Spreedly

SERVICE AGREEMENT

Part A: Parties

SPREEDLY

Name:	Spreedly, Inc.
Address:	733 Foster Street, Suite 100
City/State:	Durham, NC 27701

CUSTOMER

Name:	OpenTable, Inc.
Address:	1 Montgomery St Ste 700
City/Country:	San Francisco, CA 94104

PRIMARY SPREEDLY CONTACT

Name:	Daniel Scagnelli
Title	Sr. Enterprise Account Executive
Phone:	888-727-7750
Email:	dscagnelli@spreedly.com

PRIMARY CUSTOMER CONTACT

Name:	Ralph Matlack
Title:	Sr. Director, Restaurant Lifecycle & Partnerships
Phone:	
Email:	rmatlack@opentable.com

Part B: Terms

1. This Service Agreement (including its exhibits, the "**Agreement**") is effective as of the last date of signing below ("**Effective Date**") and is between Spreedly, Inc. ("**Spreedly**"), and the customer listed above (the "**Customer**"). Except as otherwise provided herein, this Agreement is subject to the Spreedly Privacy Policy ("**Privacy Policy**"), which is incorporated herein by reference, and which can be viewed at https://spreedly.com/. To the extent that any term in the Privacy Policy conflicts with the terms of this Agreement or any inconsistency between the Privacy Policy and this Agreement exists, the terms of this Agreement shall prevail. For clarity, to the extent any term in this Part B, Terms (or the Privacy Policy), conflicts with the Data Security Addendum attached hereto as Exhibit D ("**Data Security Addendum**"), or any inconsistency between the Terms (or Privacy Policy) and the Data Security Addendum exists, the terms of the Data Security Addendum shall prevail.

2. <u>Provision and Use of Service</u>.

   a. Spreedly hereby grants the Customer, Customer's subsidiaries, and Kayak Software Corporation (a sister company of Customer, "**Kayak**") (collectively, the "**Customer Parties**") a worldwide, limited, non-exclusive, non-transferable license, without the right to sublicense, during the Term, to electronically access and use the Spreedly API (the "**Service**") to validate, tokenize and vault credit cards (and other payment types) and then process charges against those payment methods against one or more of the payment gateways that are integrated to the Service and/or third-party payment method receivers that Spreedly supports, and, where applicable, automatically update expired or lost credit cards. Spreedly is not a payment gateway or merchant account provider and Spreedly does not assume any direct or indirect liability or responsibility for Customer's agreements with payment gateways or merchant account providers supported on our Service. The foregoing license includes Customer's right to access and use Spreedly's website and any software programs, documentation, tools, internet-based services, components, and any updates (including software maintenance, service information, help content, bug fixes or maintenance releases) provided to Customer by Spreedly in connection with the Service.

   b. Customer shall be responsible and liable to Spreedly for the performance, acts, omissions and non-compliance of Kayak and Customer's subsidiaries with the terms of this Agreement to the same extent that as if such performance, acts, omissions and/or non-compliance were by Customer.

   c. "**Laws**" means all applicable laws, directives, rules and regulations. Customer shall comply with all Laws applicable to its use of the Service and Spreedly reserves the right to restrict access to the Service if it reasonably suspects that Customer is in violation of this requirement. Customer hereby grants Spreedly authorization to share information with law enforcement about Customer, with at least five (5) days' notice to Customer unless prohibited by applicable law, Customer's transactions and Customer's Spreedly account, in each case if Spreedly reasonably suspects that Customer's use of the Service has been for an unauthorized, illegal, or criminal purpose.

   d. Spreedly reserves the right to not store or submit any transaction Customer submits that Spreedly reasonably believes is in violation of this Agreement or applicable Law or otherwise exposes Customer or other Spreedly users to harm, including but not limited to, fraud and other criminal acts; provided Spreedly provides prompt notice to Customer of any transactions that Spreedly has refused to store or submit along with an explanation of the basis for Spreedly's action(s).

3. Intellectual Property Rights.

a. The Service is licensed and not sold. Spreedly reserves all rights in the Service not expressly granted to Customer in this Agreement. The Service is protected by copyright, trade secret and other intellectual property laws. Spreedly owns the title, copyright and other worldwide Intellectual Property Rights (as defined below) in the Service and all copies of the Service. This Agreement does not grant Customer any rights to our trademarks or service marks. For the purposes of this Agreement, "**Intellectual Property Rights**" means all patent rights, copyright rights, mask work rights, moral rights, rights of publicity, trademark, trade dress and service mark rights, goodwill, trade secret rights and other intellectual property rights as may now exist or hereafter come into existence, and all applications therefore and registrations, renewals and extensions thereof, under the Laws of any state, country, territory or other jurisdiction.

b. Customer may submit comments or ideas about how to improve the Service or other Spreedly products ("**Ideas**"). By submitting any Idea, Customer agrees that its disclosure is gratuitous, unsolicited and without restriction and will not place Spreedly under any fiduciary or other obligation, and that Spreedly is free to use the Idea without any additional compensation to Customer, and/or to disclose the Idea on a non-confidential basis or otherwise to anyone. Customer further acknowledges that, by acceptance of its submission, Spreedly does not waive any rights to use similar or related ideas previously known to Spreedly, or developed by its employees, or obtained from sources other than Customer.

c. Other than: (1) Spreedly's right to use data provided by Customer solely for provision of the Service; and (2) Ideas, Customer does not transfer, assign, or license any other Intellectual Property Rights to Spreedly.

