salesforce.com, inc.

HOSTED SERVICES AGREEMENT

This HOSTED SERVICES AGREEMENT (this "**Agreement**") is made and entered into as of the Effective Date by and between SFDC and Supplier (each as defined below).

"**SFDC**"	salesforce.com, inc., a Delaware corporation
having its principal place of business at	Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105
"**Supplier**"	Spreedly, Inc., a Delaware corporation
having its principal place of business at	733 Foster Street, Durham, NC 27703
with notices to be delivered to:	Same as above
"**SFDC Terms**"	SFDC Terms and Conditions attached as Exhibit A.

Agreement Terms. This Agreement (which is comprised of the SFDC Terms, and Order Form, Exhibits, or attachments hereto) constitutes the entire agreement between the Parties with respect to the subject matter herein, supersedes all prior agreements, whether written or oral, and supersedes and merges all prior discussions between the Parties. This Agreement is in lieu of, and supersedes, any click-through license, online license electronically accepted by End Users, or other non-negotiable agreement related to the Services, which shall be void and of no effect between the Parties.

IN WITNESS WHEREOF, the Parties have executed this Agreement through their authorized representatives.

SPREEDLY, INC. (SUPPLIER)		**SALESFORCE.COM, INC. (SFDC)**	
By:	DocuSigned by: Justin Benson 9624ED07D136401...	By:	DocuSigned by: Brian Mckinney 0E04F18CF01B4F1...
Name:	Justin Benson	Name:	Brian McKinney
Title:	CEO	Title:	Sr. Director - Strategic Sourcing
Date:	January 16, 2020 | 08:47 PST	Date:	January 16, 2020 | 11:35 PST ("**Effective Date**")

EXHIBIT A

SFDC Terms and Conditions

1. **Definitions**. Capitalized terms used in this Agreement are defined in this section or in the section of this Agreement where they are first used.

1.1 "**Affiliate**" means, with respect to any entity, any other present or future entity Controlling, Controlled by, or under common Control with such entity. "**Control**" for purposes of this definition means direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the subject entity.

1.2 "**Customer Data**" means all electronic data or information submitted by or for SFDC to the Services.

1.3 **"Intellectual Property**" means all algorithms, application programming interfaces (APIs), apparatus, concepts, Confidential Information, data, databases and data collections, deliverables, designs, diagrams, documentation, drawings, flow charts, formulae, ideas and inventions (whether or not patentable or reduced to practice), know-how, materials, marketing and development plans, marks (including brand names, product names, logos and slogans), methods, models, procedures, processes, schematics, software code, specifications, subroutines, techniques, tools, uniform resource identifiers, user interfaces, works of authorship, and other forms of technology.

1.4 **"Intellectual Property Rights**" means all past, present, and future rights of the following types, which may exist or be created under the laws of any jurisdiction in the world: (i) rights associated with works of authorship, including exclusive exploitation rights, copyrights, moral rights, and mask work rights; (ii) trademark and trade name rights and similar rights; (iii) trade secret rights; (iv) patent and industrial property rights; (v) other proprietary rights in Intellectual Property of every kind and nature; and (vi) rights in or relating to registrations, renewals, extensions, combinations, divisions, and reissues of, and applications for, any of the rights referred to in clauses (i) through (v) of this sentence.

1.5 "**Malicious Code**" means viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs.

1.6 **"Order Form"** means a document that memorializes an order placed by SFDC with Supplier for the Services. The terms of the initial Order Form are attached hereto as Exhibit B (the "**Initial Order Form**").

1.7 "**Party**" means SFDC and Supplier individually, and both may be referred to collectively as the "**Parties**."

1.8 "**Payment Information**" means payment card information submitted to Supplier and processed by Supplier in connection with the Services, whether in tokenized or non-tokenized form.

1.9 "**Services**" means the online, Web-based applications provided by Supplier that are ordered by SFDC under an Order Form, including associated offline components and Third Party Applications. Services, offline components, and Third Party Applications are accessed as web-based applications unless specifically or otherwise set forth in an Order form.

1.10 "**SFDC**" means SFDC and its Affiliates.

1.11 "**Specification**" means the documentation and/or (online or offline) user guide for the Services, available via docs.spreedly.com, as updated from time to time.

1.12 "**Third-Party Applications**" means online, Web-based applications and offline software products comprising the Services that are provided by third parties (not the Supplier) and interoperate with and/or are incorporated into the Services.

1.13 "**Users**" means individuals who are authorized by SFDC to use the Services, for whom subscriptions to a Service have been purchased, and/or who have been supplied user identifications and passwords by SFDC (or by Supplier at SFDC's request). Users may include but are not limited to employees, consultants, contractors and agents of SFDC, or third parties with whom SFDC transacts business.

2. **Services**.

2.1 **Provision of Services**. Supplier shall make the Services available to SFDC pursuant to this Agreement and the applicable Order Forms during each subscription term.

2.2 **User Subscriptions**. Unless otherwise specified in the applicable Order Form, (i) Services are purchased as User subscriptions and may be accessed by no more than the specified number of Users, (ii) additional User subscriptions may be added during the subscription term at the same pricing as that for the pre-existing subscriptions, prorated for the remainder of the subscription term in effect at the time the additional User subscriptions are added, and (iii) the added User subscriptions shall terminate on the same date as the pre-existing User subscriptions. User subscriptions are for designated Users and cannot be shared or used by more than one User, but may be reassigned to new Users replacing former Users who no longer require ongoing use of the Services.

2.3 **Supplier Responsibilities**. Supplier shall (i) make the Services available in accordance with the warranties specified in Section 7, and (ii) provide the Services only in accordance with applicable laws and government regulations. Supplier shall remain responsible for the performance of Supplier's personnel (including employees, agents, and contractors) and their compliance with Supplier's obligations under this Agreement.

2.4 **SFDC Responsibilities**. SFDC shall (i) be responsible for Users' compliance with this Agreement, (ii) be solely responsible for the accuracy, quality, integrity and legality of Customer Data and of the means by which it acquired Customer Data, (iii) use commercially reasonable efforts to prevent unauthorized access to, or use of, the Services, and notify Supplier promptly of any such unauthorized access or use, and (iv) use the Services only in accordance with the Specification and applicable laws and government regulations. SFDC shall not (a) make the Services available to any third party other than Users, (b) use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights, (d) use the Services to store or transmit Malicious Code, (e) knowingly interfere with or disrupt the integrity or performance of the Services or third-party data contained therein, or (f) attempt to gain unauthorized access to the Services or their related systems or networks.

3. Third-Party Suppliers.

3.1 **Third-Party Products and Services**. If Supplier offers Third-Party Applications for sale under Order Forms in any way, any purchase of such Third-Party Applications by SFDC shall be subject only to the additional terms for such Third-Party Applications specified in such Order Forms (the "**Third-Party Application Terms**"). Any provision by Supplier of third-party products or services, including but not limited to Third-Party Applications and implementation, customization and other consulting services, and any exchange of data between Supplier and any third-party provider, is solely between Supplier and the applicable third-party provider unless specifically set forth on the applicable Order Form; *provided, however,* that SFDC shall be a deemed third party beneficiary of such agreements between Supplier and any third-party provider. Notwithstanding anything to the contrary set forth in this Agreement, Supplier does not make any representations or warranties with respect to any Third-Party Applications.

3.2 **Third-Party Applications and Customer Data**. Supplier shall not allow providers of those Third-Party Applications to access Customer Data or Payment Information except as required for the interoperation of such Third-Party Applications with the Services and as specifically set forth in the Specifications. Supplier shall be responsible for any disclosure, modification or deletion of Customer Data or Payment Information resulting from any such access by Third-Party Application providers. The Services shall allow SFDC to restrict such access by restricting Users from installing or enabling such Third-Party Applications for use with the Services.

4. Fees and Payment.

4.1 **User Fees**. SFDC shall pay only those fees specified in all Order Forms hereunder. Except as otherwise specified herein or in an Order Form, (i) fees are quoted and payable in United States dollars, (ii) fees are based on Services purchased and not actual usage and (iii) fees are non-refundable. Fees for the Services are based on periods that begin and end on the dates set forth in an Order Form.

4.2 **Professional Services/Additional Support Fees**. Supplier shall provide to SFDC basic support for the Services at no additional charge, and/or upgraded support if purchased ("**Support Services**"), provided that the terms of such upgraded support are described in the Order Form. If applicable, fees for consulting and other professional services shall be outlined in a separately executed agreement between the Parties.

4.3 **Price Increases**. The fees specified in the Initial Order Form shall not be increased during the "Initial Term" thereof.

4.4 **Payment Terms**. Supplier shall be paid in accordance with the payment method set out in the applicable Order Form. Unless otherwise provided in the relevant Order Form, (i) Supplier shall invoice SFDC monthly; and (ii) invoiced amounts for which no due date is otherwise established will be due and payable within sixty (60) days from receipt of an undisputed invoice. An acceptable invoice shall be an email sent to Invoices_NAM@salesforce.com or an invoice submitted via facsimile to (866) 257-9210 including, without limitation, the purchase order number, and a description of the items, quantities, and unit prices for all Services invoiced. Invoices submitted without a valid purchase order number or for goods or services exceeding funding authorized on the valid purchase order will be returned to Supplier for resubmission. Processing of invoices submitted more than ninety (90) days after SFDC's receipt of Services may be substantially delayed. Notwithstanding anything to the contrary contained in this Agreement, (a) invoices submitted more than six (6) months after SFDC's receipt of Services will be rejected and no payment shall be made and (b) SFDC shall have no liability whatsoever under this Agreement for amounts due under any such invoice. Invoices will be deemed paid when payment is mailed or delivered to a recognized overnight carrier. All payments will be made in U.S. dollars.

4.5 **Credit Card Payments**. Any and all payments made by credit card under this Agreement or any Order Forms shall be deemed payments made by SFDC regardless of the name of the card holder making the payment. Credit card payments are distinctive from Payment Information defined above.

