedly, if and to the extent Data Privacy Laws require additional clauses to be executed by Spreedly beyond those set forth in this Agreement, then Customer will notify Spreedly in writing of such requirement and Spreedly will in good faith review, negotiate and consider adding such clauses as an addendum to this Agreement. In the absence of such notice Customer represents and warrants that no additional clauses are required. The current processing agreement is attached hereto as Schedule C.

6.3. CCPA Service Provider Compliance. Spreedly and Customer both agree that Customer is a business and Spreedly is a service provider under CCPA. Spreedly will: (i) not retain, use or disclose personal information for any purpose (including any commercial purpose) other than for the specific purpose of providing the Platform and performing the Support Services and Professional Services contemplated by this Agreement; (ii) not retain, use or disclose personal information outside of the direct business relationship between Customer and Spreedly; and (iii) not sell the personal information to any third parties. Spreedly certifies that it understands and will comply with the restrictions, duties and obligations set forth in this Section 6.3. In the event that any consumer makes a request directly to Spreedly with respect to exercising its privacy rights under CCPA, Spreedly will promptly notify Customer and provide Customer with a copy of the consumer request, inform the consumer that the consumer's request cannot be acted upon because the request has been sent to a service provider, provide Customer with a copy of such response, and reasonably cooperate with Customer in its efforts to respond and act on the consumer's request in accordance with the requirements of CCPA, in each case unless legally prohibited from doing so. As permitted and provided by CCPA, nothing in this Section 6.3 will prohibit Spreedly from retaining, using or disclosing the personal information in connection with: (z) retaining or employing another service provider as a subcontractor, provided the subcontractor meets the requirements for a service provider under CCPA; (y) Spreedly's internal use to build or improve the quality of its Platform or services, provided that the 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 Spreedly, Customer or



a third party reasonably and in good faith believes may violate applicable law; or (t) exercising or defending legal claims. For purposes of this Section 6.3, the terms “business,” “commercial purpose,” “consumer,” “personal information,” “processing,” “sell” and “service provider” will have the meanings given to such terms in CCPA.

## 7. Fees and Payment.

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

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

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

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 Spreedly (including Spreedly’s rights under Section 2.7 and Section 9.3), Spreedly may charge interest on the past due amount at the rate of 1.5% 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 Spreedly owns all right, title and interest in and to the Platform and the Documentation, including all Intellectual Property Rights therein and all derivative works thereof. Spreedly is not granting Customer any right, license or authorization with respect to the Platform or the Documentation, except as specifically provided in Section 2.1 above (and subject to the limitations and restrictions in Section 2.3 above). Spreedly reserves all rights not expressly granted to Customer in this Agreement.

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

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

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

8.5. Publicity Rights. During the Term, Customer agrees that Spreedly may, with written consent from Customer and according to Customer’s published Trademark policies, include Customer’s name, trademarks and logos on Spreedly’s website and in other sales and marketing materials in order to factually identify Customer as a current customer. The parties will not unreasonably withhold or delay their consent to press releases or public announcements.



## 9. Term and Termination.

9.1. Term. Unless otherwise terminated in accordance with this Agreement, the initial term of this Agreement will be for the duration specified in the Initial Order Form (the "Initial Term"). Thereafter, unless a Party provides the other Party of its intention not to renew in writing at least one hundred twenty (120) days prior to the expiration of the current Order Form or Statement of Work, this Agreement will automatically renew for successive renewal terms (each, a "Renewal Term" and, together with the Initial Term, the "Term"), subject to, and in accordance with, the terms of the Initial Order Form. Unless otherwise mutually agreed upon by the Parties, the term of each additional Order Form will be the same as the term set forth in the Initial Order Form.

9.2. Termination. In addition to any other termination rights described in this Agreement, this Agreement may be terminated at any time by either Party, effective when that Party provides written notice to the other Party: (i) at any time that there are no active and outstanding Order Forms and Statements of Work; or (ii) if the other Party materially breaches the terms of this Agreement (including, for avoidance of doubt, the terms of any Order Form or Statement of Work incorporated herein) and such breach remains uncured thirty (30) days after the non-breaching Party provides the breaching Party with written notice regarding such breach.

9.3. Effect of Termination. The exercise of any right of termination under this Agreement will not affect any rights of either Party (including rights to payment or reimbursement) that have accrued prior to the effective date of termination and will be without prejudice to any other legal or equitable remedies to which a Party may be entitled. If this Agreement is terminated or expires, then: (i) 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) each Party will discontinue use of the other Party's trademarks and promptly remove any references and logos the other Party from their respective websites; and (iv) each Party will promptly return to the other or, if so directed by the other Party, destroy all originals and copies of any Confidential Information of the other Party (including all notes, records and materials developed therefrom).