4. Term and Termination.

a. Unless otherwise terminated in accordance with this Agreement, the initial term of this Agreement shall be for a period of one (1) year from the Effective Date (the "**Initial Term**"). Thereafter, this Agreement shall automatically renew for successive one year periods (each, a "**Renewal Term**" and, together with the Initial Term, the "**Term**") unless either party has provided written notice of its intent to not renew this Agreement not less than sixty (60) days prior to the expiration of the then-current Initial or Renewal Term.

b. Either party may terminate this Agreement, by written notice to the other party effective as of the date specified in such notice, if the other party materially breaches this Agreement and such breach: (i) cannot be cured; or (ii) being capable of cure, remains uncured thirty (30) days after the breaching party receives written notice thereof. Without limiting the foregoing, in the event of a breach that gives rise to the right by Spreedly to terminate this Agreement, Spreedly may elect, as an interim measure, to suspend the Service, immediately upon notice to Customer, until the breach is cured and all fees shall continue to accrue during the period of such suspension. Spreedly's exercise of its right to suspend performance shall be without prejudice to Spreedly's right to terminate this Agreement upon written notice to Customer.

c. Customer may also immediately terminate this Agreement upon written notice to Spreedly in the event that: (i) Customer becomes aware that Spreedly has become subject to a Breach of Security that is caused by Spreedly's breach of its security obligations set forth in Section 10 or the Data Security Addendum, (ii) as provided in the Service Level Agreement attached hereto as Exhibit B, (iii) if Spreedly is no longer in compliance with PCI-DSS, or (iv) Spreedly is unable to meet either SOC-2 Type I Certification or SOC-2 Type II Certification (in each case as defined in the Data Security Addendum) by the dates specified in the Data Security Addendum ("SOC-2 Termination"); provided that Customer must exercise its right to terminate this Agreement pursuant to any of the foregoing clauses within thirty (30) days after the latter of: (x) the occurrence of, or (y) the notification of, the event triggering such right otherwise Customer shall be deemed to have waived such right to terminate. In the event of SOC-2 Termination, as Customer's sole and exclusive remedy, Spreedly will provide Customer with a pro-rata refund for any unused prepaid fees for the terminated period.

d. Upon termination of this Agreement and any applicable Transition Period, (i) Spreedly will immediately discontinue Customer's access to the Service; (ii) Customer shall complete all pending transactions and stop accepting new transactions through the Service; (iii) Customer will discontinue use of any Spreedly trademarks and immediately remove any Spreedly references and logos from Customer's website; and (iv) each party promptly returns to the other or, if so directed by the other party, destroys all originals and copies of any Confidential Information of the other party (including all notes, records and materials developed therefrom).

e. If either party elects not to renew this Agreement, then upon request by Customer made 15 or more days before the expiration date, or upon notice to Spreedly upon termination, Spreedly shall continue to provide the Service in order for Customer to export or arrange export of its card data or other credit card or user information associated with Customer's account and/or other services necessary for such export in connection with Section 9.f, for a 30 day period after the expiration or termination date (the "**Transition Period**") as follows (the "**Transition Services**"):

(1) In the event that Customer terminates this Agreement in accordance with Section 4.b (material breach by Spreedly) or Section 4.c, notwithstanding the last sentence of Section 9.f, Spreedly will provide the Transition Services under the same terms, free of charge for the Transition Period.

(2) In the event that Spreedly terminates this Agreement in accordance with Section 4.b, notwithstanding the last sentence of Section 9.f, Spreedly will provide the Transition Services under the same terms and subject to the prorated Base Annual Fee (as determined in accordance with Exhibit A of this Agreement) plus a 10% price increase to such prorated amount.

(3) In the event that this Agreement expires, or this Agreement is terminated for any reason other than as contemplated in clauses (1) and (2) of this Section 4.e, Spreedly will provide the Transition Services under the same terms and subject to the prorated Base Annual Fee as determined in accordance with Exhibit A of this Agreement.

Notwithstanding any expiration of this Agreement under this Section, the terms of this Agreement shall continue to govern Spreedly's provision of the Service during the Transition Period as if it had not been terminated.

5. Representations.

a. Each party to this Agreement represents and warrants to the other that: (i) it possesses the legal right and corporate power and authority to enter into this Agreement and to fulfill its obligations hereunder; and (ii) its execution, delivery and performance of this Agreement will not violate the terms or provision of any other agreement, contract or other instrument, whether oral or written, to which it is a party.

b. Customer warrants to Spreedly that: (i) it will not use the Service, directly or indirectly, for any fraudulent undertaking or in any manner so as to knowingly or intentionally interfere with the use of the Service; and (ii) it will comply, at its own expense, with all Card Rules (as defined in Section 9.a below) applicable to merchants, and all applicable terms of service of the payment gateways, merchant service providers and/or API endpoints Customer connects with on the Service.

6. Pricing. Spreedly will charge Customer the fees outlined on Exhibit A for use of the Services.

7. Confidential Information.

a. For the purposes of this Agreement, "**Confidential Information**" means any and all technical and non-technical information, labeled or marked as "Confidential," "Proprietary" or with a similar proprietary legend, or that ought reasonably to be understood as confidential or proprietary, given the nature of the information or the circumstances surrounding its disclosure, to be confidential, which may also be disclosed verbally. "Confidential Information" does not include any information which: (i) now or hereafter enters the public domain through no breach of an obligation of confidentiality or other fault of a party; (ii) the receiving party independently knows free of any obligation of confidentiality at the time of receiving such information; (iii) a third party hereafter furnishes to the receiving party without restriction on disclosure and without breach of any confidentiality obligations; or (iv) employees or agents of a receiving party have independently developed without any use of or reference to any Confidential Information and without breaching this Agreement.

b. Each party (including a Customer Party, as applicable) shall: (i) only disclose Confidential Information to any of its and/or its subsidiaries' employees, officers, directors, partners, consultants, contractors, agents and representatives (collectively, its "**Representatives**") that have a need to know such Confidential Information and who have a confidentiality obligation, whether through contract or other legally enforceable confidentiality obligation (e.g., attorneys' duty of confidentiality), at least as protective as the obligations set forth herein; (ii) hold in strict confidence and not disclose any Confidential Information to any third party, except as permitted herein; (iii) protect and safeguard any and all Confidential Information using the same standard of care as it uses to protect and safeguard its own confidential and/or proprietary information, but in no event less than a reasonable standard of care; (iv) use such Confidential Information only to the extent required for the purposes of this Agreement; (v) not reproduce Confidential Information in any form except as required for the purposes of this Agreement; (vi) not reverse-engineer, decompile, or disassemble any software or devices disclosed by the other party; (vii) not directly or indirectly export or transmit any Confidential Information to any country to which such export or transmission is restricted by regulation or statute; and (viii) promptly provide the other party with notice upon discovery of any loss or unauthorized disclosure of the Confidential Information. Each party shall be liable for any failure of its Representatives to abide by the provisions of this Agreement as if such failure was the act or omission of such party.

c. Notwithstanding the foregoing, either party may disclose Confidential Information (i) to the extent required by a court of competent jurisdiction or other governmental authority or otherwise as required by applicable Laws; or (ii) on a "need-to-know" basis and under an obligation of confidentiality to its legal counsel, accountants, banks and other financing sources and their advisors, or to a Qualified Security Assessor ("**QSA**") for the purpose of assessing compliance with the Payment Card Industry Data Security Standards ("**PCI-DSS**").

d. All Confidential Information (including all copies thereof) shall remain the property of the disclosing party. Upon the request of the disclosing party, the receiving party shall either (a) return such materials to the disclosing party; or (b) certify in writing as to the destruction thereof.