4.6 **Disputed Payments**. SFDC may, upon notice to Supplier setting forth the nature of the dispute, withhold payment of amounts it disputes in good faith. If an entire invoice or any portion thereof is contested and then later approved by SFDC, SFDC will have forty (40) days after the approval date in which to pay the contested invoice, or portion thereof.

4.7 **Expenses**. Supplier will not be entitled to be reimbursed for travel, living or other expenses incurred in the performance of this Agreement unless expressly authorized in the Order Form. If expense reimbursement is authorized, it will be made in accordance with SFDC's Non-Employee Travel & Expense policy, available upon request.

4.8 **Taxes**. Unless otherwise stated, Supplier's fees do not include any taxes, levies, duties or similar governmental assessments of any nature, including but not limited to value-added, sales and use, or withholding taxes, assessable by any local, state, provincial, federal or foreign jurisdiction (collectively, "**Taxes**"). SFDC is responsible for paying all Taxes associated with its purchases hereunder. If Supplier has the legal obligation to pay or collect Taxes for which SFDC is responsible under this paragraph, the appropriate amount shall be invoiced to and paid by SFDC, unless SFDC provides Supplier with a valid tax exemption certificate authorized by the appropriate taxing authority. For clarity, Supplier is solely responsible for taxes assessable against it based on its income, property and employees. Where salesforce.com India Private Limited is the Salesforce Affiliate executing this Agreement, Supplier: (i) represents that it maintains an Indian Goods and Service Tax ("GST") number; (ii) will provide a copy of its GST certificate to SFDC upon execution of the Agreement; (iii) agrees to pay timely all associated GST to the Indian Tax Office; and (iv) will reimburse SFDC for all taxes, expenses, penalties, and other costs incurred by SFDC as a result Supplier's failure to perform any of the actions described in (i)-(iii).

5. Proprietary Rights.

5.1 **Reservation of Rights**. Subject to the limited rights expressly granted hereunder, Supplier reserves all rights, title and interest in and to the Services, including all related Intellectual Property Rights. No rights are granted to SFDC hereunder other than as expressly set forth herein.

5.2 **License by Supplier to Use Feedback**. SFDC hereby grants to Supplier and its Affiliates a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into the Services any suggestion, enhancement request, recommendation, correction, or other feedback provided by SFDC or its Affiliates relating to the operation of the Services.

5.3 **Ownership of Customer Data and Payment Information**. As between Supplier and SFDC, SFDC exclusively owns all rights, title and interest in and to all Customer Data and Payment Information.

6. Confidentiality.

6.1 **Definition of Confidential Information**. As used herein, "**Confidential Information**" means all confidential and proprietary information disclosed by a Party ("**Disclosing Party**") to the other Party ("**Receiving Party**"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information of SFDC shall include Customer Data and Payment Information, Confidential Information of Supplier shall include the Services, and Confidential Information of each Party shall include the terms and conditions of this Agreement (and all Exhibits and attachments hereto) as well as business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such Party. However, Confidential Information (other than Customer Data and Payment Information) shall not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was lawfully known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is lawfully received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party without use of, or reliance upon, the Disclosing Party's Confidential Information.

6.2 **Protection of Confidential Information**. Except as otherwise permitted in writing by the Disclosing Party, the Receiving Party shall: (i) use the same degree of care to protect Confidential Information that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care), (ii) not disclose or use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, and (iii) limit access to Confidential Information of the Disclosing Party to those of its employees, contractors and agents who need such access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections no less stringent than those herein. Additionally, Supplier shall provide prompt notification to SFDC of any unauthorized access to or disclosure of the Disclosing Party's Confidential Information.

6.3 **Protection of Customer Data and Payment Information**. Without limiting the above, Supplier shall maintain appropriate administrative, physical, and technical safeguards for protection of the privacy, security, confidentiality and integrity of Customer Data and Payment Information (including but not limited to those protections applicable to Services set forth in the Supplier Security Exhibit attached as Exhibit D, and the Supplier Privacy Exhibit attached as Exhibit E). Supplier shall not (i) modify Customer Data or Payment Information, (ii) disclose Customer Data or Payment Information except as compelled by law in accordance with Section 6.4 below or as expressly permitted in writing by SFDC, or (iii) access or use Customer Data or Payment Information except to prevent or address service or technical problems, or at SFDC's request in connection with customer support matters.

6.4 **Compelled Disclosure**. If the Receiving Party is compelled by law or any listing or trading arrangement concerning its publicly-traded securities to disclose Confidential Information of the Disclosing Party, it shall provide the Disclosing Party with prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to such Confidential Information.

6.5 **Remedies**. If the Receiving Party discloses or uses (or threatens to disclose or use) any Confidential Information of the Disclosing Party in breach of confidentiality protections hereunder, the Disclosing Party shall have the right, in addition to any other remedies available to it, to seek injunctive relief to enjoin such acts, it being specifically acknowledged by the Parties that any other available remedies are inadequate.

6.6 **Return of Materials**. Upon termination of this Agreement or Order Form, or at the request of a Disclosing Party at any time during or after this Agreement, the Receiving Party will deliver to the Disclosing Party or destroy and certify destruction (at the Disclosing Party's election and in the manner designated by the Disclosing Party) all of the Disclosing Party's Confidential Information.

6.7 **No Publicity; Use of SFDC Logo or Trademarks**. Supplier agrees not to issue any press release or make any public statement relating to the subject matter of this Agreement (including naming SFDC as a customer of Supplier) without the prior written consent of SFDC. Any references to SFDC or use of any SFDC logo, brand or trademark (whether publicly, in connection with the Services, or otherwise) are prohibited without SFDC's prior written approval.

7. Warranties.

7.1 **General Warranties**. Each Party represents and warrants that: (i) it is duly organized and validly existing under the laws of its state of organization and has full right, power, and authority to enter into and perform its obligations under this Agreement; (ii) it is not and will not be bound by any agreement, nor has it assumed or will it assume, any obligation, which would in any way be inconsistent with or breached by its performance of its obligations under this Agreement; (iii) it has obtained all necessary licenses, permits, and other requisite authorizations, has taken all actions required by applicable laws or governmental regulations in connection with its business as now conducted and its ability to perform its obligations under this Agreement; and (iv) it has complied with or will comply with all applicable international, federal, state, local laws and ordinances now or hereafter enacted, including data protection and privacy laws.

7.2 **Performance Warranty**. Supplier warrants that (i) the Services shall perform materially in accordance with the Specifications and the Service Levels specified in Exhibit C; *provided, however,* that the remedies specified in Exhibit C shall constitute SFDC's sole and exclusive remedies for any non-compliance with the Service Levels specified in Exhibit C, and (ii) the functionality of the Services will not be materially decreased during the term of this Agreement.

7.3 **No Malicious Code**. Supplier represents and warrants that the Services shall not transmit or include any Malicious Code or any feature or function that may enable Supplier or any third party to erase, destroy, corrupt or modify any Customer Data or Payment Information without the consent of SFDC. This Section 7.3 shall survive for 30 days post-termination of this Agreement.

7.4 **Remediation of Vulnerabilities**. Each party acknowledges that SFDC's security organization has identified and notified Supplier in writing of certain potential security issues found within the Services (the "Vulnerabilities"). Supplier shall remediate and correct (in SFDC's sole discretion) all Vulnerabilities in accordance with the dates set forth in the Security Remediation Plan defined in Exhibit F. Supplier also agrees to comply with the Vulnerability Remediation SLA, defined in Exhibit G, for remediation of any security issue found during the term of the Agreement.

7.5 **Disclaimer**. EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY MAKES ANY WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

8. Indemnification.

8.1 **Supplier Indemnities**. Supplier will indemnify, defend, and hold harmless SFDC and its Affiliates, and each of their officers, directors, employees and agents (the "**SFDC Indemnitees**") from and against all third party claims, demands, suits, causes of action, awards, judgments and liabilities, including reasonable attorneys' fees and costs (collectively "**Claims**") arising out of or alleged to have arisen out of: (a) any allegation that the Services infringe, misappropriate or violate any Intellectual Property Rights of a third party (each, a "**Services Infringement Claim**"); (b) any violation by Supplier of applicable law; (c) any unauthorized access to, or use of, Customer Data or Payment Information caused by Supplier's breach of its confidentiality obligations under Section 6; (d) Supplier's willful misconduct or grossly negligent acts or omissions; and (e) death or injury to persons (including, but not limited to Claims related to discrimination, slander or libel, or sexual harassment), or damage to, or loss or destruction of, any real or tangible personal property, in each case to the extent proximately caused by the negligent acts or omissions of Supplier, its employees, subcontractors, vendors, agents and/or invitees.

Notwithstanding the foregoing, Supplier's obligations under this Section 8.1 do not apply to the extent the applicable Claim arises from (a) a Third-Party Application that is subject to applicable Third-Party Application Terms, (b) any SFDC Indemnitees' breach of this Agreement (including any applicable Order Form), or (c) any modification of the Services by SFDC or any of its employees, agents, representatives or contractors, unless such modification was performed in accordance with written instructions provided by authorized Supplier personnel.

8.2 **SFDC Indemnities**. SFDC will indemnify, defend, and hold harmless Supplier and its affiliates, and each of their officers, directors, employees and agents (the "**Supplier Indemnitees**") from and against all Claims arising out of or alleged to have arisen out of any allegation that the Customer Data and/or Payment Information infringes, misappropriates or violates any Intellectual Property Rights of a third party.

Notwithstanding the foregoing, SFDC's obligations under this Section 8.2 do not apply to the extent the applicable Claim arises from (a) any Supplier Indemnitees' breach of this Agreement (including any applicable Order Form), or (b) any modification of the Customer Data or Payment Information, as applicable, by any Supplier or any of its employees, agents, representatives or contractors, unless such modification was performed in accordance with written instructions provided by authorized SFDC personnel.