9.4. Transition Assistance. Upon termination or expiration of this Agreement or an Order Form for Services, for any reason, then upon request by Customer (email to suffice) made prior to the expiration date, or no later than five (5) days after the issuance of a notice of termination in accordance with the terms of this Agreement, Spreadly will continue to provide access to the Platform and provide reasonable cooperation to Customer in order for Customer to export or arrange export of its card data or other credit card or user information associated with Customer's account and/or other services necessary for such export, including without limitation, an export made in connection with Section 2.8, (the "Transition Services") for a period up to 180 days after the expiration or termination date or as otherwise agreed by the parties in writing (the "Transition Period"). The terms of this Agreement will continue to govern Spreadly's provision of the Transition Services during the Transition Period as if it had not been terminated. Unless otherwise provided in an Order Form, if Customer continues to use the Platform in production, then the Fees for services covered by an Order Form during the Transition Period will be the same as those charged under the relevant Order Form in effect immediately preceding the termination date and prorated for the duration of the Transition Period or other such fees as the parties may agree to in writing.

9.5. Surviving Terms. Sections 1 (Definitions), 5 (Confidentiality), 7 (Fees and Payment), 8 (Ownership and Intellectual Property Rights), 9.3 (Effect of Termination), 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 as applicable that: (i) it is duly organized, validly existing and in good standing as a corporation or other entity under the laws of the jurisdiction of its incorporation or other organization; (ii) it has the full right, power and authority to enter into and perform its obligations under this Agreement; (iii) the execution of an Order Form by its representative has been duly authorized by all necessary corporate or organizational action of Customer; and (iv) when executed and delivered by both Parties, the Agreement will constitute the legal, valid and binding obligation of Customer, enforceable against Customer in accordance with its terms

10.2. Customer Representations. Customer represents and warrants that: (i) it will not use the Platform, directly or indirectly, for any fraudulent undertaking or in any manner so as to interfere with the use of the Platform; (ii) Customer's use of the Platform and its collection and use of all of Customer Data (including Customer's processing of Customer Data and/or any card authorization, credit, ticket only, capture or settlement request, decline transaction, or other related transaction, completed or submitted under Customer's account) will comply with (A) all applicable Laws, (B) the terms of service of the payment gateways, merchant service providers and/or API endpoints applicable to Customer through Customer's connection 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; and (iv) Spreedly's and its subcontractors' access to and use of Customer Data (including, for the avoidance of doubt, the Card Data and all personal data included with Customer Data) as contemplated by this Agreement does not and will not violate any applicable Law or infringe, misappropriate or otherwise violate any Intellectual Property Right, privacy right or other right of any third party.

10.3. Spreedly Representations. Spreedly represents and warrants that:

- 10.3.1. it will comply with all applicable rules and guidelines regarding service providers, third-party agents and processors as issued by the Card Associations (the "Card Rules"), as updated from time to time, and including Card Rules applicable to U.S. and international credit card transactions;
- 10.3.2. it will (A) be compliant with PCI-DSS and all other applicable standards and guidelines issued by the PCI Security Standards Council, LLC, (the "Council"); (B) validate its PCI-DSS compliance as required by the applicable Card Rules; (C) undergo annual PCI-DSS assessments by a Qualified Security Assessor; and (D) notify Customer if it becomes aware that it is no longer in compliance with PCI-DSS. Spreedly will provide proof of its PCI-DSS compliance to Customer upon request and evidence of its successful completion of its annual assessments on its website (currently available at <https://www.spreedly.com/pci>);
- 10.3.3. the Platform will perform in all material respects in accordance with the functional specifications set forth in the applicable Documentation. If Spreedly breaches this warranty, as Spreedly's sole obligation and liability to Customer and Customer's sole and exclusive remedy, Spreedly will, at its option: (a) promptly correct any portion of the Platform that fails to meet this warranty; (b) provide Customer with a reasonable procedure to circumvent the nonconformity; or (c) refund to Customer on a *pro rata* basis the share of any Fees prepaid by Customer for the portion of the applicable Term in which the Platform is non-conforming;
- 10.3.4. it will perform all Professional Services in a professional and workmanlike manner. If Spreedly breaches this warranty, as Spreedly's sole obligation and liability to Customer and Customer's sole and exclusive remedy, Spreedly will promptly re-perform the non-conforming Services at no additional cost to Customer.