8. [Intentionally Omitted].

9. PCI-DSS. Spreedly represents and warrants that, at all times during the Term of this Agreement, it shall be fully compliant with PCI-DSS and all other applicable standards and guidelines issued by the PCI Security Standards Council, LLC, (the "**Council**") as modified from time to time, and shall, on request or on a periodic basis in accordance with the Card Rules (as defined below), provide proof thereof. In addition:

a. Spreedly covenants, represents and warrants that, at all times during the duration of this Agreement, it complies with and will comply with all Laws applicable to providing the Service as contemplated under this Agreement, and additionally, all applicable rules and guidelines regarding service providers, third-party agents and processors as issued by the Card Associations (the "**Card Rules**"), as updated from time to time, and including Card Rules applicable to U.S. and international credit card transactions. The term "**Card Associations**" means MasterCard, VISA, American Express, Discover, JCB or any other credit card brand or payment card network for or through which Spreedly Processes payment card transactions. "**Processes**," "**Processed**" or "**Processing**" shall mean any operation in relation to Personal Information irrespective of the purposes and means applied including, without limitation, access, collection, retention, storage, transfer, disclosure, use, erasure, destruction, and any other operation. "**Personal Information**" means any information that identifies or could reasonably be used to identify an individual person, including but not limited to names, cardholder data social security numbers, driver's license numbers, tax identification numbers, addresses and telephone numbers), or any information which is compiled or derived from any of the foregoing.

b. Spreedly represents and warrants that it validates its PCI-DSS compliance as required by the applicable Card Rules, and, as of the effective date of this Agreement, Spreedly has complied with all applicable requirements to be considered compliant with PCI-DSS, and has performed all necessary steps to validate its compliance with the PCI-DSS. Without limiting the foregoing, Spreedly represents and warrants: (i) that it undergoes an Annual On-Site PCI Data Security Assessment ("**Annual Assessment**") by a QSA and pursuant to its most recent Assessment, it is currently certified as compliant with the current version of PCI-DSS by the QSA; (ii) that it undergoes a quarterly network scan ("**Scan**") by an approved scanning vendor ("**ASV**") and that it is has passed its most recent scan.

c. Spreedly will notify Customer within seven (7) days if it (i) receives a non-compliant Annual Assessment from a QSA; (ii) fails to undergo or complete any Annual Assessment prior to the expiration of the previous year's Annual Assessment; (iii) is unable to pass a Scan; or (iv) is no longer in compliance with PCI-DSS.

d. Spreedly agrees to supply Customer with evidence of its most recent Annual Assessment prior to or upon execution of this Agreement. Thereafter, Spreedly shall annually supply to Customer, or make available on www.spreedly.com, evidence of Spreedly's successful completion of its Annual Assessment and will, upon reasonable request, supply Customer with additional evidence of its overall PCI-DSS compliance status.

e. Spreedly shall, with respect to the Customer's data, use only validated third-party payment applications that have been certified as compliant with the Council's Payment Application Data Security Standards ("**PA-DSS**"), as updated from time to time.

f. Customer may elect at any time to perform an automatic export of any card data or other credit card or user information associated with Customer's account to a third party endpoint for which Spreedly supports third-party vaulting (a "**Supported TPV Endpoint**") as set forth at: https://docs.spreedly.com/guides/third-party-vaulting/. For any endpoint that is not a Supported TPV Endpoint, Customer may request that Spreedly perform one (1) free-of-charge manual export during the Term, of any card data or other credit card or user information associated with Customer's account to a recipient designated by Customer, provided the recipient has proven that it is PCI-DSS compliant and the transfer is not in violation of any applicable Laws. If Customer requires additional manual exports during the Term, each additional manual export shall incur a $1,000 charge. Spreedly reserves the right to delete all of Customer's card data and any other account data stored on its servers 30 days after the effective date of termination of this Agreement and expiration of any applicable Transition Period (the "**Data Transfer Window**"). If Customer requires additional time to arrange the export of its card data to a PCI compliant third party, it may extend the Data Transfer Window for additional 30 day periods by paying the prorated Base Annual Fee as determined in accordance with Exhibit A of this Agreement.

10. Security. Without limiting the requirements of this Agreement, Spreedly agrees that all Customer Confidential Information (including Personal Information) will be secured from unauthorized access, use, disclosure, loss, theft and Processing using industry standard security practices and technologies. Without limiting the foregoing, Spreedly represents and warrants the following:

a. Spreedly has in place and will comply in all material respects with a comprehensive, written information security program designed to protect the information under its custody, management or control, including all Customer Confidential Information. Spreedly's information security program satisfies the requirements of all data security Laws applicable to Spreedly, and includes the following safeguards: (i) secure business facilities, data centers, servers, back-up systems and computing equipment including, but not limited to, all mobile devices and other equipment with information storage capability; (ii) network, device application, database and platform security; (iii) secure transmission, storage and disposal; (iv) authentication and access controls within media, applications, operating systems and equipment; (v) encryption of Customer Confidential Information placed on any electronic notebook, portable hard drive or removable electronic media with information storage capability, such as compact discs, USB drives, flash drives, tapes; (vi) encryption of Personal Information in transit and at rest; (vii) Personal Information must not be Processed in test, development or non-production environments; and (viii) Personnel security and integrity including, but not limited to, background checks consistent with applicable Law and the requirements of this Agreement. "**Personnel**" means a party's officers, directors, employees and authorized agents who contribute to the performance of such party's obligations under this Agreement. For purposes of the foregoing, a party and its officers, directors, employees and authorized agents shall not be deemed Personnel of the other party.

b. Spreedly shall regularly, but in no event less than annually, evaluate, test and monitor the effectiveness of its information security program and shall promptly adjust and/or update such programs as reasonably warranted by the results of such evaluation, testing, and monitoring.

c. All Spreedly Personnel with access to Customer Confidential Information are provided appropriate information security and privacy training to ensure their compliance with Spreedly's obligations and restrictions under this Agreement, with applicable Laws and with Spreedly's information security program.

