SERVICE AGREEMENT

Part A: Parties

SPREEDLY

Name:	Spreedly, Inc.
Address:	300 Morris Street, Suite 400
City/State:	Durham, NC 27701

CUSTOMER

Name:	Hopper, Inc.
Address:	1-5795 Avenue De Gaspe
City/Country:	Montreal, Quebec H2S 2X3 Canada

PRIMARY SPREEDLY CONTACT

Name:	Shawn Curtis
Title:	Senior Enterprise Account Executive
Phone:	888-727-7750
Email:	shawn@spreedly.com

PRIMARY CUSTOMER CONTACT

Name:	Joost Ouwerkerk
Title:	Co-Founder & Head of Platform
Phone:	N/A
Email:	joost@hopper.com

SPREEDLY FINANCE CONTACT

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

CUSTOMER BILLING CONTACT

Name:	Hopper Accounting Department
Phone:	(514)-276-0760
Email:	invoices@hopper.com

Part B: Terms

1. This Service Agreement (including its exhibits, the "**Agreement**" or "**SA**") is effective as of the last date of signing below ("**Effective Date**") and is between Spreedly, Inc. ("**Spreedly**" or "**Service Provider**")), and the customer listed above (the "**Customer**" or "**Hopper**")). 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.

2. Provision and Use of Service.

   a. Spreedly hereby grants the Customer 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 . At Customer's request, Spreedly will offer such additional professional services to Customer which are mutually agreed upon and described in one or more statements of work ("**Professional Services**") and subject to the requirements of 3rd Party Client Rider (Exhibit E) as applicable.

b. Customer shall comply with all laws, directives, rules and regulations (collectively, "Laws") applicable to its use of the Service and Spreedly reserves the right to restrict access to the Service if it determines, in its sole discretion, that Customer is in violation of this requirement. Customer hereby grants Spreedly authorization to share information with law enforcement about Customer, Customer's transactions and Customer's Spreedly account, in each case if Spreedly reasonably suspects that Customer's use of the Service has been for an unauthorized, illegal, or criminal purpose.

c. Spreedly reserves the right to not store or submit any transaction Customer submits that Spreedly believes is in violation of this Agreement or applicable Law, any other Spreedly agreement, or otherwise exposes Customer or other Spreedly users to harm, including but not limited to, fraud and other criminal acts.

3. Intellectual Property Rights.

a. The Service is licensed and not sold. Spreedly reserves all rights 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 the Service, including without limitation, 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.

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 two (2) years 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 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. Upon termination of this Agreement, (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), except that in the event of a termination than for non-payment of any undisputed amount by Customer, Spreedly shall provide reasonable assistance to enable Customer to access and export in a reasonably usable form all Customer Confidential Information stored on Spreedly systems so as to enable Customer to transition to another provider, and the Parties shall agree on terms for the continued use of Services by Customer until such transition is completed.

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 represents and warrant to Spreedly that: (i) it will not use the Service, directly or indirectly, for any fraudulent undertaking or in any manner so as to interfere with the use of the Service; (ii) it will comply, at its own expense, with all Laws applicable to Customer, this Agreement, Customer's customer data and/or any card authorization, credit, ticket only, capture or settlement request, decline transaction, or other related transaction, completed or submitted under Customer's account, including without limitation: (A) the terms of service of the payment gateways, merchant service providers and/or API endpoints Customer connects with on the Service; (B) the operating rules, bylaws, schedules, supplements and addenda, manuals, instructions, releases, specifications and other requirements, as may be amended from time to time, of any of the payment networks including Visa, MasterCard, American Express, Discover Financial Services, and any affiliates thereof or any other payment network applicable to this Agreement; (C) PCI-DSS and PA-DSS, as applicable; and (D) any regulatory body or agency having jurisdiction over the subject matter hereof.

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

7. Confidential Information.

   a. Each party may disclose or make available its Confidential Information (in such capacity, the "**Disclosing Party**") to the other party (in such capacity, the "**Receiving Party**"). Subject to Section 7.b, "**Confidential Information**" "**Confidential Information**" means any and all technical and non-technical information, in any form or medium (whether in graphic, electronic, written or oral form), which: (i) if disclosed in writing or other tangible form or medium, is marked "confidential" or "proprietary", (ii) if disclosed orally or in other intangible form or medium, is identified by the Disclosing Party or its Representative (as defined below) as confidential or proprietary when disclosed and summarized and marked "confidential" or "proprietary" in writing by the Disclosing Party or its Representative within 30 days after disclosure, or (iii) due to the nature of its subject matter or the circumstances surrounding its disclosure, would reasonably be understood to be confidential or proprietary; including but not limited to, any trade secrets, methods, techniques, drawings, designs, descriptions, specifications, works of authorship (including, without limitation, any software), patent applications or other filings, models, inventions, know-how, processes, algorithms, software source documents, and formulae related to the current, future, and proposed technologies, products and services of the Disclosing Party, and also any information concerning research, experimental work, development, engineering, financial information, purchasing, customer lists, pricing, investors, employees, business and contractual relationships, business forecasts, business plans, individually identifiable personal information, sales and merchandising, marketing plans of or related to the Disclosing Party and information the Disclosing Party provides to the other regarding or belonging to third parties. For avoidance of doubt, Spreedly's "Confidential Information" includes the source code for the Service and the methods, algorithms, structure and logic, technical infrastructure, techniques and processes used by Spreedly in developing, producing, marketing and/or licensing the Service.

   b. "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 the Receiving 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 of the Disclosing Party's Confidential Information and without breaching this Agreement.

   c. The Receiving Party shall: (i) only disclose the Disclosing Party's Confidential Information to any of its and/or its affiliates' employees, officers, directors, partners, consultants, contractors, agents and representatives (collectively, its "**Representatives**") that have a need to know such Confidential Information and who have agreed to terms at least as restrictive as those stated in this Agreement; (ii) hold in strict confidence and not disclose any of the Disclosing Party's Confidential Information to any third party, except as permitted herein; (iii) protect and safeguard any and all of the Disclosing Party's Confidential Information using the same standard of care as it uses to protect and safeguard its own Confidential Information, but in no event less than a reasonable standard of care; (iv) use the Disclosing Party's Confidential Information only to the extent required for the purposes of this Agreement; (v) not reproduce the Disclosing Party's 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 Disclosing Party; (vii) not directly or indirectly export or transmit any of the Disclosing Party's Confidential Information to any country to which such export or transmission is restricted by regulation or statute; and (viii) promptly provide the Disclosing Party with notice upon discovery of any loss or unauthorized disclosure of the Disclosing Party's 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.