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

11. Indemnification.

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

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

11.3. Indemnification Process. Each Party will promptly notify the other Party in writing of any Claim for which such Party believes it is entitled to be indemnified pursuant to Section 11.1 or 11.2. The Party seeking indemnification (the "Indemnitee") will cooperate with the other Party (the "Indemnitor") at the Indemnitor's sole cost and expense. The



Indemnitor will promptly assume control of the defense and investigation of such Claim and will employ counsel of its choice to handle and defend the same, at the Indemnitor's sole cost and expense. The Indemnitor'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 Indemnitor 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 Indemnitor without the Indemnitor's prior written consent.

#### 11.4. Additional Terms for Infringement Claims.

- 11.4.1. Spreedly will have no liability or obligation with respect to any Infringement Claim to the extent based upon or arising out of: (A) access or use of the Platform other than as provided in the Platform Documentation; (B) use of the Service in the practice of a process or system other than that for which it was intended; or (C) any action taken by Customer relating to use of the Platform that is outside the scope of the rights and authorizations granted or otherwise in breach of this Agreement and/or any applicable Order Form.
- 11.4.2. If the Platform is, or in Spreedly's opinion is likely to be, the subject of an Infringement Claim, or if Customer's use of the Platform is enjoined or threatened to be enjoined, Spreedly may, at Spreedly's option and Spreedly's sole cost and expense: (A) obtain the right for Customer to continue to use the allegedly infringing Platform as contemplated by this Agreement, (B) modify or replace the allegedly infringing Platform to make the Platform (as so modified or replaced) non-infringing, or (C) if Spreedly determine the remedies in clauses (A) and (B) are not commercially reasonable, then Spreedly may terminate the applicable Order Form upon written notice and without any liability to Customer and Spreedly will promptly refund to Customer on a *pro rata* basis the share of any Fees prepaid by Customer for the future portion of the applicable Term that would have remained but for such termination.
- 11.4.3. THIS SECTION 11 SETS FORTH CUSTOMER'S EXCLUSIVE REMEDIES, AND SPREEDLY'S SOLE OBLIGATION AND LIABILITY TO CUSTOMER OR ANY OTHER PERSON OR ENTITY, FOR ANY ACTUAL, THREATENED OR ALLEGED CLAIMS THAT THE PLATFORM (INCLUDING CUSTOMER'S USE THEREOF) INFRINGES, MISAPPROPRIATES OR OTHERWISE VIOLATES ANY INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

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

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

#### 14. Miscellaneous.

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

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



will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable.

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

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

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

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

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

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

14.9. 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.

14.10. 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](http://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.

---

Spreedly, Inc.

("Spreedly")

DocuSigned by:

A handwritten signature in blue ink, appearing to read "Justin Benson", is written over a blue rectangular DocuSign signature line.

---

Authorized Signature

Justin Benson

---

Print Name

CEO

---

Title

9/30/2022

---

Date

---

Oracle America, Inc.

("Customer")

DocuSigned by:

A handwritten signature in blue ink, appearing to read "Simon de Montfort walker", is written over a blue rectangular DocuSign signature line.

---

Authorized Signature

Simon de Montfort walker

---

Print Name

Svp / GM fgbu

---

Title

9/30/2022

---

Date



**SCHEDULE A**  
**ORDER FORM [#]**

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

**To:**  
**Customer Legal Name:**  
**Tax ID:**  
**Billing Address:**  
**Sales Rep:**

**Order Form Issued:**  
**Offer Valid Until:**

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

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

**1) Order Form Term**

**2) Platform Fees:**

**3) API Usage Fees:**

**4) Account Updater:**

**5) Payments:**

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

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

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

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

**SAMPLE ONLY DO NOT SIGN**



## SCHEDULE B

### Oracle Supplier Information and Physical Security Standards

These Supplier Information and Physical Security Standards (the “Standards”) list the minimum security controls that Oracle’s Suppliers are required to adopt when (a) accessing Oracle or Oracle customer facilities, networks, and/or information systems, (b) handling Oracle confidential information, or (c) having custody of Oracle hardware assets.

#### SUPPLIER OBLIGATIONS

Supplier is responsible for compliance with these Standards by its personnel, including ensuring that all personnel are bound by contractual terms consistent with the requirements of these Standards. Additional security compliance requirements may be specified in Supplier’s agreement.