11. Breaches of Security.

a. "**Breach of Security**" means (i) any loss, misuse, compromise, or unauthorized access to Personal Information that Spreedly collects, generates, or obtains from or on behalf of Customer, or (ii) any other act or omission that compromises or undermines the physical, technical, or organizational safeguards put in place by Spreedly in Processing such information or otherwise providing services under this Agreement.

b. If there is a Breach of Security, Spreedly will (i) notify Customer within 24 hours of becoming aware of such occurrence and will provide such notice to Customer by contacting the primary Customer Contact set forth above, (ii) promptly investigate the Breach of Security to attempt to determine the root cause, (iii) consult with Customer in good faith about remediation and mitigation plans, and (iv) take all steps reasonably necessary to promptly remediate the effects of such occurrence, ensure the protection of those data subjects that are affected or likely to be affected by such occurrence, prevent the re-occurrence, and comply with applicable Laws.

c. Spreedly will, at its own cost, make all notifications, including to data subjects, regulatory authorities and credit reporting agencies, that are required by applicable Law or any Card Association. Spreedly shall not inform any third party of any Breach of Security, except other affected Spreedly customers or as may be required by applicable Law, without first obtaining Customer's prior written consent, which shall not be unreasonably withheld.

12. Insurance. At all times during the Term, Spreedly will maintain (i) general commercial liability, workers compensation, employers liability and any other insurance required by law or appropriate to operation of its business and (ii) errors and omissions/professional liability and cyber liability/computer crimes liability insurance which expressly (i) covers breach, loss of or unauthorized access to data or systems and other computer or employee crimes and (ii) applies to Customer's data and any other property of Customer under Spreedly's control. All insurance will be rated A-VII or higher and will have commercially reasonable limits commensurate with industry practices (but in any event no less than Two Million Dollars ($2,000,000) per claim and Five Million Dollars ($5,000,000) aggregate for the liability policies). Provider will provide certificates of insurance and add Customer as an additional insured upon request.

13. Indemnification.

a. Spreedly shall indemnify, defend and hold harmless the Customer Parties and their respective officers, directors, employees, successors and assigns (collectively, the "**Customer Indemnified Parties**") against any loss or damage that the Customer Indemnified Parties may sustain or incur (including attorneys' fees and costs), in relation to any claim or action by a third party (including, without limitation, any regulatory or government authority) (each a "**Claim**"), arising out of or related to any of the following: (i) any claim that the Service infringes, violates or misappropriates a patent, copyright, trademark, trade secret or other intellectual property right of any third party (collectively, "**Third-Party IP Rights**"); (ii) any breach by Spreedly of Section 7 (Confidential Information), Section 9 (PCI-DSS) or Section 10 (Security); (iii) any Breach of Security that is caused by Spreedly's breach of its security obligations set forth in Section 10 or the Data Security Addendum; or (iv) Spreedly's (or its subcontractors' or Personnel's) gross negligence, fraud, or willful misconduct.

b. Customer shall indemnify, defend and hold harmless Spreedly against any loss or damage that Spreedly may sustain or incur (including attorneys' fees and costs), in relation to any Claim arising out of or related to any of the following any actual or alleged infringement of any patent, copyright, trademark, or other proprietary or intellectual property right to which Spreedly becomes subject due to data Customer provides to Spreedly for provision of the Service and Spreedly's use thereof in accordance with the terms of this Agreement and/or any service or product delivered by Customer in connection with the Service (excluding the Service itself).

c. Each party shall promptly notify the other party in writing of any Claim for which such party believes it is entitled to be indemnified pursuant to Section 13.a or 13.b. The party seeking indemnification (the "**Indemnitee**") shall cooperate with the other party (the "**Indemnitor**") at the Indemnitor's sole cost and expense. The Indemnitor shall promptly assume control of the defense and investigation of such Claim and shall employ counsel of its choice to handle and defend the same, at the Indemnitor's sole cost and expense. The Indemnitee's failure to perform any obligations under this Section 13.c will not relieve the Indemnitor of its obligations under this Section 13 except to the extent that the Indemnitor can demonstrate that it has been materially prejudiced as a result of such failure. The Indemnitee may participate in and observe the proceedings at its own cost and expense with counsel of its own choosing. The Indemnitor shall not enter into any settlement that imposes any liability or obligation on the Indemnitee without the Indemnitee's prior written consent.

14. Limitation of Liability.

a. EXCEPT AS SET FORTH IN SECTION 14.d, IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY LOST PROFITS, OR ANY INDIRECT, EXEMPLARY, PUNITIVE, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF BUSINESS PROFITS) ARISING OUT OF OR RELATING TO THIS AGREEMENT, HOWEVER CAUSED, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

b. EXCEPT AS SET FORTH IN SECTION 14.c or 14.d, UNDER NO CIRCUMSTANCES SHALL EITHER PARTY'S LIABILITY TO THE OTHER PARTY UNDER THIS AGREEMENT FOR DIRECT DAMAGES EXCEED THE AMOUNT OF FEES PAID (AND, WITH RESPECT TO CUSTOMER'S LIABILITY, DUE AND PAYABLE) TO SPREEDLY BY CUSTOMER UNDER THIS AGREEMENT DURING THE TWELVE MONTH PERIOD IMMEDIATELY PRECEDING SUCH CLAIM (THE "**GENERAL LIABILITY CAP**").