8.3 **Tender**. Whenever a Party believes it is entitled to indemnification hereunder (in such capacity, the "**Indemnitee**") with respect to a Claim, the Indemnitee shall promptly notify the other Party (in such capacity, the "**Indemnitor**") of such Claim (it being understood that the Indemnitee's failure to provide such notice promptly will not relieve Supplier of its obligation to defend such Claim as long as its ability to defend the Claim was not materially prejudiced by such failure) and the Indemnitee shall tender sole control of the defense and settlement of the Claim to the Indemnitor. If the Indemnitor assumes the defense of a Claim, it will thereafter be presumed that the Claim is within the scope of the indemnification provisions in this section and the Indemnitee will cooperate with the Indemnitor, as the Indemnitor may reasonably request and at the Indemnitor's expense, in the defense of the Claim.

8.4 **Settlement**. The Indemnitor, at its expense, shall have the right to pay, compromise, settle or otherwise dispose of any Claim, however, no settlement of any Claim against the Indemnitee will be binding on the Indemnitee without the Indemnitee's prior written consent, unless such settlement (i) includes the delivery by the settling third party of a full and final release of the SFDC Indemnitees or Supplier Indemnitees, as applicable, from any and all liability with respect to such Claim, or (ii) requires any payment to be made by the Indemnitee.

8.5 **Infringement**. If any Service becomes, or in the reasonable opinion of Supplier is likely to become, the subject of an infringement or misappropriation claim, Supplier will, in addition to indemnifying the SFDC Indemnitees as provided in this Section , at Supplier's expense perform one of the following: (i) secure the right for SFDC and its Affiliates to continue using the Service or (ii) replace or modify the infringing Service to make it non-infringing, *provided* that any such replacement or modification will not materially degrade the performance or quality of the affected Service, or (iii) if Supplier determines that the remedies specified in clauses (i) and (ii) are not commercially reasonable, Supplier may require SFDC to stop using the Service, in which case Supplier may terminate SFDC's right to use such Service upon thirty (30) days' written notice and refund SFDC any prepaid fees covering the remainder of the term of the terminated Service. Supplier's obligations under Section 8.1 and this Section 8.5 constitute Supplier's sole and exclusive obligations, and SFDC's sole and exclusive remedies with respect to all Services Infringement Claims.

9. Limitation of Liability.

9.1 **General Limitation of Liability**. EXCEPT AS SET FORTH IN SECTION 9.2, TO THE EXTENT PERMITTED BY LAW, EXCEPT FOR (A) EITHER PARTY'S INDEMNIFICATION OBLIGATIONS (EXCLUDING THE INDEMNIFICATION OBLIGATION UNDER SECTION 8.1(C), WHICH SHALL BE SUBJECT TO THE SUPER LIABILITY CAP DESCRIBED IN SECTION 9.2), (B) A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, (C) EITHER PARTY'S VIOLATION OF APPLICABLE LAW, AND/OR (D) LIABILITIES THAT CANNOT BE CAPPED AS A MATTER OF APPLICABLE LAW (9.1(A) THROUGH (D), COLLECTIVELY, "**EXCLUDED LIABILITIES**"), IN NO EVENT SHALL EITHER PARTY'S LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, IN THE AGGREGATE, EXCEED THE GREATER OF: (I) TWO TIMES (2X) THE TOTAL AMOUNT PAID BY SFDC IN THE TWELVE MONTHS PRECEDING THE INCIDENT GIVING RISE TO LIABILITY AND (II) $500,000 (the "**General Liability Cap**").

9.2 **Super Liability Cap for Breach of Confidentiality**. EACH PARTY'S AGGREGATE LIABILITY FOR ALL TYPES OF DAMAGES RESULTING FROM A BREACH OF CONFIDENTIALITY, REGARDLESS OF THE TYPE OF CONFIDENTIAL INFORMATION INVOLVED AND INCLUDING CUSTOMER DATA, INCLUDING THE COST TO DEFEND THIRD PARTY CLAIMS CAUSED BY SUCH BREACH OF CONFIDENTIALITY, HOWEVER CAUSED, AND REGARDLESS OF THE LEGAL THEORY UPON WHICH THE CLAIM IS BASED, SHALL NOT EXCEED FOUR MILLION DOLLARS ($4,000,000) (THE "**SUPER LIABILITY CAP**"). FOR AVOIDANCE OF DOUBT, THE SUPER LIABILITY CAP SHALL BE IN LIEU OF, AND NOT IN ADDITION TO, THE GENERAL LIABILITY CAP AND SHALL APPLY SOLELY TO THE CLAIMS DESCRIBED UNDER THIS SECTION 9.2.

9.3 **Exclusion of Consequential and Related Damages**. TO THE EXTENT PERMITTED BY LAW, EXCEPT FOR THE EXCLUDED LIABILITIES, IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FOR CLARITY, ANY DAMAGES AWARDED AGAINST EITHER PARTY BASED ON A CLAIM SUBJECT TO INDEMNIFICATION UNDER SECTION 8 SHALL BE CONSIDERED DIRECT DAMAGES, NOTWITHSTANDING A DIFFERENT CLASSIFICATION (E.G., CONSEQUENTIAL, INDIRECT, ETC.) IN THE AWARD, AND SHALL THEREFORE BE EXCLUDED FROM THE LIMITATIONS IN THIS SECTION 9.2.

10. Term and Termination.

10.1 **Term of Agreement**. This Agreement commences on the Effective Date and continues for the period(s) specified in the applicable Order Forms. For avoidance of doubt, if there are no outstanding Order Forms this Agreement shall automatically terminate.

10.2 **Termination for Cause**. A Party may terminate this Agreement for cause (i) upon thirty (30) days' written notice to the other Party of a material breach of this Agreement if such breach remains uncured at the expiration of such period, or (ii) if the other Party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. The parties further acknowledge and agree that in the event Supplier does not obtain both ISO27001 and SOC2 certifications by December 31, 2021, SFDC shall have the right to immediately terminate this Agreement upon written notice.

10.3 **Refund or Payment upon Termination for Cause**. Upon termination of this Agreement by SFDC pursuant to Section 10.2, Supplier shall refund SFDC any prepaid fees covering the remainder of the term of all subscriptions after the effective date of termination. Should SFDC terminate this Agreement as a result of Supplier failing to remediate the Vulnerabilities as described in the Security Remediation Plan (Exhibit F), as SFDC's sole and exclusive remedy, Supplier shall provide SFDC with a refund of any and all fees paid for the Services and SFDC shall cease all use of the Services.

10.4 **Return of Customer Data and Payment Information**. Promptly upon request by SFDC made within ninety (90) days after the effective date of termination, Supplier will make available to SFDC for download a file of Customer Data and Payment Information stored in the Services in comma separated value (.csv) format along with attachments in their native format. After such 90-day period, Supplier shall, unless legally prohibited, delete all Customer Data and Payment Information in systems or otherwise in its possession or under its control and certify destruction of the same in writing.

10.5 **Transition Services**. Following any termination of this Agreement, upon SFDC's request made 30 or more days before the effective date of the expiration or termination, Supplier shall continue to provide the Services for a period up to 12 months after the applicable expiration or termination date (the "**Transition Period**"). The terms during any Transition Period shall be the same as those that applied immediately prior to the termination date (i.e., under all of the terms of the Agreement), except that the price of the subscriptions will increase by 3% over the prices applicable to those subscriptions immediately preceding the Transition Period.

10.6 **Surviving Provisions**. Sections 1 (Definitions), 4 (Fees and Payment), 5 (Proprietary Rights), 6 (Confidentiality), 7.1 (General Warranties), 7.3 (Malicious Code), 7.5 (Disclaimer), 8 (Indemnification), 9 (Limitation of Liability), 10.3 (Refund or Payment upon Termination), 10.4 (Return of Customer Data and Payment Information), 10.5 (Transition Services), 10.6 (Surviving Provisions), 11 (Compliance with Laws), 12 (Insurance) and 13 (General Provisions) shall survive any termination or expiration of this Agreement.

11. Compliance with Laws.

11.1 **Export Administration Regulations**. Each Party shall comply with the export laws and regulations of the United States and other applicable jurisdictions in providing and using the goods, services and deliverable furnished under this Agreement. Without limiting the foregoing, (i) each Party represents that it is not named on any U.S. government list of persons or entities prohibited from receiving exports, and (ii) Supplier shall not permit any individual to access or use information provided by SFDC in violation of any U.S. export embargo, prohibition or restriction.

11.2 **Immigration**. Supplier agrees that it will comply with the provisions of the Immigration Reform and Control Act ("IRCA"), and will assign to SFDC only personnel who are authorized to work in the United States.

11.3 **Equal Opportunity**. Supplier represents and warrants that it will not discriminate against any employee or applicant for employment because of race, color, religion, disability, sex, national origin, age, physical or mental disability, veteran status, or any other unlawful criterion and that it shall comply with all applicable laws against discrimination and all applicable rules, regulations and orders issued thereunder or in implementation thereof including, but not limited to, Executive Order 11246. Supplier further warrants that it shall comply with all applicable provisions of the Americans with Disabilities Act ("ADA").

11.4 **Anti-Corruption**. It is the intent of the parties that no payments or transfers of anything of value shall be made which have the purpose or effect of public or commercial bribery, acceptance of or acquiescence in extortion, kickbacks, or other unlawful or improper means of obtaining business or any improper advantage. Supplier represents and warrants that it shall comply with all international anti-corruption laws, such as the Foreign Corrupt Practices Act 15 U.S.C. § 78dd-1, *et seq*. and that, with respect to Supplier's performance of any of its activities hereunder:

11.4.1 No portion of any fees paid or payable by SFDC to Supplier will be paid to, or accrued directly or indirectly for the benefit of, any person, firm, corporation or other entity other than Supplier.