#### PART A: PERSONNEL/HUMAN RESOURCES SECURITY

A.1 Unless prescribed otherwise in the agreement, Supplier will perform background checks, consistent with local laws and regulations, for all personnel. The level of verification performed should be proportional to risk correlated to roles within the organization.

A.2 Supplier personnel are required to agree, in writing, to abide by Supplier’s security requirements and organizational policies.

A.3 Supplier must have a comprehensive security awareness program for all personnel that encompasses education, training and updates for security policies, procedures and requirements. Security awareness training must occur at time of hiring and repeated at regular intervals thereafter (no less than every two (2) years).

A.4 Supplier must have formal disciplinary processes in place for personnel and take appropriate action against personnel who violate Supplier’s organizational policies, based upon the nature and gravity of the violation.

A.5 Upon termination of employment, Supplier will promptly remove personnel access to information systems, networks, and applications. Personnel must also return all company provided computers, mobile devices and other equipment used to perform the services. Supplier will remind personnel that they must not retain any confidential information.

A.6 Unless otherwise specified in an Oracle Supplier Data Processing Agreement (SDPA), Supplier is authorized to use subcontractors for the provision of the Services as long as they are contractually bound to comply with nondisclosure terms and security standards consistent with those set forth in the agreement and these Standards.

A.7 Supplier will maintain a list of its authorized subcontractors, the country/countries to which confidential information may be transferred to or accessed from, a description of the services performed by such subcontractors, and make that list available to Oracle.

#### PART B: BUSINESS CONTINUITY AND DISASTER RECOVERY

B.1 Suppliers must have a Disaster Recovery (DR) program and maintain a documented organizational Business Continuity Plan (BCP). The program and plans must be designed to ensure that Supplier can continue to function through operational interruption and continue to provide services, as specified in the agreement.

B.2 Supplier must ensure that the scope of the BCP covers all locations, personnel and information systems that are used to perform services for Oracle.

B.3 The BCP must be tested on a regular basis (at minimum, on an annual basis). Supplier must document the results. On request, Supplier will provide documentation for Oracle’s review to confirm that tests are being performed.

B.4 If there is an event, which will or does impact Supplier’s capability to perform services for Oracle, including execution of the DR plan, Supplier must promptly notify their Oracle business contact.

## **PART C: INFORMATION SECURITY ORGANIZATION, POLICIES, AND PROCEDURES**

C.1 Supplier must have clearly defined organizational IT/information security roles, responsibilities and accountability.

C.2 Supplier must publish and maintain formal written information security policies. Information security policies must be approved by management and communicate personnel's obligations to protect confidential information and the acceptable use and protection of information.

C.3 Supplier must classify and label Information in accordance with their information classification scheme and in terms of its sensitivity.

C.4 Supplier will implement security processes for managing suppliers and subcontractors throughout the business relationship lifecycle.

C.5 Supplier will maintain an inventory of assets that includes all business critical information systems and information processing sites that are used in the delivery of services to Oracle. The asset inventory should be accurate, up to date and have owners assigned to each asset.

C.6 Where applicable, Supplier will maintain a complete list of all personnel with permission to access Oracle facilities, information systems, networks and applications, including their employment location.

## **PART D: COMPLIANCE AND ASSESSMENTS**

### **D.1 Regulatory Compliance**

D.1.1 If services involve the processing of payment card information, Supplier will maintain compliance with the current version of the Data Security Standards (DSS) from the Payment Card Industry Security Standards Council (PCI SSC) for the duration of the services provided to Oracle. On request, Supplier will provide Oracle with the most recent PCI SSC "Attestation of Compliance" (AoC) reports prepared by a third-party PCI Qualified Security Assessor (QSA) for both Supplier's systems and for any third-parties used by the Supplier for handling payment card data.

### **D.2 Security Compliance and Assessments**

D.2.1 If Supplier is provided access to Personal Information by Oracle or Oracle customers, or Personal Information is otherwise processed by Supplier on Oracle's or Oracle customer's behalf, Supplier must sign an Oracle SDPA.

D.2.2 All Suppliers accessing Oracle's network must execute an Oracle Network Access Agreement (NAA).

D.2.3 Supplier will provide Oracle with the contact information of the person(s) Oracle may contact in relation to any information security and/or compliance issues.

D.2.4 If requested, on an annual basis, Supplier will complete a documented security questionnaire and provide written responses about its security practices, to enable Oracle to assess compliance with the requirements of these Standards and applicable law.

D.2.5 If requested, in order to confirm compliance with these Standards, upon reasonable notice and in coordination with Supplier, Oracle may perform on-site security assessments.