c. NOTWITHSTANDING THE FOREGOING, EACH PARTY'S AGGREGATE LIABILITY FOR LIABILITIES RESULTING FROM: (1) A BREACH OF SECURITY, SECURITY INCIDENT (AS DEFINED IN THE DATA SECURITY ADDENDUM) AND/OR REMEDIAL ACTIONS (AS DEFINED IN THE DATA SECURITY ADDENDUM), (2) A BREACH OF SECTION 7 (CONFIDENTIAL INFORMATION), (3) A BREACH OF SECTION 10 (SECURITY), OR (4) INDEMNIFICATION (SECTION 13), SHALL NOT EXCEED THE GREATER OF: (X) $2,000,000 OR (Y) 10X THE FEES PAID BY CUSTOMER UNDER THIS AGREEMENT DURING THE TWELVE MONTH PERIOD IMMEDIATELY PRECEDING SUCH CLAIM (THE "**SUPER LIABILITY CAP**"). 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 14.c. FOR AVOIDANCE OF DOUBT, THE PARTIES AGREE THAT THE FOLLOWING LIABILITIES SHALL BE DEEMED DIRECT DAMAGES THAT ARE RECOVERABLE UNDER THIS SECTION 14.c.: (I) ANY SETTLEMENT AMOUNTS ARISING FROM SPREEDLY'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 13; (II) ANY DAMAGES FINALLY AWARDED BY A COURT OF COMPETENT JURISDICTION AND ARISING FROM SPREEDLY'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 13; (III) THE REMEDIATION COSTS (AS DEFINED IN THE DATA SECURITY ADDENDUM); AND (III) ANY FINES, PENALTIES, NON-COMPLIANCE FEES OR SIMILAR AMOUNTS ASSESSED OR IMPOSED BY A GOVERNMENTAL AUTHORITY OR CARD ASSOCIATION IN CONNECTION WITH BREACH OF SECURITY OR SECURITY INCIDENT.

d. NOTWITHSTANDING THE FOREGOING, (1) THE LIMITATIONS AND EXCLUSIONS OF LIABILITY IN SECTION 14.a, 14.b AND 14.c DO NOT APPLY TO THE FRAUDULENT, CRIMINAL OR GROSSLY NEGLIGENT OR MORE CULPABLE ACTS OR OMISSIONS OF A PARTY.

15. Assignment. The parties' rights and obligations under this Agreement will bind and inure to the benefit of their respective successors and permitted assigns. Neither party shall assign or delegate its obligations under this Agreement either in whole or in part without the prior written consent of the other party; provided, however, that either party may assign this Agreement in its entirety, without the other party's consent, to an entity that acquires all or substantially all of the business or assets of the assigning party relating to the subject matter of this Agreement, whether by merger, reorganization, acquisition, sale or otherwise.

16. Notices. Any notices required to be delivered in writing hereunder shall be sent to the party's address set forth in Part A and shall be deemed delivered when (i) by personal delivery (when actually delivered); (ii) by overnight courier (upon written verification of receipt); or (iii) by certified or registered mail, return receipt requested (upon verification of receipt). Either party may change its address at any time by giving written notice of the change to the other party.

17. Force Majeure. Neither party will be liable for failure or delay in performance due to causes beyond its reasonable control, including without limitation acts of God, terrorism, war, riots, fire, earthquake, flood or failure of internet or communications infrastructure. Notwithstanding the foregoing, if any force majeure event lasts more than thirty (30) days, Customer will have the right to terminate the Agreement.

18. Survival. Sections 3.a (Ownership), 4.c and 14.d (Effect of Termination), 4.e (Transition), 7 (Confidential Information), 13 (Indemnification), 14 (Limitation of Liability), 18 (Survival) and 19 (Miscellaneous) will survive expiration or termination of this Agreement.

19. Miscellaneous. This Agreement shall be governed by the Laws of the State of Delaware (without regard to its choice of law provisions). Each party irrevocably waive any and all rights they may have to trial by jury in any judicial proceeding involving any claim relating to or arising under this Agreement. This Agreement contains the final, complete and exclusive agreement of the parties relative to the subject matter hereof and supersedes all prior and contemporaneous understandings and agreements relating to its subject matter and may not be changed, modified, amended or supplemented except by a written instrument

signed by both parties. If any provision of this Agreement is found by a proper authority to be unenforceable or invalid, such unenforceability or invalidity shall not render this Agreement unenforceable or invalid as a whole and in such event, such provision shall be changed and interpreted so as to best accomplish the objectives of such provision within the limits of applicable Law or court decisions. The parties are independent contractors and this Agreement does not create an agency, partnership, joint venture, employee/employer or other similar relationship between them. The failure to require performance of any provision shall not affect a party's right to require performance at any time thereafter, nor shall a waiver of any breach or default of this Agreement constitute a waiver of any subsequent breach or default or a waiver of the provision itself.

20. Notification of Material Change.

a. If Spreedly undergoes a Change in Control, it shall provide Customer with written notice thereof within thirty (30) days after Spreedly has consummated such Change in Control transaction. For purposes hereof, "Change in Control" means the acquisition of Spreedly by a third party entity of fifty percent (50%) or more of the outstanding voting securities of Spreedly by means of any transaction or series of related transactions (including, without limitation, any stock acquisition, merger or consolidation, but excluding any sale of stock for capital raising purposes) other than a transaction or series of related transactions in which the holders of the voting securities of Spreedly outstanding immediately prior to such transaction or series of related transactions retain at least a majority of the total voting power represented by the outstanding voting securities.

b. Spreedly shall notify Customer as soon as reasonably practicable of any of the following if such changes are reasonably likely to have a material or significant impact on the Service or Spreedly's ability to perform any of its obligations under this Agreement: financial difficulty, insolvency event, third-party service or system interruption, PCI-DSS compliance lapse, or enforcement, litigation or other regulatory action against Spreedly.

[SIGNATURES ON FOLLOWING PAGE]

IN WITNESS WHEREOF, authorized representatives of the parties have executed this Agreement as of the last date of signature below:

Spreedly, Inc.

DocuSigned by:

By:

C9132818B2F844A...

Name: Justin Benson

Title: CEO

Date: 2/28/2020

Customer: OpenTable, Inc.

DocuSigned by:

By: Joseph Essas

AEB4428E93C548A...

Name: Joseph Essas

Title: CTO

Date: 2/28/2020

EXHIBIT A

PRICING

The initial term of this agreement is 12 months. Customer shall pay Spreedly a "**Base Annual Fee**" of $85,000 for each 12 months of service, which shall entitle Customer to the following for the duration of the Term:

Enterprise Pricing Table	
Enterprise Platform Fee:	**$75,000**
Enterprise Assurance Agreement & SLAs	Included
Existing Spreedly Endpoints	Unlimited
PCI Compliant Card Storage Limit	Unlimited
Add New Standard PMD Endpoints	Included
API Usage Fee:	**$10,000**
Included API Calls	2,000,000
Cost per API Call	$.005
Total Base Annual Fee	**$85,000**

In the event Customer's actual API usage exceeds the included volumes used to determine the Base Annual Fee, Spreedly will bill Customer monthly in arrears at a rate determined by the contract month in which the Customer first exceeds the included API volume.