   d. Notwithstanding the foregoing, the Receiving Party may disclose the Disclosing Party's Confidential Information: (i) to the extent required by a court of competent jurisdiction or other governmental authority or otherwise as required or compelled 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**"). If the Receiving Party or any of its Representatives is compelled to disclose the Disclosing Party's Confidential Information pursuant to clause (i) above then, to the extent permitted by applicable Law, the Receiving Party shall: (x) promptly, and prior to such disclosure, notify the Disclosing Party in writing of such requirement so that the Disclosing Party can seek a protective order or other remedy or waive its rights under Section 7.c; and (y) provide reasonable assistance to the Disclosing Party, at the Disclosing Party's sole cost and expense, in opposing such disclosure or seeking a protective order or other limitations on disclosure. If the Disclosing Party waives compliance or, after providing the notice and assistance required under this Section 7.d, the Receiving Party remains required by Law to disclose any of the Disclosing Party's Confidential Information, the Receiving Party shall disclose only that portion of the Disclosing Party's Confidential Information that the Receiving Party is legally required to disclose and shall use commercially reasonable efforts to obtain assurances from the applicable court or other presiding authority that such Confidential Information will be afforded confidential treatment.

   e. 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 (i) return such materials to the Disclosing Party; or (ii) certify in writing as to the destruction thereof.

f. Each party acknowledges and agrees that a breach or threatened breach by such party of any of its obligations under this Section would cause the other party irreparable harm for which monetary damages would not be an adequate remedy and that, if such breach or threatened breach, the other party will be entitled to equitable relief, including a restraining order, an injunction, specific performance and any other equitable relief that may be available from any court of competent jurisdiction, without any requirement to post a bond or other security, or to prove actual damages or that monetary damages are not an adequate remedy. Such remedies are not exclusive and are in addition to all other remedies that may be available at law, in equity or otherwise.

8. References to Relationship. Customer agrees that, from the Effective Date, Spreedly may identify Customer as a customer of Spreedly and use Customer's logo on our customers page (https://spreedly.com/customers) for the Term of this Agreement.

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 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 any of its Scans; 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, unless such request for manual export is for fulfilment of Customer's obligations to data subject customers under the EU General Data Protection Regulation. 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 (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 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. Supplier Oversight. Spreedly recognizes that the Service provided to Customer hereunder will be used by Customer in connection with products and services that Customer is contracted to provide to third-parties ("**Clients**"). Such Service(s) used by Customer in connection with delivery of products and services to Clients, pursuant to written notice by Customer, shall be provided by Spreedly in accordance with the additional terms set forth in Exhibit E ("**3rd Party Client Rider**") and the Schedules thereto.

13. Insurance. At all times during the Term, Spreedly shall maintain the insurance requirements provided in Article 8 of the 3rd Party Client Rider (Exhibit E).

14. Indemnification.

a. Spreedly shall indemnify, defend and hold harmless Customer against any loss or damage that Customer 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); or (iii) any Breach of Security that is caused by Spreedly's material breach of its security obligations set forth in Section 10.

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: (i) any breach of Section 7 (Confidential Information); and/or (ii) Customer's use of the Service in violation of the terms of this Agreement and/or any applicable Law.

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 14.a or 14.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 14 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.

15. Limitation of Liability.

    a. 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. SUBJECT TO SECTION 15.c BELOW, 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.
    c. NOTWITHSTANDING SECTION 15.b, UNDER NO CIRCUMSTANCES SHALL SPREEDLY'S AGGREGATE LIABILITY TO CUSTOMER FOR DIRECT DAMAGES RESULTING FROM CLAIMS ARISING UNDER ARTICLE 9.1.3 OF EXHIBIT E EXCEED THE GREATER OF: (i) $2,500,000 OR (ii) FIVE (5) TIMES THE AMOUNT OF FEES PAID TO SPREEDLY BY CUSTOMER UNDER THIS AGREEMENT DURING THE TWELVE MONTH PERIOD IMMEDIATELY PRECEDING SUCH CLAIM.
    d. NOTWITHSTANDING THE FOREGOING, THE LIMITATIONS AND EXCLUSIONS OF LIABILITY IN SECTIONS 15.a., 15.b. AND 15.c. DO NOT APPLY TO THE FRAUDULENT, CRIMINAL OR GROSSLY NEGLIGENT OR MORE CULPABLE ACTS OR OMISSIONS OF A PARTY.

16. 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.

17. 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.

18. 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.

19. Survival. Sections 3.a (Ownership), 4.d (Effect of Termination), 7 (Confidential Information), 14 (Indemnification), 15 (Limitation of Liability), 19 (Survival) and 20 (Miscellaneous) will survive expiration or termination of this Agreement.

20. Miscellaneous. This Agreement shall be governed by the Laws of the State of Delaware (without regard to its choice of law provisions). The parties agree that the exclusive venue for any actions or claims arising under or related to this Agreement shall be in the appropriate state or Federal court located in Wake County, North Carolina. 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 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.

[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.		**Hopper, Inc.**	
By:	DocuSigned by: Justin Benson 6793B5D8B8EC48E...	By:	DocuSigned by: 5B0A6ABFE5804AF...
Name:	Justin Benson	Name:	Joost Ouwerkerk
Title:	CEO	Title:	Co-Founder
Date:	May 25, 2021	Date:	May 25, 2021

EXHIBIT A

PRICING

The initial term of this agreement is 24 months. Customer shall pay Spreedly a "**Base Annual Fee**" for each 12 months of service, which shall entitle Customer to the following for the duration of the Term:

Enterprise Pricing Table		
	Year 1	**Year 2**
Enterprise Platform Fee:	**$150,000**	**$150,000**
Enterprise Assurance Agreement & SLAs	Included	Included
Existing Spreedly Endpoints	Unlimited	Unlimited
PCI Compliant Card Storage Limit	Unlimited	Unlimited
Add New Standard PMD Endpoints	Included	Included
API Usage Fee:	**$125,000**	**$140,000**
Included API Calls	50,000,000	70,000,000
Cost per API Call	$0.0025	$0.0020
Total Base Annual Fee	**$275,000**	**$290,000**

API Usage Fees
The API Usage Fee in the table above includes an initial allotment of 50,000,000 API calls in Year 1 and 70,000,000 API calls in Year 2. 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 the contract rate in accordance with the table above ($0.0025 per API call in Year 1 and $0.0020 per API call in Year 2) for the remainder of the contract term.