D.2.6 Only when and to the extent required of Oracle by contract or applicable law, Supplier will ensure that Oracle has direct access to assess subcontractors.

D.2.7 Supplier must promptly correct any noncompliance issues identified during the documented and/or on-site security assessment process.

## **PART E: SECURITY INCIDENT MANAGEMENT AND REPORTING**

E.1 Supplier must have documented information security incident response procedures that enable the effective and orderly management of security incidents. The procedures must cover the reporting, analysis, monitoring and resolution of security incidents.

E.2 Reported security incidents shall be verified and then analyzed to determine their impact. All confirmed incidents should be classified, prioritized and logged.

E.3 Security incidents should be handled by a dedicated security incident response team or personnel who are trained in handling and assessing security incidents in order to ensure appropriate procedures are followed for the identification, collection, acquisition, and preservation of information.

E.4 Supplier must report security incidents of which they become aware relating to the Oracle services without undue delay (but at the latest within 24 hours) to their business contacts at Oracle for the applicable services impacted by the security incident and sending e-mail to security\_breach\_ww@oracle.com.

E.5 Other than to law enforcement or as otherwise required by law, Supplier may not make or permit any statements concerning security incidents involving Oracle confidential information, information systems or assets to a third-party without the written authorization of Oracle's Legal Department, unless the statements do not identify or could not reasonably be used to identify Oracle as being impacted by the incident.

E.6 Unless prohibited by law, Supplier will promptly notify Oracle in the event it receives an external request to provide access to Oracle confidential information or information systems.

## **PART F: IT SECURITY STANDARDS**

### **F.1 IT Security Controls**

F.1.1 Suppliers information systems, network devices, and applications should be configured and deployed using a secure baseline. Ports/services that are not used should be disabled.

F.1.2 Supplier must implement controls to terminate inactive sessions and restrict the connection times of idle/inactive sessions on information systems, network devices and applications.

F.1.3 System clocks should be synchronized to a trusted time server source so that time/time zone is accurately maintained on all information systems, network devices, and applications, to ensure logs files have consistent time stamp information recorded.

F.1.4 Prior to implementation of information systems, network devices, and applications that will be used to process/store Oracle confidential information, a security review process should be followed to validate security of the information systems, network devices, and applications to identify and remediate critical security issues ahead of deployment.

F.1.5 Supplier will perform security assessments in the form of technical scans and testing of information systems, networks, and applications at planned intervals, at least annually, to verify compliance with organizational security policies and standards.

F.1.6 Supplier will maintain documented change management procedures that provide a consistent approach for controlling and identifying configuration changes for information systems, network devices, and applications.

F.1.7 If mobile devices are used in the delivery of services to Oracle, devices should be managed using centralized solution that has the capability to remotely lock and wipe lost/stolen devices.

## **F.2 Network Security**

F.2.1 Supplier will implement network security infrastructure such as Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS) and other security controls that provide continuous monitoring, have the capability to restrict unauthorized network traffic, detect and limit the impact of attacks.

F.2.2 Network traffic shall be appropriately segregated with routing and access controls separating traffic on internal networks from public or other untrusted networks.

F.2.3 Remote access to the Suppliers network must be approved and restricted to authorized personnel. Remote access must be controlled by secure access control protocols, strong encryption, authentication and authorization.

F.2.4 Where applicable to services provided to Oracle, if VPN access (either site-to-site or IPsec) is used to connect to Oracle networks and information systems, Supplier must segregate computers that remotely connect to Oracle (using either physical segregation or VLAN subnets) to prevent Oracle confidential information, networks and information systems from potentially being accessible or visible by other personnel on the Supplier network.

F.2.5 To the extent permitted by law, Oracle reserves the right to monitor Supplier access to and use of Oracle information systems, networks, and applications.

## **F.3 Logging**

F.3.1 Supplier must maintain logs from information systems, network devices, and applications for a minimum period of ninety (90) days and store log files on a centralized logging server. Logs should be sufficiently detailed in order to assist in the identification of the source of an issue and enable a sequence of events to be recreated.

F.3.2 Logs must record when (date and time), who (such as user or service account) and where (IP address/hostname) for all access and authentication attempts.

F.3.3 Logs must capture information system, network device and application security related event information, alerts, failures, and errors.

F.3.4 Integrity of logs files must be maintained and protected from tampering by restricting access to systems that store log files.

F.3.5 Logs must be continually monitored, reviewed and analyzed for suspicious and unauthorized activity and to verify the integrity of the logging process.