- If the overage first occurs in Months 1 through 10: billed at $.01 per API call for the remainder of the contract term.
- If the overage first occurs in Month 11 or 12: billed at $.0075 per API call for the remainder of the contract term.

Customer may also or instead elect to purchase additional blocks of 1,000,000 API calls at the contract rate of $0.005 per API call any time during the Initial or Renewal Term. Each additional block of API calls purchased will conform with the current term and will be added to the API usage allotment and expire at the end of that term.

Enterprise Account Management
All enterprise accounts benefit from support prioritization and a named account manager.

Payment
Customer will pay the Base Annual Fee for the first year of the Initial Term in full within 15 days of the Effective Date. Each subsequent annual payment shall be invoiced 30 days prior to the anniversary of the Effective Date ("**Annual Renewal Date**") and shall be due and payable prior to the Annual Renewal Date. All payment obligations hereunder are non-cancelable and all fees paid hereunder are non-refundable.

All payments to be made under this Agreement shall be made in cleared funds, without any deduction or set-off, and free and clear of, and without deduction for or on account of any taxes, levies, imports, duties, charges, fees and withholdings of any nature now or hereafter imposed by any government, fiscal or other authority, save as required by law. If Customer is compelled to make any such deduction, it will pay Spreedly such additional amounts as are necessary to ensure receipt by Spreedly of the full amount which Spreedly would have received but for the deduction.

Total fees owed under this contract:

- Year 1: $85,000

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

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

Receiver:	Silicon Valley Bank
ABA/Routing #:	121140399
SWIFT Code:	SVBKUS6S
Beneficiary:	3301451580 Spreedly, Inc. 733 Foster Street, Suite 100 Durham, NC 27701 USA

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

EXHIBIT B

SERVICE LEVEL AGREEMENT

Service Level Agreement

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

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

Remedies

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

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

Service Credits may not be redeemed for cash and shall be applied to Customer's next applicable payment of Base Annual Fee. Notwithstanding the foregoing, Spreedly has no obligation to issue any Service Credit unless Customer requests such Service Credit in writing within ten (10) days of the Service Level Failure. Customer shall also have the right to terminate the Agreement if: (a) the Transaction Processing Service availability in any given calendar month is less than 98%; and/or (b) a Service Failure occurs in any three (3) calendar months within any five (5) consecutive calendar month period.

The foregoing termination rights and the issuance of Service Credits, collectively, set forth Spreedly's sole obligation and liability and Customer's sole remedy for Service Level Failures.

EXHIBIT C

Support

Spreedly will provide email support between 8.30 am and 8.00 pm (US Eastern timezone). Customer and its employees and consultants can contact Spreedly 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. Spreedly will maintain a sufficient number of Spreedly Support Contacts to ensure timely responses to emails from Customer and to otherwise satisfy Spreedly's obligations under this Exhibit C.

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

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

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

Open Table will be assigned a dedicated Enterprise Account Manager, included with this agreement, and will be the primary point of contact and escalation point in the event of a critical issue/request.

EXHIBIT D

DATA SECURITY ADDENDUM

(SEE ATTACHED)

EXHIBIT D

OpenTable Data Security Addendum

This OpenTable Data Security Addendum, inclusive of Appendix 1 ("**Addendum**") sets out the essential terms required by OpenTable, Inc., a Delaware corporation with its principal place of business located at 1 Montgomery St., Suite 700, San Francisco, California 94104 and/or its applicable subsidiary(ies) ("**OpenTable**"), for Spreedly, Inc. (the "**Provider**") who collects, processes, receives or otherwise has access to OpenTable Data (as defined below). With respect to the OpenTable Data, OpenTable is the data controller of such data and Provider will operate as a data processor of such data.

1. Definitions:

   a. "Agreement" means the Service Agreement dated 2/28/2020, 2020 between the parties under which Provider receives, collects, accesses or otherwise processes OpenTable Data. This Addendum incorporates the terms and conditions of the Agreement and as set forth below. In the event of any conflict between any term of the Agreement and any of this Addendum, the terms of this Addendum shall govern and prevail. All capitalized terms used but not defined herein shall have their respective meanings as set forth in the Agreement.

   b. "OpenTable Data" means any data that is provided by OpenTable to Provider through the Service or collected, accessed or processed by Provider through the Service on behalf of OpenTable, including any Personal Data.

   c. "Personal Data" means any information that can be used to identify, locate, or contact an individual including: (i) first and last name; (ii) home or other physical address; (iii) telephone number; (iv) email address or online identifier associated with an individual; (v) social security number, passport number, driver's license number, or similar identifier; (vi) credit or debit card number; (vii) employment, financial or health information; (viii) IP address or device identifier, or (ix) any other information relating to an individual, including cookie information and usage and traffic data or profiles, that is combined with any of the foregoing.

   d. "Service" means the services provided by Provider under the Agreement.

2. Use of OpenTable Data. Except as expressly permitted in writing by OpenTable, Provider will not directly or indirectly (1) disclose, sell, distribute or transmit the OpenTable Data to any third party, or (2) use the OpenTable Data for any purpose other than to provide OpenTable the Service hereunder at the direction of and in accordance with the instructions of OpenTable, and in accordance with all applicable privacy and data protection laws. Provider will notify OpenTable in writing promptly upon making a determination that it has not met, or can no longer meet, its obligations under this Section 2 of this Addendum, and, in such case, will abide by OpenTable's written instructions, including instructions to cease further processing of the Personal Data, and take any reasonably requested steps to remediate any processing of such Personal Data not in accordance with this Section 2 of this Addendum.