11.4.2 Supplier has not, and will not at any time, directly or indirectly, pay, offer, authorize or promise to pay, offer, or authorize the payment of, any monies or any other thing of value to: (i) any officer or employee of any government, department, agency or instrumentality thereof; (ii) any other person acting in an official capacity for or on behalf of any government, department, agency or instrumentality thereof; (iii) any political party or any official or employee thereof; (iv) any candidate for political office; (v) any other person, firm, corporation or other entity at the suggestion, request or direction of, or for the benefit of, any government officer or employee, political party or official or employee thereof, or candidate for political office; or (vi) any other person, firm, corporation or other entity with knowledge that some or all of those monies or other thing of value will be paid over to any officer or employee of any government department, agency or instrumentality, political party or officer or employee thereof, or candidate for political office.

12. Insurance.

12.1 **Required Policies**. Supplier shall, at its own cost and expense, maintain the following insurance during the term of this Agreement. Supplier shall cause each of its agents, independent contractors and subcontractors performing any services hereunder to maintain appropriate limits of the same insurance at its sole cost and expense:

a) Workers' Compensation (or locally applicable social scheme) as required by law where work is performed. Coverage to include waiver of subrogation in favor of SFDC for any services performed on a SFDC location.

b) Commercial General (or Public) Liability insurance including Products, Completed Operations Liability, Personal Injury, Contractual Liability and Broad Form Property Damage Liability coverage for bodily injury (including death) or damages to any property of not less than US$2,000,000 per occurrence. "Salesforce.com, its subsidiaries, officers, directors and employees" shall be noted on the policy as an additional insured.

c) Professional Liability (or Professional Indemnity)/Errors and Omissions Liability Insurance in an amount not less than US$5,000,000 per claim. Such insurance shall cover any and all acts, errors, omissions or negligence in the delivery of products and services under this Agreement. The Professional Liability Insurance retroactive coverage date shall be no later than the Effective Date of this Agreement. If such coverage is written on claims made basis, Supplier shall maintain coverage for a period of up to three (3) years following the termination of Services provided under this Agreement.

If Supplier is providing software, software development, software as a service or any technology services and products, then such Errors and Omissions insurance shall include coverage for Network Security and Privacy and Media Liability including but not limited to malicious code, unauthorized use or access, failure of security, invasion of privacy, wrongful disclosure of data, other negligence in handling of confidential information and infringement of Intellectual Property (except patent infringement).

d) Employee Dishonesty/Crime insurance covering the fraudulent or dishonest acts of Supplier's employees and agents, acting alone or in collusion with others, and including third party property coverage and computer crime coverage, with limits of not less than $1,000,000 per occurrence if Supplier has unescorted access to SFDC's facilities and/or access to SFDC's assets and internal systems.

e) Property Insurance. If Supplier is using its own property or the property of SFDC in connection with the performance of its obligations under this Agreement, then Property Insurance on an All Risk basis with replacement cost coverage for property and equipment of others in the care, custody, and control of Supplier is required.

12.2 **Additional Requirements**. The above insurance limits may be achieved by a combination of primary and follow form excess policies. All insurance coverages required hereunder shall be procured from insurers with a current A.M Best rating of not less than A- VII (or local equivalent). Where permitted by law, such policies shall contain a waiver of subrogation in favor of SFDC. General Liability and Automobile Liability above shall contain provisions stating they are primary and non-contributory with any insurance SFDC maintains. Any deductible (excess) or self-insured retention in case of an insured event shall be solely borne by the Supplier. The insurance coverage described in this section shall not limit the extent of Supplier's responsibilities and liabilities specified within this Agreement or by law.

12.3 **Evidence of Insurance**. If requested by SFDC, certificates of insurance evidencing the required coverage shall be furnished and shall evidence that the insurance carriers will provide notice of cancellation or reduction in such coverage in accordance with policy provisions. SFDC's failure to request certificates of insurance shall not relieve Supplier from the responsibility to maintain the specified insurance coverage.

13. General Provisions.

13.1 **Relationship of the Parties**. The Parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the Parties.

13.2 **No Third-Party Beneficiaries**. There are no third-party beneficiaries to this Agreement.

13.3 **Non-Restrictive Relationship**. Nothing in this Agreement shall be construed so as to preclude SFDC from developing, acquiring, marketing or providing products or services that may perform the same or similar functions as the Services.

13.4 **Notices**. Except as otherwise specified in this Agreement, all notices, permissions and approvals hereunder shall be in writing and shall be deemed to have been given upon: (i) personal delivery, (ii) the second business day after mailing, (iii) the second business day after sending by confirmed facsimile, or (iv), except for notices of breach, termination or an indemnifiable claim ("**Legal Notices**"), the first business day after sending by email. Notices to SFDC shall be addressed to the attention of its SVP, GCSS, with a copy to its General Counsel. All service-related notices to SFDC shall be addressed to the relevant Service system administrator designated by SFDC. Billing-related notices to SFDC shall also be addressed to accountspayable@salesforce.com. Legal Notices to Supplier shall also be addressed to Supplier's signatory of this Agreement.

13.5 **Waiver and Cumulative Remedies**. No failure or delay by either Party in exercising any right under this Agreement shall constitute a waiver of that right. Other than as expressly stated herein, the remedies provided herein are in addition to, and not exclusive of, any other remedies of a Party at law or in equity.

13.6 **Severability**. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in effect.

13.7 **Assignment**. Neither Party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of the other Party (not to be unreasonably withheld). Notwithstanding the foregoing, either Party may assign this Agreement in its entirety (including Order Form), without consent of the other Party, to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of Supplier. A Party's sole remedy for any purported assignment by the other Party in breach of this paragraph shall be, at the non-assigning Party's election, termination of this Agreement upon written notice to the assigning Party; provided, however, that in the event of such a termination by SFDC, Supplier shall also refund SFDC any prepaid fees covering the remainder of the term of all subscriptions after the effective date of termination. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the Parties, their respective successors and permitted assigns.

13.8 **Disputes**. If a dispute should arise between the Parties relating to the Agreement, the Parties shall promptly hold a meeting, attended by persons with decision-making authority regarding the dispute, in an attempt in good faith to negotiate a resolution of the dispute; provided, however, that no such meeting shall be deemed to vitiate or reduce the obligations and liabilities of the Parties or be deemed a waiver by either Party hereto of any remedies to which such Party would otherwise be entitled. If the dispute is not resolved within thirty (30) days after the commencement of negotiations, or if no negotiations are commenced within sixty (60) days after one Party notifies the other Party of such dispute, then either Party may initiate litigation per the terms of this Agreement.

13.9 **Governing Law**. This Agreement, and any disputes arising out of or related hereto, shall be governed exclusively by the internal laws of the State of California, without regard to its conflicts of laws rules or the Uniform Computer Information Transactions Act or United Nations Convention on the International Sale of Goods.

13.10 **Venue; Waiver of Jury Trial**. The state and federal courts located in New York, New York shall have exclusive jurisdiction to adjudicate a dispute arising out of or relating to this Agreement. Each Party hereby consents to the exclusive jurisdiction of such courts. To the extent permitted by applicable law, each Party also hereby waives any right to jury trial in connection with any action or litigation in any way arising out of or related to this Agreement.

13.11 **Entire Agreement**. This Agreement, including all exhibits and addenda hereto and Order Form, constitutes the entire agreement between the Parties and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. Without limiting the foregoing, this Agreement supersedes the terms of any online Master Subscription Agreement electronically accepted by SFDC. No modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and signed by the party against whom the modification, amendment or waiver is to be asserted. However, to the extent of any conflict or inconsistency between the provisions in the body of this Agreement and any exhibit or addendum hereto or any Order Form, the terms of such exhibit, addendum or Order Form shall prevail. Notwithstanding any language to the contrary therein, no terms or conditions stated in a SFDC purchase order or in any other SFDC order documentation (excluding Order Form) shall be incorporated into or form any part of this Agreement, and all such terms or conditions shall be null and void.

13.12 **Counterparts**. This Agreement may be executed by electronically (e.g., Docusign, exchange of executed PDFs via e-mail), facsimile and in counterparts, which taken together shall form one legal instrument.

EXHIBIT B

INITIAL ORDER FORM

See attached

EXHIBIT C

SERVICE LEVEL AGREEMENT

1. **Availability**. Supplier shall make the Services available 99.9% of the time, except as provided below. Availability will be calculated per calendar quarter, as follows: total *minus* nonexcluded *minus* exclude *divided by* (total *minus* excluded) *then multiplied by* 100

   Where:

   - *total* means the total number of minutes in the calendar month;
   - *nonexcluded* means downtime that is not *excluded*; and
   - *excluded* means:
     - Any planned downtime of which Supplier gives 24 or more hours' notice in accordance with the Agreement or via a conspicuous on-screen message in the Services. Planned downtime shall not exceed 60 minutes individually or 24 hours in aggregate during a calendar month. Supplier shall schedule planned downtime during the hours from 6:00 p.m. Friday to 3:00 a.m. Monday, U.S. Pacific Time.
     - Any unavailability caused by circumstances beyond Supplier's reasonable control, including, without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving Supplier employees), or third-party Internet service provider failures or delays (other than those Internet service providers under contract with Supplier).

   For any partial calendar month during which SFDC uses to the Services, availability will be calculated based on the entire calendar month, not just the portion for which SFDC used.

2. **Remedies**. In the event of a failure to comply with foregoing service level for a given calendar month (a "**Service Level Failure**"), Supplier shall issue a credit to SFDC (each, a "**Service Credit**") as an offset against its monthly invoice in the following amounts based on the availability for the applicable calendar month (as follows):

Tier	Monthly Availability Percentage	Credit Percentage
1	Less than 99.95% but greater than or equal to 99.90%	15% of 1/12th of Base Annual Fee
2	Less than 99.90% but greater than or equal to 99.80%	20% of 1/12th of Base Annual Fee
3	Less than 99.80% but greater than or equal to 99.70%	25% of 1/12th of Base Annual Fee
4	Less than 99.70% but greater than 96.0%	30% of 1/12th of Base Annual Fee

   In the event of two (2) Tier 4 Service Level Failures within any three (3) consecutive months, SFDC may terminate this Agreement upon notice to Supplier.