Customer may also or instead elect to purchase additional blocks of 5,000,000 API calls at the contract rate in accordance with the table above ($0.0025 per API call in Year 1 and $0.0020 per API call in Year 2) any time during the Initial or Renewal Term. Each additional block of API calls purchased will conform with the current Contract Year and will be added to the API usage allotment and expire at the end of that Contract Year.

Pricing Expiration and Signing Discount.
The above pricing is contingent on contract execution on or before May 25, 2021 and Spreedly will apply a one-time $10,000 discount off the Year 1 Enterprise Platform Fee.

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 Initial Term in equal quarterly installments, with the first installment due and payable within 30 days of the invoice Date. Spreedly shall invoice Customer for each subsequent quarterly payment 30 days prior to the three, six and nine month anniversaries of the Effective Date (a "**Quarterly Renewal Date**"), with such amount due and payable prior to the relevant Quarterly Renewal Date. For each subsequent Renewal Term, the first quarterly payment of such Renewal Term 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. Any late payments shall accrue a 1% monthly service fee applied to Customer's outstanding balance. Previously assessed and unpaid service fees are included in the outstanding balance
Fees do not include any taxes. If Spreedly is legally obligated to collect applicable taxes, such taxes shall be invoiced to and paid by Customer, unless Customer provides Spreedly with a valid tax exemption certificate authorized by the appropriate taxing authority.

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.

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.

300 Morris St, Suite 400
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 99.99%, 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).

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 99.99%	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. The issuance of Service Credits sets forth Spreedly's sole obligation and liability and Spreedly's sole remedy for any Service Level Failure.

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.

EXHIBIT C

Support

Spreedly will provide email support between 8.30 am and 8.30 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 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.

EXHIBIT D
Data Privacy Addendum
and
Spreedly Partner GDPR Annex

Compliance with the EU General Data Protection Regulation

Recitals:

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

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

Each of the Agreements contains provisions requiring each party to comply with all applicable laws. This GDPR Annex documents the data protection requirements imposed upon the parties by the GDPR. To the extent applicable, this GDPR Annex is hereby incorporated by reference into each Agreement in order to demonstrate the parties' compliance with the GDPR.

1. For purposes of this Annex, "GDPR" means Regulation (EU) 2016/679, the General Data Protection Regulation, together with any additional implementing legislation, rules or regulations that are issued by applicable supervisory authorities. Words and phrases in this Annex shall, to the greatest extent possible, have the meanings given to them in Article 4 of the GDPR. In particular:

   (a) "Controller' has the meaning given to it in Article 4(7) of the GDPR: "means the natural of legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."

   (b) "Personal Data" has the meaning given to it in Article 4(1) of the GDPR: "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person," but only to the extent such personal data pertains to residents of the European Economic Area (EEA) or are otherwise subject to the GDPR.

   (c) "Personal Data Breach" has the meaning given to it in Article 4(12) of the GDPR: "[any] breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

   (d) "Processing" has the meaning given to it in Article 4(2) of the GDPR: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

   (e) "Subprocessor" means any processor as defined in Article 4(8) of the GDPR: "[any] natural or legal person, public authority, agency or other body which processes personal data" on behalf of the Processor (including any affiliate of the Processor).

   (f) "Transfer" means to disclose or otherwise make Personal Data available to a third party (including to any affiliate or Subprocessor), either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means. Transfer also includes moving the Personal Data within a single party from an EU member State to a country not within the EU, or otherwise making such data accessible outside the EU.

2. In accordance with GDPR Article 28(1), Processor represents that it has implemented appropriate technical and organizational measures in such a manner that its Processing of Personal Data will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects.

3. The Processor will maintain a current list of Subprocessors used throughout the service, including the Subprocessor's name and purpose of their processing. This list will be accessible via http://www.spreedly.com/gdpr/subprocessors. Controllers may receive notifications of new Subprocessors by emailing subprocessor@spreedly.com with the subject "Subscribe" and once subscribed in this manner that Controller will receive notification of new Subprocessors before those Subprocessors are authorized to process Personal Data on behalf of the Processor.

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

4. In accordance with GDPR Article 28(3), the following terms are incorporated by reference into the Agreements:

   (a) The Processor shall only process the Personal Data (i) as needed to provide the Services, (ii) in accordance with the specific instructions that it has received from the Controller, including with regard to any Transfers, and (iii) as needed to comply with law (in which case, the Processor shall provide prior notice to the Controller of such legal requirement, unless that law prohibits this disclosure);

   (b) Processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

   (c) Processor shall take all security measures required by GDPR Article 32, namely:

      i. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

      ii. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

      iii. The Processor shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not process such Personal Data except upon instructions from the Controller, unless the Processor is required to do so by EEA Member State law.

   (d) Taking into account the nature of the processing, Processor shall reasonably assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights;

   (e) Taking into account the nature of processing and the information available to the Processor, Processor shall comply with (and shall reasonably assist the Controller to comply with) the obligations regarding Personal Data Breaches (as set forth in GDPR Articles 33 and 34), data protection impact assessments (as set forth in GDPR Article 35), and prior consultation (as set forth in GDPR Article 36);

   (f) At the Controller's discretion, the Processor shall delete or return all the Personal Data to The Controller after the end of the provision of services relating to Processing, and delete existing copies unless applicable EEA member state law requires storage of the Personal Data;

   (g) The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations laid down in the GDPR, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller; and

   (h) The Processor shall immediately inform The Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

5. The Processor shall not Transfer any Personal Data (and shall not permit its Subprocessors to Transfer any Personal Data) without the prior consent of the Controller. The Processor understands that the Controller must approve and document that adequate protection for the Personal Data will exist after the Transfer, using contracts that provide sufficient guarantees (such as standard contractual clauses) unless another legal basis for the Transfer exists.