3. EU Personal Data. If the OpenTable Data that Provider processes contains Personal Data of residents of the European Union ("**EU**"), then Provider shall at all relevant times for purposes of this Addendum, maintain a "current" certification status with the EU-U.S. Privacy Shield Framework (the "Framework") related to its processing of Personal Data of residents of the EU and remain at all times in compliance with the requirements of the Framework. Provider will provide OpenTable with ninety (90) days written notice prior to any date on which Provider's "current" certification status ends in accordance with the notice provisions set forth in the Agreement. If Provider is not certified under the Framework as of the date of this Addendum or at any time during the term of this Addendum, Provider then agrees that this Addendum incorporates by reference the European Commission Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries (2010/87/EU) ("**Model Processor Contract**"), where Provider is "data importer," each of OpenTable's affiliates established in the EU are the "data exporter," and the data processing activities in Appendix 1 to the Model Processor Contract shall be such activities as necessary for Provider to perform its services for OpenTable as described in this Addendum, and the data security measures in Appendix 2 to the Model Processor Contract shall be those identified in Section 5 of this Addendum.

4. Subcontractors. To the extent any subcontractors of Provider are required to have access to the OpenTable Data in order to provide the Service, Provider shall (i) impose via written agreement the same privacy, security, and other requirements on any such subcontractor to which Provider is subject under this Addendum; (ii) remain responsible for any subcontractor's actions with respect to the OpenTable Data; and (iii) provide OpenTable with an accurate and complete list of any subcontractors of Provider which have access to the OpenTable Data within two (2) business days of OpenTable's request.

5. Security. Provider has implemented, and will maintain, a comprehensive written information security program ("Information Security Program") that includes administrative, technical, and physical safeguards that are designed (i) to ensure the confidentiality, security, integrity, and availability of the OpenTable Data and (ii) to protect against unauthorized access, use, disclosure, alteration or destruction of the OpenTable Data. In particular, the Information Security Program shall include, but not be limited to, the following safeguards where appropriate or necessary to ensure the protection of the OpenTable Data:

   a. Access Controls – policies, procedures, and physical and technical controls: (i) to limit physical access to its information systems, data processing equipment, data processing systems, and the facility or facilities in which they are housed to properly authorized persons; (ii) to ensure that all members of its workforce who require access to the OpenTable Data have appropriately controlled access and will maintain the confidentiality of the OpenTable Data, and to prevent those workforce members and others who should not have access from obtaining access; (iii) to authenticate and permit access only to authorized individuals and to prevent members of its workforce from providing the OpenTable Data or information relating thereto to unauthorized individuals; (iv) to encrypt and decrypt the OpenTable Data where appropriate; and (v) to ensure that data collected for different purposes can be processed separately.

   b. Security Awareness and Training – a security awareness and training program for all members of Provider's workforce (including management) who have access to the OpenTable Data, which includes training on how to implement and comply with its Information Security Program.

   c. Security Incident Procedures – policies and procedures to detect, respond to, and otherwise address Security Incidents (as defined herein), including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into the OpenTable Data or information systems relating thereto, and procedures to identify and respond to suspected or known security or privacy incidents, mitigate harmful effects of such incidents, and document such incidents and their outcomes.

   d. Contingency Planning – policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages the OpenTable Data or systems that contain the OpenTable Data, including a data backup plan, a Business Continuity Plan (BCP) and a disaster recovery plan.

   e. Device and Media Controls – policies and procedures that govern the receipt and removal of hardware and electronic media that contain the OpenTable Data into and out of a Provider facility, and the movement of these items within a Provider facility, including policies and procedures to address the final disposition of the OpenTable Data, and/or the hardware or electronic media on which it is stored, and procedures for removal of Personal Data from electronic media before the media are made available for re-use. Provider shall ensure that no the OpenTable Data is downloaded or otherwise stored on laptops or other portable devices.

   f. Audit Controls – hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance therewith, and measures to ensure that it is possible to check and establish whether and by whom data have been input into data processing systems or removed.

   g. Data Integrity – policies and procedures to ensure the confidentiality, integrity, and availability of the OpenTable Data and protect it from disclosure, improper alteration, or destruction.

h. Storage and Transmission Security – technical security measures to guard against unauthorized access to the OpenTable Data that is being transmitted over an electronic communications network, including a mechanism to encrypt Personal Data in electronic form while in transit and at rest in storage on networks or systems to which unauthorized individuals may have access, and to ensure that it is possible to check and establish to which bodies the transfer of Data by means of data transmission facilities is envisaged.

i. Storage Media - policies and procedures to ensure that prior to any storage media containing OpenTable Data being assigned, allocated or reallocated to another user, or prior to such storage media being permanently removed from a facility, Provider will irreversibly delete such OpenTable Data from both a physical and logical perspective, such that the media contains no residual data, or if necessary physically destroy such storage media such that it is impossible to recover any portion of data on the media that was destroyed. Provider shall maintain an auditable program implementing the disposal and destruction requirements set forth in this Section for all storage media containing OpenTable Data.

j. Assigned Security Responsibility – Provider shall designate a security official responsible for the development, implementation, and maintenance of its Information Security Program. Provider shall inform Provider as to the person responsible for security.

k. Testing – Provider shall regularly test the key controls, systems and procedures of its Information Security Program, including all production and non-production environments, to ensure that they are properly implemented and effective in addressing the threats and risks identified. Tests should be conducted or reviewed by reputable independent third parties or staff independent of those that develop or maintain security programs. Provider shall ensure that the scope of regular third party (not consisting of internal staff) tests includes penetration testing of CDE, non CDE, pre-production, and production systems, applications, and endpoints on an annual basis at a minimum, and, Provider will provide OpenTable with the summary results of such testing within thirty (30) days of OpenTable’s written request. Additionally, Provider will engage with an accredited independent third party to conduct (on at least an annual basis) ongoing Red Team exercises that ensure the highest levels of security and vulnerability risk mitigation and provide OpenTable with the summary results of such testing upon OpenTable’s written request.

l. Adjust the Program – Provider shall monitor, evaluate, and adjust, as appropriate, the Information Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of the Personal Data, internal or external threats to Provider or the OpenTable Data, and Provider's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

6. Compliance, Reports & Inquiries.

a. Provider will obtain SOC-2 Type I certification effective August 31, 2020 (“SOC-2 Type I Certification”) and Type II certification by December 31, 2020 (“SOC-2 Type II Certification”) (collectively, “SOC-2 Certification”). Provider will provide OpenTable with updates on its SOC-2 Type I and Type II Certification at completion, and promptly upon request by OpenTable. Upon obtaining certification, Provider will maintain, at a minimum, SOC-2 Type II report compliance audit documentation, or its equivalent, during the Term and will provide a copy (without charge) to OpenTable at least once per year during the Term upon written request by OpenTable.