   Should Services availability be 96.0% or less within any calendar month, SFDC may terminate this Agreement upon notice to Supplier.

   The foregoing Service Credits and termination rights specified in this Section 2 shall constitute SFDC's sole and exclusive remedies for any Service Level Failure.

3. **Support**

   Supplier will provide email support between 8.30 am and 8.00 pm (US Eastern timezone). SFDC and Users can contact Supplier at support@spreedly.com with questions about the Transaction Processing Service, to report errors or other problems with the Transaction Processing Service, or to otherwise request support or assistance with respect to the

Transaction Processing Service. Supplier will maintain a sufficient number of Supplier Support Contacts to ensure timely responses to emails from Customer and to otherwise satisfy Supplier ‘s obligations under this Exhibit C.

Supplier shall make updates to the Transaction Processing Service available to Customer on a regular basis. In addition, Supplier shall troubleshoot and resolve errors related to the Transaction Processing Service in accordance with the following table:

Category	**Definition**	**Supplier Acknowledgement Time**	**Resolution**
Low	End-user or SFDC complaint that requires investigation by Supplier (including bugs not impacting API uptime)	Up to 48 hours	Next update
Critical	SFDC’s use of Transaction Processing Service is severely impaired due to Supplier -side issue or Transaction Processing Service is unavailable due to Supplier -side issue	Up to 60 minutes	Within 1 day

Supplier represents that it 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.

4. **Reporting, Claims and Notices**. Supplier will provide SFDC quarterly SLA reports showing Services availability for the prior calendar quarter, within 10 business days following the end of such calendar quarter. All claims will be verified against Supplier’s system records. Should Supplier dispute any period of unavailability alleged by SFDC, Supplier will provide to SFDC a record of Services availability for the applicable period. Supplier will provide such records only in response to claims made by SFDC in good faith.

EXHIBIT D

SUPPLIER SECURITY EXHIBIT

Security Controls

The Services include customer-configurable security controls that allow SFDC to tailor the security of the Services for its own use. These controls include:

- Unique User identifiers (User IDs) to ensure that activities can be attributed to the responsible individual.
- Controls to revoke access after several consecutive failed login attempts.
- Controls on the number of invalid login requests before locking out a User.
- Controls to insure generated initial passwords must be reset on first use.
- Controls to force a User password to expire after a period of use.
- Controls to terminate a User session after a period of inactivity.
- Password history controls to limit password reuse.
- Password length controls.
- The ability to accept logins to the Services from only certain IP address ranges.
- The ability to restrict access to the Services to specific time periods.

Software Security

The Services include effective and comprehensive controls to prevent the classes of software vulnerabilities relevant to the Services, the design of the services, and the software languages used in the delivery of the services. For general web applications, these vulnerability classes include, but are not limited to:

- SQL injection
- Cross site scripting
- Cross site request forgery
- XML or LDAP injection
- Server execution of user-uploaded files
- Session fixation
- Sensitive cookies permitted to be sent over insecure channels
- Buffer overflows
- Command injection
- Directory traversal
- Insecure third party domain access and cross domain policies
- HTTP response splitting
- Unauthorized privilege escalation
- Use of HTTPS using other than SSLv3 or TLS
- Use of SSL/TLS with null ciphers or ciphers using symmetric keys of less than 128 bits in length
- View States not encrypted with session-specific elements incorporated into the encryption key
- Returning verbose error information to clients
- Exposing cryptography errors to client (e.g. incorrect padding)
- Arbitrary redirection

For Force.com applications, these vulnerability classes also include:

- Not enforcing configured access control (Sharing, field level security, CRUD)

Security Procedures, Policies and Logging

The Services are operated in accordance with the following procedures to enhance security:

- User credentials or credential equivalents stored on Supplier servers or in persistent cookies are not stored in a format from which the original password can be derived (e.g. plaintext, encryptions other than one-way hashes) or easily discovered by brute force attacks given knowledge of the stored representation.
- User access log entries will be maintained, containing date, time, User ID, URL executed or entity ID operated on, operation performed (viewed, edited, etc.) and source IP address. SFDC acknowledges that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by SFDC or its ISP.
- If there is suspicion of inappropriate access, Supplier can provide SFDC log entry records to assist in forensic analysis.
- Logging will be kept for a minimum of 90 days.
- Logging will be kept in a secure area to prevent tampering.

- Passwords are not logged under any circumstances.
- Administrative changes to the Services (such as password changes and customizations) are tracked and are available for viewing by SFDC's system administrator. SFDC may download and store this data locally.
- Supplier personnel will not set a defined password for a User. Passwords are reset to a random value through programmatic means (which must be changed on first use) and delivered automatically via email to the requesting User.

Intrusion Detection
Supplier, or an authorized third party, will monitor the Services for unauthorized intrusions using network-based intrusion detection mechanisms.

User Authentication
Access to the Services requires a valid User ID and password combination, which are encrypted via SSL while in transmission. A random session ID cookie greater than or equal to 128 bits in length is used to uniquely identify each User.

Security Logs
Supplier shall ensure that all Supplier systems, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable the security audits referred to herein.

Incident Management
Supplier maintains security incident management policies and procedures, including detailed security incident escalation procedures. Supplier will promptly notify SFDC in the event Supplier becomes aware of an actual or reasonably suspected unauthorized disclosure of Customer Data or Payment Information.

Right to Audit Security Procedures
Following any notice from Supplier to SFDC of an actual or reasonably suspected unauthorized disclosure of SFDC Data, SFDC shall have the right to conduct, with reasonable prior written notice, under reasonable time, place and manner conditions, pursuant to appropriate confidentiality and technical restrictions, and at its own expense, an audit of Supplier's systems, policies and procedures relevant to the security and integrity of SFDC Data.

Additionally, (i) upon any Update to the Services; (ii) upon SFDC's reasonable belief that Supplier is not in compliance with its security policies and procedures under the Agreement regarding Customer Data or Payment Information; or (iii) if such audit is required by SFDC's governmental regulators, SFDC may conduct, either itself or through a third party independent contractor selected by SFDC at SFDC's expense, an on-site audit and review of Supplier's architecture, systems and procedures used in connection with the Services. For the purpose of (i) above, an "Update" shall mean any change to the Services resulting from a change to APIs or web applications. Audits and reviews conducted pursuant to (ii) and (iii) above may be conducted up to one time per year, with one week's advance notice. Upon Supplier Request, after conducting an audit, SFDC shall notify Supplier of the manner in which Supplier does not comply with any of the security, confidentiality or privacy obligations herein, if applicable. Upon such notice, Supplier shall use commercially reasonable efforts to make any necessary changes to ensure compliance with such obligations. Any audits described in this Section shall be conducted during reasonable times and upon reasonable advance notice to Supplier and shall be of reasonable duration and shall not unreasonably interfere with Supplier's day-to-day operations. In the event that SFDC conducts an audit through a third party independent contractor, such independent contractor shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Supplier's proprietary information.

Reports
Subject to reasonable confidentiality obligations consistent with generally accepted industry practices regarding the report, once per year during the term of the Agreement Supplier will, upon request, provide SFDC with third party reports relating to Supplier's information security obligations herein.

Physical Security
Supplier's data centers have an access system that controls access to the data center. This system permits only authorized personnel to have access to secure areas. The facility is designed to withstand adverse weather and other reasonably predictable natural conditions, is secured by around-the-clock guards, biometric access screening and escort-controlled access, and is also supported by on-site back-up generators in the event of a power failure.

Reliability and Backup
All networking components, SSL accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data and Payment Information is stored on a primary database server that is clustered with a backup database server for redundancy. All Customer Data and Payment Information is stored on carrier-class disk storage using RAID disks and multiple data paths. All Customer Data and Payment Information, up to the last committed transaction, is automatically backed up on a regular basis. Any backup tapes are verified for integrity and stored in an offsite facility in a secure, fire-resistant, location.

Disaster Recovery
Supplier has a disaster recovery facility that is geographically remote from its primary data center, along with required hardware, software, and Internet connectivity, in the event Supplier production facilities at the primary data center were to be rendered unavailable. Supplier has disaster recovery plans in place and tests them at least once per year. Supplier will discuss results of these tests with SFDC on request.

Supplier's disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Services within 12 hours after Supplier's declaration of a disaster; and (b) maximum SFDC Data loss of 4 hours.

Viruses
The Services will not introduce any viruses to SFDC's systems. However, SFDC content uploaded into the Services by SFDC is not scanned for viruses.

Data Encryption
Supplier uses industry accepted encryption products to protect Customer Data and Payment Information and communications during transmissions between SFDC's network and the Services, including minimum 128-bit VeriSign SSL Certification and minimum 1024-bit RSA public keys.

System Changes and Enhancements
Supplier plans to enhance and maintain the Services during the term of the Agreement. Security controls, procedures, policies and features may change or be added. Supplier will provide security controls that deliver a level of security protection that is not materially lower than that provided as of the Effective Date. A comprehensive description of the Services' current security controls can be found in the Specifications.

EXHIBIT E
VENDOR PRIVACY EXHIBIT

This Vendor Privacy Exhibit ("**Privacy Exhibit**") is entered into as of the Effective Date between salesforce.com, inc. ("SFDC") and Supplier, and forms part of the Agreement (as defined below) between SFDC and Supplier. In case of a conflict between the terms of this Privacy Exhibit and the Agreement, the terms of this Privacy Exhibit shall preempt and control. All capitalized terms that are not expressly defined in this Privacy Exhibit will have the meanings given to them in the Agreement. All examples are illustrative and not the sole examples of a particular concept.