6. The Processor will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Data. Processor will notify The Controller without undue delay in the event of any Personal Data Breach.

7. The Processor shall maintain all records required by Article 30(2) of the GDPR, and (to the extent they are applicable to Processor's activities for the Controller) Processor shall make them available to the Controller upon request.

8. The Processor will allow the Controller, or a third-party appointed by the Controller, to conduct audits (including inspections) to verify the Processor's compliance with the Agreements described in this document.

   (a) The Controller may request an audit by emailing success@spreedly.com.

   (b) Following receipt of this request, the Processor and Controller will discuss and agree in advance on the reasonable scope, start date and duration of this audit, as well as any applicable security and confidentiality controls that may be required.

   (c) The Processor may charge a fee (based on the Processor's reasonable costs) for any such audit. The Processor will provide the Controller with additional details of this fee including the basis of its calculation, in advance of the audit. Additionally, the Controller will be responsible for any fees charged by any third-party auditor appointed by the Controller for this audit.

9. In Accordance with GDPR Article 24(1), the following terms are incorporated by reference into the Agreements:

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

Exhibit E

Hopper Software & Professional Services Rider

This Software & Professional Services Rider (this "Rider") shall be attached as Exhibit E to the Service Agreement dated on or about May 25, 2021 entered into between Hopper (USA), Inc. ("Hopper") and Spreedly, Inc. ("Service Provider," and together with Hopper, the "Parties") ("SA"), and shall apply to Hopper's worldwide, limited, non-exclusive, non-transferable license, without the right to sublicense, during the Term, to electronically access and use the Spreedly API to (i) validate, tokenize and vault credit cards and other payment types and process charges against those payment methods and subsequently against payment gateways; and (ii) automatically update expired or lost credit cards, where applicable; and any Professional Services provided by Service Provider to Hopper, in each case pursuant to and as set forth in the SA and/or pursuant to and as set forth in any subsequent order form or statement of work ("SOW") incorporating the terms of this Rider (collectively, the "SA Services"). Capitalized terms used in this Rider but not expressly defined herein shall have the meaning set forth in the SA. If there is a conflict or inconsistency between the terms of this Rider and the SA, the parties shall give the provisions their broadest interpretation so as to reconcile the conflict or apparent conflict. If such an interpretation is not possible then the terms of the Rider shall control, but only in respect to the subject matter herein and specifically excluding the pricing and payment terms in Exhibit A, the terms of Section 15 (Limitation on Liability) and all other terms not addressed in this Rider. If any terms or conditions of this Rider conflict with any terms of the Card Rules, the Card Rules will supersede and control. This Rider cannot be superseded, eliminated, modified or amended except pursuant to a written amendment or agreement executed by the Parties providing expressly for such change to this Rider.

1. Service Provider Personnel	
1.1	**Qualifications**. Service Provider shall assign an adequate number of Service Provider employees and individual independent contractors (collectively, "Service Provider Personnel") to perform the SA Services. Service Provider Personnel shall be properly educated, trained, experienced and fully qualified for the Services they are to perform.
1.2	**Location of Services**. Service Provider is a financial technology company providing services over the internet. As a result of Service Provider's service model, Service Provider is rarely, if ever, required to perform work on-site at a customer facility. If such work becomes necessary, the parties agree to outline the precise nature and scope of such work to be performed in a separate SOW. To the extent so specified in a SOW, Service Provider, shall deliver the Professional Services at or from the Service Provider facility(ies) so specified. Service Provider must obtain Hopper's prior written approval to change any approved facility(ies) in an SOW, including the proposed provision of any Professional Services or any portion thereof at any new or different facility(ies), which approval Hopper may withhold in its sole discretion, not to be unreasonably withheld.

1.3	**Training**. To the extent that Service Provider Personnel are required in connection with the Services to communicate directly with Hopper's end customers and/or Hopper's customer ("End-Customer Facing Services"), (i) Service Provider shall at Hopper's election permit Hopper to provide, training to Service Provider Personnel assigned to provide the End-Customer Facing Services regarding applicable consumer protection laws and Hopper policies and procedures communicated to Service Provider, including unfair or deceptive practices; (ii) As periodically requested by Hopper, Service Provider shall provide written reports to Hopper, which shall include sufficient information to allow Hopper to verify the satisfactory completion of training of any Service Provider Personnel engaged in providing the End-Customer Facing Services to Hopper; (iii) Alternatively, in its sole discretion, Hopper may prepare and provide Service Provider with training materials relevant to the End-Customer Facing Services being provided (which may include web-based training materials); (iv) Service Provider shall cause each of Service Provider Personnel that are involved in the provision of the End-Customer Facing Services (as such classes of employees are reasonably identified by Hopper in consultation with Service Provider) to undertake such training before providing any of the End-Customer Facing Services; and in addition, Hopper shall provide Service Provider with such updated training materials as Hopper deems appropriate, and Service Provider shall promptly cause each of Service Provider Personnel that are involved in the provision of the End-Customer Facing Services affected by such change (as such classes of Service Provider Personnel are reasonably identified by Hopper in consultation with Service Provider) to undertake additional training.
1.4	**Sole Employer**. All Service Provider Personnel are the responsibility and employees of Service Provider, subject to employee tax withholdings to be completed by Service Provider. Service Provider shall be solely responsible for the payment of all compensation and wages (including applicable overtime and hourly pay), employee benefits, and required insurance for Service Provider Personnel (including unemployment and workers' compensation), accommodation and leave and employment authorization (including form I-9 compliance) and immigration laws, in compliance with the laws and regulations applicable where such Personnel are employed. Service Provider shall be solely responsible for the withholding and payment of employment taxes for Service Provider Personnel. Service Provider agrees and acknowledges, for itself and for Service Provider Personnel, that Service Provider Personnel shall not be entitled to any benefits provided to employees of Hopper or its Affiliates, clients or partners, including participation in an employee retirement, pension, supplemental compensation, defined contribution or similar plan; workers' compensation; disability or other similar benefits; unemployment or other similar insurance or otherwise. Service Provider further agrees and acknowledges that Hopper shall not be responsible to Service Provider Personnel for any payment of compensation or wages (including applicable overtime), employee benefits, and insurance (including unemployment and workers' compensation) or for the withholding or payment of employment taxes. Service Provider agrees and acknowledges that Hopper is not the employer or a co-employer of Service Provider Personnel. Service Provider agrees and acknowledges, for itself and for Service Provider Personnel, that Service Provider shall (directly or indirectly through a Service Provider Affiliate or an Approved Subcontractor) at all times remain the employer of all of its employees, including all Service Provider Personnel, (and remain liable for the acts and omissions of all Service Provider Personnel) performing the Services, in whole or in part, and Service Provider shall perform all of the responsibilities of an employer under applicable laws. In particular, Service Provider shall (directly or through a Service Provider Affiliate or an Approved Subcontractor) be responsible for: (A) selecting and hiring Service Provider Personnel legally, including compliance with all applicable laws in connection therewith; (B) assuming full responsibility for the actions and omissions of Service Provider Personnel while performing the Services; (C) providing the supervision, direction and control of Service Provider Personnel; (D) paying Service Provider Personnel