## **F.4 4 Technical Vulnerability and Patch Management**

F.4.1 Supplier must track information from technology vendors and other authoritative sources in relation to technical vulnerabilities of all technology in use, including hardware, operating systems, applications, and network devices; and must promptly evaluate exposure to reported vulnerabilities to ensure that appropriate measures are taken to address risk.

F.4.2 Supplier may only use technology vendors that provide patch updates. Supplier's own procedures must have patch and vulnerability management processes that promptly apply patches to all technology in use including hardware, operating systems, applications and network devices in a consistent, standardized and prioritized manner based upon criticality and risk. If a security patch cannot be promptly applied, then effective risk mitigation controls must be implemented until such time patches can be applied.

F.4.3 Laptop/desktop computers should be configured to automatically receive operating system patches and updates from a centralized service that manages and distributes updates.

F.4.4 Supplier must use endpoint protection, such as anti-virus/malware detection software. This software must be installed, configured, enabled, and updated to prevent, detect and remove malicious code, e.g. malware, viruses, spyware and Trojans. Endpoint protection solutions should detect if the software has been removed, disabled, or is not receiving regular updates.

F.4.5 Automatic virus and malware scanning checks must be carried out on all e-mail attachments that are sent to or received from external sources. Attachments that are identified as containing malicious code must be removed.

## **F.5 Information Backup**

F.5.1 Supplier must ensure that information systems, computers and software involved in the performance of the services provided to Oracle are backed up. Backups must be tested in accordance with operational backup standards.

F.5.2 Oracle confidential information that is stored in backups must be encrypted using AES-256-bit or higher encryption or other strong encryption standard depending on backup method. Where applicable, backups that leave Supplier's facility must be protected against unauthorized access, misuse or corruption during transportation and storage.

## **F.6 Account Management (inclusive of user, systems, and admin)**

F.6.1 Supplier must have account management procedures to support the secure creation, amendment and deletion of accounts on information systems, network devices and applications.

F.6.2 The procedures should include processes for ensuring that information systems, applications, and network device owners authorize all account requests and revoke any unnecessary access based on job role..

F.6.3 Supplier personnel must not share account credentials. All user accounts must be attributable to individuals (i.e. every account will have a unique authentication credential).

## **F.7 Access Controls**

F.7.1 Access controls must be implemented for information systems, networks, and applications that verify the identity of all users and restrict access to authorized users.

F.7.2 Access controls must use a role based access model and differentiate access levels for end-users and privileged access (e.g. systems administrators).

F.7.3 Approvals for access requests must have appropriate segregation of duties, e.g. different personnel must perform the access authorization and access administration roles.

F.7.4 Access lists for information systems, network devices and applications must be reviewed on a regular basis and access removed when no longer required such as personnel job role change or termination.

F.7.5 Access to Oracle information systems, networks, and applications by Supplier personnel is limited to the purposes of performing services, as specified in the agreement.

## **F.8 Password Management**

F.8.1 Account authentication credentials must be unique and not be reused for other accounts.

F.8.2 Password must have no less than a minimum of eight characters for password length and require character complexity (e.g. no dictionary words, use a mix of alpha numeric characters and symbols etc.). Multifactor authentication may be used in Supplier's discretion depending on Services.

F.8.3 Passwords must have a set expiration period that does not exceed twelve months.

F.8.4 Passwords must be distributed separately from account information.

F.8.5 Passwords must be encrypted when transmitted between information systems, network devices and applications.



## **F.9 Protection of Oracle Confidential Information**

F.9.1 Supplier may access, use, and process Oracle confidential information only on behalf of Oracle and only for the purposes specified in the agreement and in compliance with these Standards.

F.9.2 Where Oracle confidential information is stored on Supplier personnel laptop/desktop computers and external electronic media (e.g. USB drives), the media must be fully encrypted using AES-256-bit or higher encryption.

F.9.3 Oracle confidential information may not be stored on mobile devices unless the devices encrypts content stored on the device by default, or the devices and media cards are encrypted using AES-256-bit or higher encryption.

F.9.4 Supplier will delete Oracle confidential information upon Oracle's request, upon completion of services, or upon the termination of services. If required for regulatory retention purposes, by law, or as specified in the agreement, Supplier is permitted to retain one copy of the foregoing materials, as required, provided that any such copy is encrypted, is not used or accessed for any other purpose and is protected in accordance with the requirements of these Standards, and is promptly deletion if no longer required for regulatory retention purposes.