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Agreement" means this Hosted Services Agreement.

"Confidential Information" has the meaning as set forth in the Agreement.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Data Subject" means the individual to whom Personal Data relates.

"Data Protection Laws and Regulations" means all laws, regulations, and legally binding requirements of any governmental authority or regulator applicable to the Processing of Personal Data under the Agreement. This includes laws and regulations of the United States, the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, including but not limited to GDPR.

"GDPR" means General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"Personal Data" means any information relating to an identified or identifiable natural person (the Data Subject). 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.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"Protected Information" means (a) SFDC Customer Data, (b) Payment Information and (c) all Personal Data that SFDC may provide to Supplier, including Personal Data about (i) SFDC prospective customers, suppliers and other business partners (and their respective employees and personnel) and (ii) Personal Data about SFDC employees and personnel.

"Security Breach" means (i) the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Protected Information or Confidential Information transmitted, stored or otherwise processed by Supplier or its Sub-processors or (ii) an event which led Supplier to suspect or would lead a reasonable person exercising a reasonable level of diligence and investigation to suspect that (i) has occurred.

"Services" means any goods and/or services that Supplier provides to SFDC under the Agreement.

"SFDC" means salesforce.com, inc., a company incorporated in Delaware.

"SFDC Customer" means a customer who purchases services from SFDC.

"SFDC Customer Data" means (a) data or information submitted by or for SFDC Customers to SFDC's online services (including services of SFDC Affiliates) and (b) all data or information disclosed by or for SFDC Customers to SFDC in connection with receiving services from SFDC, including payment information. Customer Data may include Personal Data.

"Sub-processor" means an entity which Processes Protected Information on behalf of Supplier, who is a Processor of Protected Information on behalf of the Controller.

2. PRIVACY REQUIREMENTS

2.1 **Compliance with Applicable Laws**. With respect to its activities hereunder involving Protected Information, Supplier hereby represents, warrants and covenants that: (i) it is and will remain at all times during the term of this Agreement, and to the extent it Processes any Protected Information after the term of the Agreement, in compliance with all applicable Data Protection Laws and Regulations and will enable SFDC to use the Services in compliance with all Data Protection Laws and Regulations applicable to SFDC and the customers to whom SFDC provides services; and (ii) its performance under this Agreement will not cause SFDC to be in violation of any Data Protection Laws and Regulations.

2.2 **Written Instructions on Processing of Protected Information**. Supplier shall Process Protected Information only on behalf of and in accordance with SFDC's documented written instructions. If any other Processing is required by applicable Data Protection Laws and Regulations, Supplier shall inform SFDC of the legal requirement before commencing such Processing, unless providing this information to SFDC is legally prohibited. For purposes of this section, SFDC instructs Supplier to Process Protected Information for the following purposes: (i) Processing in accordance with the Agreement and Order Form(s) and (ii) Processing to comply with other documented reasonable instructions provided by SFDC (e.g., via email) where such instructions are consistent with the terms of the Agreement. Further details on the Supplier's Processing activities under this Agreement are set out in Schedule 1. Supplier shall immediately inform SFDC if, in its opinion, an instruction from SFDC infringes Data Protection Laws and Regulations.

2.3 **Provision of Information to Demonstrate Compliance**. Supplier shall make available to SFDC all information necessary to demonstrate Supplier's compliance with the obligations laid down in this Privacy Exhibit.

2.4 **Personnel and Third Parties Authorized to Process Protected Information**. Supplier shall treat Protected Information as Confidential Information and shall not disclose Protected Information to any of its personnel or any third party except as necessary to perform the Services. Supplier shall ensure that personnel or third parties authorized to Process the Protected Information: (i) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, (ii) are informed of the confidential nature of the Protected Information, (iii) have received appropriate training on their responsibilities and (iv) do not Process Protected Information except on written instructions from SFDC, unless required by applicable law.

2.5 **Technical and Organizational Measures**. Supplier shall implement and maintain appropriate technical and organizational measures (and provide reasonable assistance to SFDC in implementing its own technical and organizational measures to the extent SFDC's implementation of such measures are dependent on Supplier) in order to:

a. Protect Protected Information and Confidential Information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access or Processing in accordance with Data Protection Laws and Regulations, thereby taking into account the principles of privacy-by-design and privacy-by-default.

b. Enable SFDC to meet its legal obligations to respond to requests from individuals under Data Protection Laws and Regulations in a timely manner, including the ability of Supplier to implement requests from individuals to access, rectify, amend, object to Processing, erase, not to be subject to automated decision-making including profiling, or port their Personal Data or to restrict or cease Processing of such Personal Data where SFDC instructs Supplier to implement such a request. Supplier shall immediately notify SFDC of any request related to SFDC made by an individual to exercise any individual right under Data Protection Laws and Regulations and shall cooperate with SFDC in executing SFDC's obligations related to such request. Supplier may not reach out to the individual without SFDC's prior written consent except to confirm that the request relates to Salesforce.

c. Ensure and be able to demonstrate that Processing of Protected Information is performed in accordance with applicable Data Protection Laws and Regulations.

2.6 **Data Protection Impact Assessment**. Upon SFDC's request, Supplier shall assist SFDC when SFDC carries out any data protection impact assessment related to Processing carried out with respect to Supplier's Services under the Agreement and provide assistance to SFDC in SFDC's consultation with regulators regarding the Processing that is the subject of a data protection impact assessment. If Supplier Processes SFDC Customer Data, upon SFDC's request, Supplier shall also provide SFDC with cooperation and assistance needed to fulfill SFDC's obligation to assist SFDC's Customers in ensuring compliance with their obligation to carry out a data protection impact assessment or consult with regulators regarding Processing that is the subject of a data protection impact assessment, including by providing all relevant information, to the extent SFDC does not otherwise have access to the relevant information needed by SFDC's Customers and to the extent such information is available to Supplier.

2.7 **Records of Processing**. Upon SFDC's request, Supplier shall provide cooperation and assistance compiling or maintaining SFDC's records of processing as required by Data Protection Laws and Regulations. Supplier acknowledges that SFDC may be required, upon its supervisory authority's request, to make such records available to the supervisory authority.

2.8 **Privacy Certifications**. Supplier will, on or before the second anniversary of the Effective Date, meet the following certification obligations:

a. Subject to reasonable confidentiality obligations consistent with generally accepted industry practices regarding the report, once per year during the term of the Agreement Supplier will, upon request, provide SFDC with an SSAE 18 SOC 2, Type 2 Report and all other third party reports relating to Supplier's information security obligations herein.

b. Supplier operates an information security management system (ISMS) for the Services in accordance with the ISO 27001 international standard. Supplier has achieved ISO 27001 certification for its ISMS from an independent third party. Supplier's ISO 27001 Certificate and Statement of Applicability shall be made available to SFDC upon request.

3. TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

3.1 **Standard Contractual Clauses ("SCCs")**. Supplier agrees that it shall abide by the relevant terms of the SCCs attached as Schedule 2 to this Privacy Exhibit. The SCCs shall apply to Supplier in its role as processor as if it were the "data importer." The SCCs shall apply to SFDC and, to the extent legally required, all of SFDC's Affiliates established within the European Economic Area, Switzerland and/or the United Kingdom, in their role as controllers and these entities shall be deemed "data exporters." In particular, Supplier agrees that as provided in the SCCs, individuals shall be third party beneficiaries to the SCCs. In addition, SFDC and Supplier hereby agree that the security provisions in the Agreement shall apply to Appendix 2 of the SCCs. To the extent SFDC is acting as Processor with respect to the Personal Data, then the parties agree that SFDC shall be entitled to exercise the rights under the SCCs on behalf of the Controller (as if it were the "data exporter") or to delegate such rights to the Controller and/or to procure from Supplier that Controller may directly exercise such rights with Supplier.

3.2 **EU-US and Swiss-US Privacy Shield Frameworks**. Supplier will:

a. Provide at least the same level of protection for Personal Data as is required by the relevant principles of the EU-U.S. and Swiss-U.S. Privacy Shield frameworks.

b. Promptly notify SFDC of any failure or inability to provide at least the same level of protection.

c. Where Supplier permits a Sub-processor to access Personal Data (subject to SFDC's approval right as set forth in the "Sub-processing" section), Supplier will require the Sub-processor to provide at least the same level of protection as is required by the relevant principles of the EU-U.S. and Swiss-U.S. Privacy Shield frameworks.

3.3 **Binding Corporate Rules**. If Supplier processes SFDC Customer Data, then Supplier acknowledges that SFDC has obtained approval of the Salesforce Processor Binding Corporate Rules ("BCR"), which is included as a legal transfer mechanism in the agreement with its Customers to cover any transfer of Personal Data outside of the European Union, the European Economic Area, their European Union's member states, or Switzerland. Supplier agrees that it shall abide by the relevant terms of the BCR, as updated from time to time, and as published at http://www.sfdcstatic.com/assets/pdf/misc/Salesforce-Processor-BCR.pdf, regarding such Personal Data.

4. SECURITY INCIDENT RESPONSE

4.1 **Security Incident Response Program**. Supplier maintains appropriate security incident management policies and procedures. Supplier will immediately, but at least within 24 hours upon discovery, notify SFDC of an actual or reasonably suspected Security Breach. In the notification, Supplier shall include details of when the Security Breach occurred and when it was detected, the nature and scope of the Protected Information involved in the Security Breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned, the observed and probable consequences of the Security Breach, measures taken or proposed to mitigate the negative effects of the Security Breach, the name and contact details of the data protection officer or other contact point where more information can be obtained, and all other information requested by SFDC regarding the Security Breach. In addition, Supplier shall (i) investigate and remediate the effects of the Security Breach; (ii) provide SFDC, in writing, an impact assessment and assurance satisfactory to SFDC that such Security Breach will not recur; and (iii) upon SFDC's request, provide SFDC with cooperation and assistance needed to fulfill SFDC's obligations to provide information to regulators or individuals without undue delay as required by Data Protection Laws and Regulations. To the extent Supplier does not have full information about the Security Breach at the time of the initial notification, Supplier shall still complete the initial notification on the timing set forth above and then supplement that with additional information as it becomes available. Without limiting any other rights or remedies of SFDC, if as the result of any act or omission of Supplier or any of its personnel, contractors, or agents, one or more third parties is required to be notified of unauthorized access or use of Protected Information, Supplier agrees it shall be responsible for any reasonable costs associated with such communication (including providing call center services) and for any costs of providing a credit monitoring services. In addition, Supplier will provide indemnification to SFDC related to such Security Breach as set forth in the Agreement.