	compensation and wages (including applicable overtime and hourly pay) and benefits, including providing all Service Provider Personnel with all such benefits as may be required by applicable law and/or by the terms of any employee retirement, pension, supplemental compensation, defined contribution or similar plan in or to which Service Provider or any Service Provider Personnel participates or contributes; (E) paying or withholding all required payroll taxes and mandated insurance premiums, including making payments to the appropriate governmental authorities for any and all statutory withholdings and other amounts in connection with any and all governmental taxes or fees; (F) providing workers' compensation coverage for Service Provider Personnel as required by applicable law; (G) fulfilling its obligations with respect to unemployment compensation; and (H) making any required withholdings from payments to Service Provider Personnel with respect to payments to any union, club or other organization of or to which Service Provider or any member of Service Provider Personnel is a member or is subject.
1.5	**Harassment and Discrimination**. In the event that Service Provider is providing Professional Services to Hopper, at a Hopper site or facility, at Hopper's request, Service Provider shall provide to Hopper its respective policies on illegal harassment and discrimination to Service Provider Personnel, including identification of the processes to be used by Service Provider Personnel to make internal complaints of any violations for investigation by Service Provider, as applicable.
1.6	**Claims**. Service Provider must promptly notify Hopper of any actual or threatened lawsuits, administrative charges or other proceedings, demands, or complaints filed internally or externally that arise from or relate to Service Provider Personnel and that are based on events allegedly occurring on a Hopper site or alleged conduct by any employee, customer or agent of Hopper, or of its Affiliates, clients or partners ("Service Provider Personnel Claims"). Service Provider will reasonably cooperate with Hopper regarding any investigation of Service Provider Personnel Claims. Service Provider agrees that it will conduct a prompt and thorough investigation of any Service Provider Personnel Claims and undertake appropriate remedial and corrective actions, if needed.
1.7	**[Intentionally Omitted]**
1.8	**Resources**. Except to the extent specifically provided otherwise in a statement of work or elsewhere in the SA, Service Provider shall be responsible for providing all resources (including facilities, personnel, equipment and software, and any associated third-party consents thereto) necessary to provide the Services and shall recover the costs and expenses of such resources through the charges identified in the applicable statement of work or the SA. Service Provider shall remain responsible for the obligations, services, and functions performed by any Service Provider Personnel to the same extent as if such obligations, services, and functions were performed directly by Service Provider, and for purposes of the SA, all work performed by Service Provider Personnel shall be deemed work performed by Service Provider.
2. Service Levels	
2.1	**Service Levels**. Service Provider shall perform the Services in accordance with the Service Levels, as set forth in Exhibit B of the SA ("**SLA Addendum**").

2.2	**Failure to Meet Service Levels**. Each time Service Provider fails to meet a Service Level, Service Provider shall promptly: 1. investigate, assemble, and preserve pertinent information with respect to, and report on the causes of, the problem, including performing a root cause analysis of the problem(s); 2. advise Hopper, as and to the extent requested by Hopper, of the status of remedial efforts being undertaken with respect to such problem; 3. minimize the impact of and correct the problem(s) and begin meeting the Service Level requirements; 4. take appropriate preventive measures so that the problem does not recur; and 5. demonstrate to Hopper's reasonable satisfaction that causes of the problem have been or will be corrected permanently. If Service Provider fails to meet any Service Levels, then in addition to other remedies available to Hopper, Service Provider shall pay or credit to Hopper any Service Level Credits specified in the SLA Addendum ("Service Credits"). Any such Service Credits reflect the diminished value of the Services resulting from Service Provider's failure to meet the agreed upon Service Levels, and are not a penalty.
2.3	**Measurement and Monitoring Tools**. Service Provider shall utilize the necessary measurement and monitoring tools and procedures required to measure and report Service Provider's performance of the Services against the applicable Service Levels. Such measurement and monitoring shall permit reporting at a level of detail sufficient to verify compliance with the Service Levels, and shall be subject to audit by Hopper pursuant to Article 4 of this Rider.
3. Project and Contract Management	
3.1	**Financial Records**. Upon Hopper's written request (which shall only be requested if deemed reasonably necessary to meet legal and/or regulatory requirements of Hopper or Hopper's customers), Service Provider shall provide to Hopper financial records, business records or other documentation related to reasonably demonstrate Service Provider's ability to provide the Services under this SA within ten (10) Business Days of Service Provider's receipt of such request. Failure to provide documentation requested by Hopper shall constitute grounds for Hopper to terminate immediately this SA, without further obligation to Service Provider, provided that Hopper has paid Service Provider all fees outlined in Exhibit A for use of the Services for the then-current Term (or Hopper shall pay all such fees due for the remainder of the then-current Term in connection with such termination).
3.2	**Reports and Meetings**: Service Provider shall provide Hopper with regular reports related to: (i) Service Provider's performance of the Services as reasonably requested by Hopper, and (ii) any developments, additional products, or service enhancements offered by Service Provider. Service Provider shall attend an appropriate set of meetings as reasonably determined by Hopper to review Service Provider's performance under the SA. These meetings may take place in person or via audio