b. Prior to obtaining SOC-2 Certification, Provider shall maintain (for three (3) years after the Agreement ends) complete and accurate records relating to its processing of OpenTable hereunder and its compliance with this Addendum. OpenTable may audit such records during regular business hours, with reasonable advance notice and subject to reasonable confidentiality procedures. OpenTable may not audit Provider more than once annually unless an audit reveals a noncompliance or is needed to satisfy OpenTable’s own legal compliance obligations.

c. To the extent Provider has access to, stores, processes, or transmits credit card information, Provider agrees to provide the evidence of compliance with PCI DSS based on the Provider's Merchant Level and/or Provider status (i) on the date hereof, (ii) annually thereafter during the term of the Agreement, and (iii) upon request from OpenTable.

d. Upon OpenTable's reasonable request, Provider will provide OpenTable with information demonstrating that it maintains information security controls aligned with the requirements in this Addendum.

e. Provider will provide OpenTable with the contact details of Provider's global data privacy lead, chief privacy officer, data protection officer, or other employee appointed by Provider to address data privacy issues.

f. Provider will cooperate with OpenTable in connection with any audits or inquiries conducted by any data protection authorities, courts, and/or other authorities related to the processing of the Personal Data via the Service, including by providing support to OpenTable with respect to (i) assisting OpenTable in responding to data subject requests for exercising data subject rights under applicable law, including erasing or blocking Personal Data without delay on OpenTable's instruction; (ii) assisting OpenTable in responding to data protection authority or other regulatory requests for information related to Provider's processing; and (iii) providing all information necessary related to Provider's processing for OpenTable to demonstrate compliance with applicable data protection laws.

g. Provider shall promptly notify OpenTable if it receives a request for subject access, rectification, cancellation, objection or any other data protection related requests, and, should any court, government agency or law enforcement agency contact Provider with a demand for any OpenTable Data, Provider will direct the law enforcement agency to request such information directly from OpenTable. As part of this effort, Provider may provide OpenTable's basic contact information to the agency. If compelled to disclose OpenTable's Data to law enforcement, then Provider will promptly, and without any undue delay, notify OpenTable and deliver a copy of the request (except when Provider is legally prohibited from doing so) to allow OpenTable to seek a protective order or any other appropriate remedy.

7. Security Breach. Provider will notify OpenTable promptly (for the avoidance of doubt, no later than the timeframe required under applicable law) in writing upon discovery of any actual (or as otherwise required by applicable law) breach of, or compromise or unauthorized access to, any OpenTable Data's security or confidentiality (each, a "Security Incident"). The notice will describe the Security Incident, the status of Provider's investigation, and, if applicable, the potential number of persons affected. Provider shall cooperate with OpenTable in the investigation of the Security Incident. To the extent that a Security Incident is caused by Provider's breach of the Agreement and/or its obligations under this Addendum and such Security Incident gives rise to a legal obligation imposed on OpenTable to (i) provide notification to public authorities, individuals, or other persons, or (ii) undertake other remedial measures (including, without limitation, notice, credit monitoring services and the establishment of a call center to respond to inquiries (each of the foregoing a "Remedial Action")), at OpenTable's request, Provider shall, at Provider's cost, undertake such Remedial Actions (all such costs actually incurred by Provider to perform such Remedial Actions, the "Remediation Costs"). Provider will not communicate with any third party regarding any Security Incident except as permitted by applicable Law and/or as otherwise directed by OpenTable in its sole discretion.

8. [Intentionally Deleted.]

9. Additional Agreements. Upon OpenTable's request, Provider shall, and shall cause any third party to which it discloses Personal Data or allows access to Personal Data, to engage in good faith discussions with OpenTable regarding the (i) execution of supplemental data processing agreement(s) with OpenTable or any of its affiliated companies or (ii) need to take other appropriate steps to address cross-border transfer or other data protection requirements, if OpenTable reasonably believes that such steps are necessary to address applicable data protection or privacy laws concerning Personal Data.

10. Term and Termination. This Addendum shall remain in full force and effect for the term of the Agreement and any applicable Transition Period thereof. Upon termination of the Agreement and any applicable Transition

Period, the Provider shall, and shall cause any and all subcontractors to, immediately at OpenTable 's request destroy all copies of such OpenTable Data in a secure manner that is reasonably designed to render the information permanently unreadable and not reconstructable into a usable format (i.e., in accordance with the then-current U.S. Department of Defense, or similar data destruction standard or CESG standards, as applicable). Upon OpenTable's request, Provider shall also promptly certify to OpenTable that it and its subcontractors have carried out Provider's directions as per this Section 10. This Section 10 of this Addendum will survive any termination or expiration of the Agreement.

11. Governing Law. This Addendum will be governed by and construed in accordance with the governing law designated in the Agreement.

In Witness Whereof, this Addendum is entered into and becomes a binding part of the above-referenced Agreement(s) as of the later of the dates beneath the parties' signatures below.

OpenTable, Inc.		**Provider: Spreedly, Inc.**	
By:	DocuSigned by: C9132818B2F844A...	By:	DocuSigned by: Joseph Essas AEB4428F93C548A...
Name:	Justin Benson	Name:	Joseph Essas
Title:	CEO	Title:	CTO
Date:	2/28/2020	Date:	2/28/2020

Appendix 1

Subject Matter
The subject matter of the data processing under this Addendum is the OpenTable Data.

Duration
The duration of the data processing under this Addendum is the period during which Provider performs services for OpenTable under the Agreement or as otherwise required by law.

Purpose
The purpose of the data processing under this Addendum is the provision of the Service under the Agreement (as amended from time to time).

Nature of Processing
The data processing will involve any such processing that is necessary for the purposes set out in the Agreement, this Addendum, and below (as applicable).

[If anything additional, list here:] ________________________________

Type of Personal Data
The types of Personal Data processed are as described in the Agreement (as amended from time to time), this Addendum, and below (as applicable).

[If anything additional, list here:] ________________________________

Categories of Data Subjects
In providing the Service to OpenTable, Provider processes the personal data of the data subjects referenced in the Agreement (as amended from time to time), this Addendum, and below (as applicable).

[If anything additional, list here:] _________________________________