5. DATA STORAGE AND DELETION

5.1 Data Storage. Supplier will abide by the following with respect to storage of Protected Information and Confidential Information:

a. Supplier will not store or retain any Protected Information or Confidential Information except as necessary to perform Services under the Agreement.

b. Supplier will (i) inform SFDC in writing of all countries where Protected Information is Processed or stored and (ii) obtain consent from SFDC for Processing or storage in the identified countries. As of the Effective Date, Supplier stores Protected Information in the following countries to which SFDC hereby consents: United States. If Supplier processes SFDC Customer Data, SFDC may make this country list available to SFDC Customers.

5.2 Data Deletion. Supplier will abide by the following with respect to deletion of Protected Information and Confidential Information:

a. Within 30 calendar days of the Agreement's expiration or termination, or sooner if requested by SFDC, Supplier will securely destroy (per subsection (c) below) all copies of Protected Information and Confidential Information (including any automatically created archival copies).

b. Upon SFDC's request, Supplier will promptly return to SFDC a copy of all Protected Information and Confidential Information within 30 days and, if SFDC also requests deletion of the Protected Information and Confidential Information, will carry that out as set forth above.

c. All deletion of Protected Information and Confidential Information must be conducted in accordance with best practices for deletion of sensitive data. For example, secure deletion from a hard drive is defined at a minimum as a seven-pass write over the entire drive.

d. Tapes, printed output, optical disks, and other physical media must be physically destroyed by a secure method, such as shredding performed by a bonded provider.

e. Upon SFDC's request, Supplier will provide a "Certificate of Deletion" certifying that Supplier has deleted all Protected Information and Confidential Information. Supplier will provide the "Certificate of Deletion" within 30 days of SFDC's request.

6. SUB-PROCESSING

6.1 Consent for Sub-processing. Supplier will not sub-process any of its obligations under this Agreement except as set forth in this Section. The list of Supplier's authorized Sub-processors is set forth on Schedule 3. Supplier may add additional Sub-processors to this list provided that it gives 30 days' prior written notification of the identity of the Sub-processor to SFDC and SFDC does not object to the appointment within that period. In the event Supplier is required to engage a Sub-processor with less than 120 days' notice, Supplier shall provide written notice to SFDC describing the circumstances as to why Supplier is unable to provide 120 days prior notice, along with the identity of the Sub-processor. Supplier agrees to provide any additional materials, upon SFDC's reasonable request, to SFDC to evaluate the new Sub-processor. In the event SFDC objects to a new Sub-processor, Supplier will use reasonable efforts to make available to SFDC a change in the affected Services or recommend a commercially reasonable change to SFDC's use of the affected Services to avoid Processing of Protected Information by the objected-to new Sub-processor without unreasonably burdening SFDC. If Supplier is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, SFDC may terminate the Order Form(s) in respect to those Services which cannot be provided by Supplier without the use of the objected-to new Sub-processor, by providing written notice to Supplier, without Supplier imposing a penalty for such termination on SFDC. SFDC shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services. For the avoidance of doubt, sub-processing includes any Processing of Protected Information, including access, transmission, or storage by Supplier, its Affiliates, or its Sub-processors. Unless SFDC expresses in the consent an intent to allow Supplier to sub-process generally, any consent provided by SFDC per this section is limited to the specific Statement of Work and the specific Sub-processor for which the consent was provided. Supplier's use of Sub-processors shall be subject to the following:

a. Supplier shall be fully responsible for the performance of any Sub-processor and the compliance with all of the obligations of this Agreement by any Sub-processor. To this end, Supplier will conduct proper due diligence on all Sub-processors to ensure each Sub-processor can comply with Data Protection Laws and Regulations, all applicable terms and conditions of this Agreement, and all applicable SFDC policies and procedures to which Supplier may be subject during the term of this Agreement.

b. Sub-processors retained by Supplier to provide Services for SFDC will at all times be deemed Sub-processors of Supplier and shall not under any circumstance be construed or deemed to be employees or Sub-processors of SFDC.

c. Supplier shall ensure that it has a written contract in place with the relevant Sub-processor which meets the same obligations in respect of Processing of SFDC's Protected Information as are imposed on Supplier under this Privacy Exhibit.

d. Supplier shall flow down all obligations in this Agreement regarding, among other things: (i) Protected Information and (ii) all SFDC's and SFDC's regulator's (and, if Supplier processes SFDC Customer Data, SFDC's Customers and SFDC's Customers' regulator's) rights regarding review and audit (including SFDC's right to appoint an independent third party to perform such review or audits).

6.2 **Copies of sub-processing agreements**. Upon SFDC's request, Supplier will provide SFDC copies of any sub-processing agreements it has in support of the provision of the Services. Supplier will provide such copies to SFDC within ten (10) days of SFDC's request. Supplier may remove any commercial information from such copies before providing such agreements to SFDC. SFDC may share such copies with SFDC Customers who request this information.

7. AUDITS

7.1 **Right to Audit; Permitted Audits**. In addition to any other audit rights described in the Agreement, SFDC and its regulators (and, if Supplier processes SFDC Customer Data, SFDC's Customers and SFDC's Customers' regulator's) shall have the right to an on-site audit of Supplier's architecture, systems, policies and procedures relevant to the security and integrity of Protected Information, or as otherwise required by a governmental regulator:

a. Following any notice from Supplier to SFDC of an actual or reasonably suspected Security Breach or unauthorized disclosure of Protected Information.

b. Upon SFDC's reasonable belief that Supplier is not in compliance with its security policies and procedures under the Agreement regarding Protected Information.

c. As required by governmental regulators.

d. For any reason, or no reason at all, once annually.

7.2 **Audit Terms**. Any audits described in this Section shall be:

a. Conducted by SFDC or its regulator (or, if Supplier processes SFDC Customer Data, SFDC's Customers and SFDC's Customers' regulator's), or through a third party independent contractor selected by one of these parties.

b. Conducted during reasonable times.

c. To the extent possible, conducted upon reasonable advance notice to Supplier.

d. Of reasonable duration and shall not unreasonably interfere with Supplier's day-to-day operations.

7.3 **Third Parties**. In the event that SFDC conducts an audit through a third party independent auditor or a third party accompanies SFDC or participates in such audit, such third party shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Supplier's and Supplier's customers' confidential and proprietary information. For the avoidance of doubt, regulators shall not be required to enter into a non-disclosure agreement.

7.4 **Audit Results**. Upon Supplier request, after conducting an audit, SFDC shall notify Supplier of the manner in which Supplier does not comply with any of the applicable security, confidentiality or privacy obligations herein. Upon such notice, Supplier shall make any necessary changes to ensure compliance with such obligations at its own expense and without unreasonable delay and shall notify SFDC when such changes are complete. Notwithstanding anything to the contrary in the Agreement, SFDC may conduct a follow-up audit within six (6) months of Supplier's notice of completion of any necessary changes. To the extent that a Supplier audit and/or SFDC audit identifies any material security vulnerabilities, Supplier shall remediate those vulnerabilities within fifteen (15) days of the completion of the applicable audit, unless any vulnerability by its nature cannot be remedied within such time, in which case the remediation must be completed within a mutually agreed upon time not to exceed sixty (60) days.

8. MISCELLANEOUS TERMS

8.1 **Legal Process**. If Supplier or anyone to whom Supplier provide access to Protected Information becomes legally compelled by a court or other government authority to disclose Protected Information, then to the extent permitted by law, Supplier will promptly provide SFDC with sufficient notice of all available details of the legal requirement and reasonably cooperate with SFDC's efforts to challenge the disclosure, seek an appropriate protective order, or pursue such other legal action, as SFDC may deem appropriate.

8.2 **Conflict**. In the event of any conflict or inconsistency between this Privacy Exhibit and the Agreement, this Privacy Exhibit shall prevail.

8.3 **Disclosure of this Exhibit**. As required or upon request, SFDC may provide a summary or copy of this Privacy Exhibit to any government regulator or SFDC Customer.

8.4 **Survival**. Supplier's obligations under this Privacy Exhibit will survive expiration or termination of the Agreement and completion of the Services as long as Supplier continues to have access to Protected Information.

8.5 **Suspension**. SFDC may immediately suspend Supplier's Processing of Protected Information if Supplier is not complying with this Privacy Exhibit.

8.6 **Termination**. SFDC may terminate the Agreement or an Order Form(s) if SFDC reasonably determines that (a) Supplier has failed to cure material noncompliance with the Privacy Exhibit within a reasonable time; or (b) SFDC needs to do so to comply with Data Protection Laws and Regulations.

List of Schedules

Schedule 1: Details of the Processing
Schedule 2: Standard Contractual Clauses
Schedule 3: Authorized Sub-processors

The parties' authorized signatories have duly executed this Privacy Exhibit:

VENDOR **SALESFORCE.COM, INC.**

Signature:_________________________________

Print Name: _______________________________

Title: ____________________________________

Date: ____________________________________

Signature:_________________________________

Print Name: _______________________________

Title: ____________________________________

Date: ____________________________________

SCHEDULE 1 - DETAILS OF THE PROCESSING

Categories of Data Subjects

SFDC may submit Personal Data to the Services, the extent of which is determined and controlled by SFDC in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of SFDC (who are natural persons)
- Employees or contact persons of SFDC's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of SFDC (who are natural persons)
- SFDC's users authorized by SFDC to use the Services

Categories and nature of Personal Data

SFDC may submit Personal Data to the Services, the extent of which is determined and controlled by SFDC in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localisation data

Scope and purpose of Processing

The objective of Processing of Personal Data by Supplier is the performance of the Services pursuant to the Agreement.