	or video conference, as appropriate.
3.3	**Use of Subcontractors**. Service Provider may subcontract or otherwise delegate its performance of the Services to a third-party entity other than Service Provider Personnel, only in accordance with the following: (i) Prior to entering into any agreement to delegate any of its material performance obligations to a third party (including an Affiliate of Service Provider) other than Service Provider Personnel (a "Subcontractor"), Service Provider shall give Hopper at least thirty (30) Business Days prior written notice specifying the components of the Services affected, the scope of the proposed delegation, the identity and qualifications of the proposed Subcontractor and the address of the proposed site(s) from which such Services would be provided. Permitting any third-party to directly access, view, or process unencrypted or plain text Hopper Data or Confidential Information (including an Affiliate of Service Provider) shall be considered a delegation of material performance obligations requiring Hopper's consent as set forth herein. (ii) Service Provider shall perform reasonable due diligence on any proposed Subcontractor to ensure compliance with the applicable terms of the SA, which due diligence may include site visits, financial research and other investigation required by Hopper. Service Provider shall forward to Hopper a description of the scope and material terms (other than financial terms but including any key performance metrics) of any proposed agreement between Service Provider and a proposed Subcontractor. Service Provider's agreements with its Subcontractors shall require of such Subcontractors the same level of risk mitigation as Hopper requires of Service Provider. (iii) Hopper may approve or disapprove proposed Subcontractors, and/or may withdraw prior approvals, in its sole discretion. All such approvals by Hopper will be in writing and no oral approval shall be effective. No such approval shall be deemed a waiver of any of Hopper's rights or Service Provider's obligations under the SA. Subcontractors approved by Hopper in writing shall be added to and identified on Schedule C to this Rider ("**Approved Subcontractors**"). (iv) Service Provider shall remain responsible for obligations, services, and functions performed by its Approved Subcontractors to the same extent as if such obligations, services, and functions were performed by Service Provider, and for purposes of the SA, all work performed by Service Provider's Approved Subcontractors shall be deemed work performed by Service Provider. Service Provider shall have appropriate controls in place, including the performance of audits and monitoring of its Approved Subcontractors' performance, to ensure full compliance with all of Service Provider's

responsibilities under the SA.

(v) Upon Hopper's written request, Service Provider shall provide, and/or shall use commercially reasonable efforts to cause any Approved Subcontractors to provide where such information is not publicly available, financial records, business records or other documentation related to such Approved Subcontractor's ability to provide the Services, within ten (10) Business Days of Service Provider's receipt of such request. Failure to provide documentation requested by Hopper shall constitute grounds for Hopper to revoke immediately its approval of the Approved Subcontractor.

(vi) Service Provider shall not pay its Approved Subcontractors any incentive-based compensation (e.g., compensation that increases as a result of meeting certain goals or standards related to enhanced customer experience, or increased or enhanced performance of the Services).

(vii)[Intentionally Omitted] .

(viii) Hopper shall have a right to verify Service Provider's compliance with these provisions pursuant to the terms of Article 4 of this Rider; provided that, if there is any breach of any term, condition, representation or warranty condition in this section by Service Provider, and/or there is any disagreement as to whether a third-party or Affiliate should be deemed a Subcontractor and/or if Hopper withdraws any prior approval or disapproves of any proposed Subcontractor and Service Provider continues to use such Subcontractor to provide the Services, Hopper's sole and exclusive remedy shall be the right to terminate the SA to which this Rider is attached effective immediately upon notice to Service Provider without further liability, obligation or penalty of either party, provided that Hopper has paid Service Provider all fees outlined in Exhibit A for use of the Services for the then-current Term (or Hopper shall pay all such fees due for the remainder of the then-current Term in connection with such termination).

4. Audits; Records Retention

4.1	**Audit Rights; Obligations**. Service Provider shall, and shall use commercially reasonable efforts to cause its Approved Subcontractors to maintain in English complete auditable records related to its/their performance of the Services and compliance with its/their obligations under the SA. Upon written request no more than on an annual basis, Service Provider shall (i) promptly complete any reasonable data protection questionnaire provided by Hopper and (ii) provide a copy of its (and if applicable, its Approved Subcontractors') SOC2 report(s) which may be used as an element to demonstrate compliance with Service Provider's Information Security obligations hereunder. To the extent such proof or information is determined by a regulatory agency auditing Hopper or Hoppers' customers to be inadequate to demonstrate Service Provider's compliance, then during the Term and for the period thereafter that Service Provider is required to maintain records hereunder, Service Provider shall, and shall use commercially reasonable efforts to, and cause its Approved Subcontractors to, provide to Hopper, its auditors (including internal audit staff and external auditors), inspectors, government regulators, and other applicable entities as Hopper may from time to time designate in writing, access (and in the case of regulators at any time required by such regulators), to Service Provider Personnel, and to data, and records, systems and applications relating to the Services for the purpose of performing audits of Service Provider in order to: (i) verify the accuracy of charges and invoices; (ii) verify the integrity of Hopper Confidential Information and examine the systems that process, store, support and transmit the same, including by dynamic testing (by Hopper security professionals or designated third parties), provided however that such is requested by a Hopper Client and Hopper has a contractual obligation with that Client to perform such testing or examinations;; (iii) verify compliance with the terms of Schedule B ("Information Security"); (iv) verify the accuracy of the representations, warranties and covenants detailed in Article 7.1 of this Rider ("Adequate Internal Controls"); (v) verify Service Provider's controls, performance and information systems as they relate to the Services; (vi) verify Service Provider's policies, procedures, internal controls, and training materials to ensure Service Provider conducts appropriate training and oversight of Service Provider Personnel or agents that have consumer contact or compliance responsibilities; (vii) verify the financial condition of Service Provider; (viii) verify compliance with the insurance coverage provisions set forth in the SA; (ix) verify Service Provider's risk management procedures; (x) verify Service Provider's compliance with Article 6 of this Rider ("Compliance with Laws and Policies"), including determining compliance with the applicable legal obligations of Service Provider regarding Service Provider Personnel; and (xi) otherwise examine Service Provider's performance of the Services and conformance to the terms of the SA including by performing audits and inspections (a) of practices and procedures; (b) of the use of Hopper assets (if any); (c) of other systems, equipment and software, including with respect to the Services (e.g., Service Provider's work standards and compliance with other requirements relating to the Services); (d) of supporting information and calculations regarding compliance with Service Levels; (e) of general controls and security practices and procedures; (f) of disaster recovery and back-up procedures; (g) of the efficiency and costs of Service Provider in performing the Services (but only to the extent directly affecting charges for, or timing of, Services); (h) of Service Provider's compliance with applicable Hopper policies, training materials and training requirements (but only to the extent they relate to the individual(s) performing End-Customer Facing Services); (i) of Service Provider Personnel performing End-Customer Facing Services (e.g., on-site monitoring, remote phone monitoring, review of recorded calls and any other written communications with customers); (j) of the compensation structure of Service Provider but only to the extent that it relates to Service Provider Personnel performing End-Customer Facing Services; and (k) as necessary to enable Hopper to meet, or to confirm that Service Provider is meeting the requirements imposed by Applicable Laws and/or Hopper's policies and procedures as communicated to Service Provider that may