F.9.5 Electronic media that is decommissioned and has been used in the delivery of services to Oracle must be sanitized before disposal or repurposing, using a process that assures data deletion and prevents data from being reconstructed or read, as prescribed in a recognized standard (e.g. NIST SP 800-88). Defective electronic media containing Oracle confidential information must be physically destroyed

F.9.6 Oracle confidential information must be transmitted using encrypted protocols that protect the transfer of information, e.g., SFTP, TLS.

F.9.7 Where services require Oracle confidential information to be exchanged using e-mail, Transport Layer Security (TLS) between Oracle mail gateways and Supplier mail gateways must be used.

F.9.8 Supplier will not permit the use of personal email accounts for exchanging Oracle confidential information.

F.9.9 Supplier must not use Oracle confidential information from production systems for development, testing or staging purposes.

## **PART G: BASELINE PHYSICAL AND ENVIRONMENTAL SECURITY**

### **G.1 Supplier Facilities**

Supplier must maintain the following controls at all Supplier facilities (including third party facilities used by Supplier) from which Oracle networks, information systems and/or confidential information may be accessed.

G.1.1 Supplier must maintain a physical security plan to protect offices and information processing facilities that addresses internal and external threats to sites. Plans must be reviewed and updated on at least an annual basis.

G.1.2 Sites must have secure entry points that restrict access and protect against unauthorized access. Access to all locations must be limited to authorized personnel and approved visitors. All visitors must be required to sign a visitor register. Entry points should have security cameras.

G.1.3 Access areas to information processing facilities should be manned by a security guard. Out of hours access should be monitored, recorded, and controlled. Logs detailing access must be stored for a period of at least 90 days.

G.1.4 Supplier personnel and authorized visitors must be issued identification cards. Visitor identification cards must be distinguishable from Supplier personnel identification cards and must be retrieved and inventoried daily.

G.1.5 Access cards and keys that provide access to secure areas and information processing facilities such as data centers must be monitored and limited to authorized personnel. Regular reviews of access rights must be performed.

G.1.6 Off-site removal of information systems, computers, and network devices must be restricted, approved and authorized by asset owners and appropriate security departments.

G.1.7 Documents that contain Oracle confidential information must be kept in a secure location when not in use.

## G.2 Oracle Facilities

Supplier personnel must abide by the following requirements at Oracle facilities.

G.2.1 Supplier personnel are required to abide by Oracle's security requirements and direction when working at Oracle facilities. The security measures employed at Oracle facilities (e.g., use and placement of security cameras, use and placement of other physical and logical security controls) are Oracle confidential information. Personnel may not photograph or otherwise record Oracle facilities or infrastructure, unless required for the performance of services.

G.2.2 Supplier personnel may not access Oracle computers or networks unless access expressly authorized by Oracle personnel.

## PART H: DEFINITIONS

The following definitions apply to these Standards:

**“agreement”** means, individually or collectively, an agreement, statement of work, or ordering document (as applicable), between Oracle and a Supplier under which (a) Supplier performs services for Oracle and/or (b) Supplier is provided access to Oracle facilities, network(s), information systems and/or confidential information.

**“applications”** means middleware, databases, applications, web portals or other software that are used in the delivery of services to Oracle.

**“computer”** means any desktop or laptop computer, mobile device (e.g., cellular phone, smartphone, tablet), server and/or storage device that (i) is involved in the performance of the services, (ii) may be used to access a network or an environment, or (iii) may access or store confidential information.

**“information systems”** means any system, including but not limited to development, test, stage and production systems, or storage/backup systems, that (a) is involved in the performance of the services, (b) may access, process or store Oracle confidential information.

**“confidential information”** means all Oracle confidential information to which Supplier may be provided access in connection with the performance of services, including without limitation personal information of a customer, employee, partner, or supplier; intellectual property (IP); source code; passwords; non-personal information concerning Oracle's customers, employees, suppliers or partners; any data stored in or provided from the information systems of Oracle or its customers, employees, suppliers, or partners; and any other Oracle confidential information as defined in the agreement.

**“electronic media”** means hard disk, solid state disk, DVD/CD, tape or any other form of media that can store electronic information.

**“facilities”** means any offices, data centers and other locations (whether owned or managed by Oracle, an Oracle customer, Supplier or a third-party) from which Oracle confidential information, information systems or networks may be accessed. References herein to (i) “Oracle facilities” include facilities of Oracle customers, and (ii) “Supplier facilities” include third-party facilities used by Supplier.

**“network”** means any Oracle networks to which Supplier is provided access in connection with the performance of services under the agreement and/or any Supplier networks that are used to access confidential information or information systems.