Duration of Processing

Subject to the Data Storage and Deletion section of the Privacy Exhibit, Supplier will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

SCHEDULE 2 - STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: salesforce.com, inc.

Address: Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105

Tel.: + 1 415 901 7000; fax: + 1 415 901 7400; e-mail: privacy@salesforce.com

Other information needed to identify the organisation: Not applicable

(the data **exporter**)

And

Name of the data importing organisation: Spreedly, Inc.

Address: 733 Foster Street, Durham, NC 27701

Tel.: 917-951-4372 e-mail: eliot@spreedly.com

Other information needed to identify the organisation: Not applicable

(the data **importer**)
each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor’s obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

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

Data exporter

The data exporter (as such term is applied *mutatis mutandis* per the Vendor Privacy Exhibit) is (please specify briefly your activities relevant to the transfer): Salesforce.com, inc. is a provider of enterprise cloud computing solutions.

Data importer

The data importer (as such term is applied *mutatis mutandis* per the Vendor Privacy Exhibit) is (please specify briefly activities relevant to the transfer):

Supplier

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit personal data to the Service which may include, but is not limited to personal data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's Users authorized by data exporter to use the SCC Services

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit personal data to the Services which may include, but is not limited to the following categories of personal data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localisation data

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Data exporter may submit special categories of data to the Services, and which is for the sake of clarity personal data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of processing of personal data by data importer is the performance of the Services pursuant to the Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses:

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of personal data contained in Customer Data, as described in the Vendor Privacy Exhibit. Data Importer will not materially decrease the overall security of the Services during a subscription term.

SCHEDULE 3 - AUTHORIZED SUB-PROCESSORS

	Name of entity conducting the data processing (i.e. Spreedly or a Subprocessor (affiliate or subcontractor)	Country	Description of processing activity
1	DropBox	USA	Document hosting
2	Slack	USA	Communication
3	Asana	USA	Project planning and management
4	HubSpot	USA	Sales/Marketing
5	Google	USA	Communication
6	LeadFeeder	USA	Marketing
7	Mixpanel	USA	Product usage analytics
8	Zendesk	USA	Customer support
9	SurveyMonkey	USA	Customer messaging
10	Netsuite	USA	Billing and financial reporting
11	Quickbooks	USA	Billing and financial reporting
12	Heroku	USA	Application hosting
13	AWS	USA	Data processing
14	Adroll	USA	Marketing

EXHIBIT F
SECURITY REMEDIATION PLAN

Per section 7.4 of the Agreement, SFDC has notified the Supplier of Vulnerabilities. Supplier agrees to the following plan (the "**Security Remediation Plan**") and shall take the following actions to remediate and correct (in SFDC's sole discretion) the Vulnerabilities in accordance with the plan set forth below.

- Implement two-factor authentication in place, including all IaaS platform access points and paths to production access, and external client facing applications id.spreedly.com and dashboard.spreedly.com by April 1st (required for go-live).
- Rotate all SFDC Spreedly API keys exposed to Mixpanel by April 1st (required for go-live).
- Notify all Spreedly customers of the key rotation process by April 1st.
- Rotate all Spreedly API keys exposed to Mixpanel by October 1st.
- Build regular key rotation process for all production servers, path to production access, encryption keys, and customer secrets by April 1st (required for go-live).
- Remediate the following Salesforce issues from the NCC report by April 1st (required for go-live).
  - 013 - "Sessions Do Not Time Out"
  - 006 - "Arbitrary URL Redirection"
- Agree to and execute an additional "red team" style security assessment by Salesforce by February 18th (required for go-live).
- Remediate all severity 0 and severity 1 issues (pursuant to agreed vulnerability definitions) from "red team" engagement in accordance with the Vulnerability Remediation SLA defined in Exhibit G (required for go-live).

EXHIBIT G
VULNERABILITY REMEDIATION SLA

Supplier agrees to comply with the following Salesforce vulnerability remediation service-level agreement (the "**Vulnerability Remediation SLA**") for remediation of any security issue found during the Term of the Agreement pursuant to the following definitions.

- 1.1 Severity Level: Critical
    - Priority Code: P0
    - Fix SLA: Within 7 days
    - 1.2. Severity Level Description includes but is not limited to:
        - 1.2.1. Vulnerabilities that can compromise the confidentiality, integrity, or availability of production and corporate resources and data with limited exploitation difficulty and/or attacker skill.
        - 1.2.2. Vulnerabilities that could be easily exploited by a remote or unauthenticated attacker and lead to system compromise and/or exposure of highly sensitive or customer data without requiring user interaction.
    - 1.3. Vulnerability Examples include, but are not limited to:
        - 1.3.1. External facing remote arbitrary code execution without mitigating circumstances.
        - 1.3.2. External facing overflow vulnerability resulting in native code execution without mitigating circumstances.
        - 1.3.3. External facing SQL injection.
        - 1.3.4. External facing unintended cross tenant information disclosure and multi-tenancy break.
        - 1.3.5. External use of weak cryptography that is practically exploitable in a real killchain without nation state resources.
        - 1.3.6. Authentication flaws resulting in arbitrary account compromise.
        - 1.3.7. Session management flaws leading to arbitrary account compromise.
        - 1.3.8. External facing default credential usage.
        - 1.3.9. Client and server software and systems susceptible to publicly disclosed and exploited vulnerability.
        - 1.3.10. Susceptibility to external simply executed single actor DOS resulting in service outage.
    - 1.4. Tooling Score Estimates include, but are not limited to:
        - 1.4.1. Nessus: Critical *In a small subset of cases
        - 1.4.2. CVSSv3 Temporal Score: 9-10
        - 1.4.3. Qualys: Severity 5
        - 1.4.4. nCircle: 1000+ (Based on risk)
        - 1.4.5. PCI Violating Vuln: Yes
        - 1.4.6. AppDetective: High (Based on risk)
        - 1.4.7. Whitehat: Urgent
- 2.1. Severity Level: High
    - Priority Code: P1
    - Fix SLA: Within 30 days
    - 2.2. Severity Level Description includes but is not limited to:
        - 2.2.1. Vulnerabilities that can compromise the confidentiality, integrity, or availability of production and corporate resources and data.
        - 2.2.2. Vulnerabilities that could be easily exploited by an internal and/or external, authenticated/unauthenticated attacker and lead to system

compromise and/or exposure of highly sensitive or customer data without requiring user interaction.

        - 2.2.3. Vulnerabilities that allow local users to gain increased privileges.
        - 2.2.4. Vulnerabilities that allow unauthenticated remote users to view sensitive information.
        - 2.2.5. Vulnerabilities that allow local or remote users to cause a denial of service condition.
    - 2.3. Vulnerability Examples include, but are not limited to:
        - 2.3.1. External facing Persistent/Stored Cross Site Scripting (XSS).
        - 2.3.2. External Cross Site Request Forgery (CSRF) exposure on sensitive or critical functions.
        - 2.3.3. External facing stack traces containing sensitive information exposed to clients.
        - 2.3.4. External use of weak cryptography that is practically exploitable in a real killchain with nation state resources.
        - 2.3.5. Internal use of weak cryptography that is practically exploitable in a real killchain without nation state resources.
        - 2.3.6. Internal remote arbitrary code execution without mitigating circumstances.
        - 2.3.7. Internal command or SQL injection without mitigating circumstances.
        - 2.3.8. Internal exposure of sensitive information.
        - 2.3.9. Internal use of default or weak credentials.
        - 2.3.10. Susceptibility to internal simply executed DOS resulting in service outage.
        - 2.3.11. Client software and systems susceptible to publicly disclosed vulnerability.
    - 2.4. Tooling Score Estimates include, but are not limited to:
        - 2.4.1. Nessus: Critical/Severe
        - 2.4.2. CVSSv3 Temporal Score: 7 - 8.9
        - 2.4.3. Qualys: Severity 4
        - 2.4.4. nCircle:1000+
        - 2.4.5. PCI Violating Vuln: Yes
        - 2.4.6. AppDetective: High
        - 2.4.7. Whitehat: Critical
- Moderate Severity Level
    - 3.1. Severity Level: Moderate
    - Priority Code: P2
    - Fix SLA: Within 90 days
    - 3.2. Severity Level Description includes but is not limited to:
        - 3.2.1. Vulnerabilities that may be more difficult to exploit but could still lead to some compromise of the confidentiality, integrity, or availability of resources, under certain circumstances.
        - 3.2.2. Vulnerabilities that could have had a critical or high impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations.
    - 3.3. Vulnerability Examples include, but are not limited to:
        - 3.3.1. External unintended internal information disclosure.
        - 3.3.2. Internal Cross Site Scripting (XSS).
        - 3.3.3. XSS from an authenticated customer admin
        - 3.3.4. Internal Cross Site Request Forgery (CSRF).

  - 3.3.5. Internal use of weak cryptography that is practically exploitable in a real killchain with nation state resources.
  - 3.3.6. Usage of end of lifed operating systems or software.
  - 3.3.7. External facing content spoofing.
- 3.4. Tooling Score Estimates include, but are not limited to:
  - 3.4.1. Nessus: Moderate
  - 3.4.2. CVSSv3 Temporal Score: 4 - 6.9
  - 3.4.3. Qualys: Severity 3
  - 3.4.4. nCircle: 500-999
  - 3.4.5. PCI Violating Vuln: No
  - 3.4.6. AppDetective: Medium
  - 3.4.7. Whitehat: High