potentially impact the Services.

Service Provider shall provide to such auditors, inspectors, regulators, and other representatives such reasonable assistance as they request. Service Provider shall cooperate fully with Hopper or its designees in connection with audit and inspection functions and with regard to examinations by regulatory authorities. Hopper's auditors, inspectors and other representatives shall comply with Service Provider's reasonable security requirements made known to Hopper in advance and in writing.

Any audits described in the preceding paragraphs of this Article 4.1 shall be conducted at Hopper’s expense, no more than on an annual basis, during reasonable business hours and in such way as to not interfere with Service Provider’s business.

For Service Provider’s breach of any term, condition or representation in this Article 4.1, Hopper’s sole and exclusive remedy shall be the right to terminate the SA to which this Rider is attached without further liability, obligation or penalty of either party, provided that Hopper has paid Service Provider all fees outlined in Exhibit A for use of the Services for the then-current Term (or Hopper shall pay all such fees due for the remainder of the then-current Term in connection with such termination).

Service Provider shall maintain internal audit controls necessary to monitor Service Provider's compliance with its obligations under the SA and under applicable laws. In addition, Service Provider shall conduct audits and inspections of or pertaining to the Services in such manner and at such times as is consistent with the audit practices of well-managed operations performing services similar to the Services. At a minimum, Service Provider shall conduct an audit of its internal controls, data processing systems and security and business continuity programs used to provide or support the provision of the Services, at least annually using an independent auditor who shall be a reputable, US accounting firm. Service Provider shall perform the audit in accordance with American Institute of Certified Public Accountants’ Audit and Accounting Guide and shall provide Hopper a report of the audit in the Soc 2, Type 2 format.

4.2	**Audit Follow-up**. Upon request, Service Provider shall make available promptly to Hopper the results of any audit or inspection conducted by Service Provider or its Affiliates (including by internal audit staff or external auditors) relating to Service Provider's operating practices and procedures to the extent relevant to the Services for Hopper. Following an audit or inspection, Hopper may conduct, or request its external auditors or examiners to conduct, an exit conference with Service Provider to obtain factual concurrence with issues identified in the review. Service Provider and Hopper shall promptly meet to review each audit or inspection report after its issuance and to mutually agree upon the appropriate manner, if any, in which to respond to the changes suggested by the audit or inspection report. Hopper and Service Provider agree to develop operating procedures for the sharing of audit and regulatory findings and reports related to Service Provider's operating practices and procedures produced by auditors or regulators of either party. Service Provider shall promptly develop and implement an appropriate action plan to address and resolve any deficiencies, concerns and/or recommendations identified in an exit interview or audit or inspection report. Service Provider, at its own expense, shall undertake remedial action in accordance with such exit interview or action plan and the dates specified therein, including for all actions, to the extent necessary to comply with Service Provider's obligations under the SA. For Service Provider’s breach of any term, condition or representation in this Article 4.2, Hopper’s sole and exclusive remedy shall be the right to terminate the SA to which this Rider is attached without further liability, obligation or penalty of either party, provided that Hopper has paid Service Provider all fees outlined in Exhibit A for use of the Services for the then-current Term (or Hopper shall pay all such fees due for the remainder of the then-current Term in connection with such termination).
4.3	**Records Retention**. Unless otherwise directed by Hopper pursuant to other written provisions of any agreement, Service Provider shall maintain such information and records referenced in this Article 4 until the latest of: (i) the period of time set forth in Service Provider’s record retention policy, which shall be provided to Hopper upon request; or (ii) to the extent such information and records pertain to pending matters relating to the SA (e.g., disputes), until such pending matters are closed; or (iii) the expiration of any applicable legal "hold order" as to which Hopper has provided Service Provider with written notice, and provide access upon request to the records, documents and other information required to meet Hopper's audit rights under the SA.
5. Confidential Information	