**“network devices”** means routers, switches, load balancers, firewalls and virtual private network (VPN) devices.

**“personnel”** means all Supplier employees, contractors, sub-contractors, representatives, and agents who are provided access to Oracle facilities, networks, information systems and/or confidential information.

**“personal information”** means any information to which Supplier is provided access that relates to an identified or identifiable individual, including without limitation the individual’s name; address; government identification/national identification number; health, financial or employment information; phone number; e- mail address; IP address.

**“security incident”** means (a) misappropriation or unauthorized access to or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of confidential information, (b) unauthorized access to information systems, or (c) theft, loss or damage to assets.

**“services”** means the work to be performed by Supplier for Oracle as specified in an agreement.

**“Supplier”** means an entity (including its personnel) that performs services under an agreement and granted access to Oracle facilities, networks, information systems and/or confidential information.

**“Supplier facilities”** means all facilities used by Supplier, including third-party facilities.

**SCHEDULE C**

**ORDER FORM #1**

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

**To:** Oliver Auerbach  
**Customer Legal Name:** Oracle Global Services Romania S.R.L.  
**Tax ID:**  
**Billing Address:** Sector 1, No. 246C Calea Floreasca  
Sky Tower Building, Floors 24 to 31, Bucharest, B 014476, RO  
**Sales Rep:** Helen Kruskamp

**Order Form Issued:** September 15, 2022

**Offer Valid Until:** September 30, 2022

**Support Level:** Advanced

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 will govern. Capitalized terms used but not defined in this Order Form have the meanings set forth in the Agreement or in the Documentation.

### 1) Order Form Term

The initial term of this order form is 12 months, after which this order form will automatically renew for successive 12-month 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. Each 12 months of service hereunder will be deemed a "Contract Year".

### 2) Platform Fees

For each Contract Year, Customer will pay Spreedly an "Annual Platform Fee" which entitles Customer to the services set out in the table below.

Approved Enterprise Pricing	
	Year 1
<b>Annual Platform Fee</b>	<b>\$90,000</b>
Enterprise Assurance Agreement & SLAs	Included
Existing Spreedly Endpoints	Unlimited
PCI Compliant Card Storage Limit	Unlimited
Add New Standard PMD Endpoints	Included
Advanced-Tier Support Subscription	Included
<b>API Usage Fee</b>	<b>\$150,000</b>
Committed APIs during initial term	60,000,000
Cost per API call	\$0.0025
<b>Total Annual Fees</b>	<b>\$240,000</b>



**3) API Usage Fees**

In addition to the Annual Platform Fee, Customer is pre-purchasing 60,000,000 API calls for use during the Initial Term at a cost per API call rate of \$0.0025 ("API Usage Fee"). Spreedly will invoice Customer monthly in arrears at the rate of \$0.0025 for any additional API call more than the initial purchase volume of 60,000,000.

**4) Renewal Terms Fees**

Except as otherwise agreed by the Parties in writing, the Annual Platform Fee and API Usage Fee will increase by 6% over the prior Contract Year in each successive Renewal Term.

**5) Support Services**

Upon payment of the applicable fees, Spreedly will provide the technical Support Services in accordance with the Support Service Terms posted at <https://www.spreedly.com/support-services-terms> at the support level specified in this Order Form.

**6) Payments**

All payments are subject to the terms prescribed in Section 7 of the Agreement. Customer will pay the Total Annual Fees of \$240,000 for the first year of the Initial Term in full within 30 days of the Order Form Effective Date. Each subsequent annual payment shall be invoiced 30 days prior to the anniversary Effective Date ("**Annual Renewal Date**") and shall be due and payable 30 days after 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: Webster Bank  
ABA/Routing #: 211170101  
SWIFT Code: WENAUS31  
Beneficiary: 0024760830  
Spreedly, Inc.  
300 Morris Street, Suite 400  
Durham, NC 27701  
USA

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

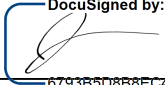
[Signatures on Next Page]



CONFIDENTIAL

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

**Spreedly, Inc.**

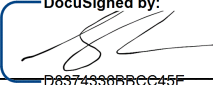
By:    
6793B5D8B8EC48E...

Name: Justin Benson

Title: CEO

Date: 9/30/2022

**Oracle Global Services Romania S.R.L.**

By:    
D8374330BBCC45E...

Name: Simon de Montfort walker

Title: Svp / GM fbgbu

Date: 9/30/2022