5.1	**Confidential Information**. This Article 5 shall supersede and replace the provisions of Section 7 (“Confidential Information) of the SA with respect to the SA Services (as defined above). Service Provider and Hopper each acknowledge that they may be furnished with, receive or otherwise have access to information of or concerning the other party that such party considers to be confidential, a trade secret or otherwise restricted. "Confidential Information" means all information, in any form, furnished or made available directly or indirectly by one party to the other that is marked confidential, restricted, or with a similar designation, or information which, under the circumstances of its disclosure, a reasonable party would deem to be confidential information. The terms and conditions of the SA shall be deemed Confidential Information of each party. Confidential Information shall also include: (i) all non-public information pertaining to a party's operations, affairs and businesses as well as a party's financial condition and projections, business ventures, strategic plans and marketing strategies and programs; (ii) Personally Identifiable Information; (iii) in the case of Confidential Information of Hopper, any strategic insights or statistical models about Hopper's customers or former or prospective customers and their behavior; and (iv) any other information that is customarily or reasonably deemed confidential, a trade secret or otherwise restricted under the circumstances. Confidential Information of Hopper shall be referred to herein as "Hopper Confidential Information." Hopper Confidential Information shall also include Personally Identifiable Information regarding any Hopper customer and any and all information entered in or otherwise transferred to software or equipment by or on behalf of Hopper and information derived from such information, including as stored in or processed through the equipment or software of Service Provider (“Hopper Data”). Hopper Data, wherever located and however configured, is, and shall at all times remain, the exclusive property of Hopper. **5.2. Obligations.** The party that receives the Confidential Information of the other party will not use, disclose, commercialize, exploit or otherwise exercise any rights in connection with the Confidential Information of the other party in any manner or for any purpose except as expressly permitted under the SA. Unless subject to a higher standard of care elsewhere herein, each party shall use at least the same degree of care as it employs to avoid unauthorized disclosure of its own Confidential Information, but in any event no less than commercially reasonable efforts, to prevent disclosing to unauthorized parties the Confidential Information of the other party. Service Provider shall limit access to systems that process, store, support and transmit Hopper Confidential Information to authorized Service Provider Personnel to the extent necessary to carry out the specific purposes for which such Confidential Information was disclosed to Service Provider. Service Provider shall advise such Service Provider Personnel, prior to any disclosure by Service Provider, of the confidential nature of such Confidential Information and shall ensure that such Service Provider Personnel are bound by written restrictions on use and disclosure and other confidentiality restrictions, if not subject to existing obligations at least as restrictive as those contained in the SA. Each party shall be permitted to disclose or make available any Confidential Information to its affiliates, directors, officers, employees, contractors, agents, accountants, attorneys and other confidential advisors, and to Clients and its Affiliates (collectively, the “Representatives”) who need to know such Confidential Information for the purpose of assisting Hopper in connection with the SA or with complying with applicable law or enforcing it’s rights under the SA. Each party shall advise its Representatives, prior to any disclosure , of the confidential nature of such Confidential Information and shall ensure that its Representatives are bound by written restrictions on use and disclosure and other confidentiality restrictions, if not subject to existing obligations at least as restrictive as those

contained in the SA.

As requested by a furnishing party during the Term, upon expiration or any termination of the SA, or completion of Service Provider's obligations under the SA, a receiving party shall (a) return in the format specified by the furnishing party in the request but in any case in a usable format or (b) destroy, each as the furnishing party may direct, all material in any medium that contains, refers to, or relates to the furnishing party's Confidential Information, and retain no copies or reproductions. Upon request, a receiving party shall promptly provide to the furnishing party a written certification signed by an officer of a receiving party affirming that it has met its obligation under this provision.

In the event of any actual or reasonably suspected misuse, disclosure or loss of, or inability to account for, any Confidential Information of the furnishing party (hereinafter, a "Confidential Information Violation"), the receiving party promptly shall: (a) notify the furnishing party upon becoming aware thereof; (b) furnish to the other party full details of the Confidential Information Violation and use commercially reasonable efforts to assist the other party in investigating or preventing the recurrence of same; (c) take such actions as may be necessary, appropriate or reasonably requested by the furnishing party to minimize the Confidential Information Violation; and (d) cooperate in all reasonable respects with the furnishing party to minimize the impacts of Confidential Information Violation and any damage resulting therefrom.

Neither party shall commence any legal action or proceeding against a third party in respect of any Confidential Information Violation by any person or entity which action or proceeding identifies the other party or its Confidential Information without such party's prior written consent.

With respect to Confidential Information that is Personally Identifiable Information, the terms of this Article 5 shall not supersede any different, or similar but more protective, rights or obligations set forth in Article 5.6 (“Safeguarding”)

The Parties' obligations respecting Confidential Information (including all Personally Identifiable Information) shall survive expiration or termination of the SA without limitation.

5.3. Exclusions. The provisions of this Article 5 shall not apply to any particular information (other than Personally Identifiable Information) which Service Provider or Hopper can demonstrate: (a) was, at the time of disclosure to it, in the public domain; (b) after disclosure to it, is published or otherwise becomes part of the public domain through no fault of the receiving party; (c) was lawfully in the possession of the receiving party at the time of disclosure to it without obligation of confidentiality; (d) was received after disclosure to it from a third party who had a lawful right to disclose such information to it without any obligation to restrict its further use or disclosure; or (e) was independently developed by the receiving party without use of or reference to Confidential Information of the furnishing party. In addition, a party shall not be considered to have breached its obligations by disclosing Confidential Information of the other party as required to satisfy any legal requirement of a competent government body provided that, promptly upon receiving any such request and to the extent that it may legally do so, such party advises in writing the other party of the request prior to making such disclosure in order that the other party may interpose an objection to such disclosure, take action to assure confidential handling of the Confidential Information, or take such other action as it deems appropriate to protect the Confidential Information.

Service Provider may disclose Hopper Confidential Information (including Personally Identifiable Information) to Affiliates of Service Provider that are approved Subcontractors; provided, however, that: (a) such disclosure is only to the extent and for the duration necessary for Service Provider to

perform its obligations under the SA; and (b) such Affiliate is bound to comply with substantially the same obligations to which Service Provider is subject under this Rider with respect to Confidential Information (including as provided in this Article 5).

Service Provider may disclose Hopper Confidential Information (including Personally Identifiable Information) for processing and/or storage in encrypted form only (and provided that no ability to decrypt such Information is also provided) to third-party service providers upon written notice to Hopper and Hopper shall be deemed to have consented to the handling of encrypted Information by such third party service providers if: (a) such disclosure is only to the extent and for the duration necessary for Service Provider to perform its obligations under the SA; and (b) prior to any such disclosure the third party service provider agrees in writing (1) to use and disclose such Confidential Information only to the extent necessary to carry out the specific purposes for which such Confidential Information was disclosed to Service Provider; and (2) to comply with substantially the same obligations to which Service Provider is subject under the SA with respect to Confidential Information (including as provided in this Article 5). For avoidance of doubt, unencrypted Hopper Confidential Information (including Personally Identifiable Information) shall only be disclosed to a Subcontractor approved in writing by Hopper pursuant to Article 3 of this Rider.

Hopper may withdraw prior approvals to a Subcontractor or to a third-party processor pursuant to the preceding paragraph (whether such approval was express or deemed), in its sole discretion. If there is any breach of any term, condition or representation in this Article 5.3 by Service Provider, and/or if Hopper withdraws any prior approval or disapproves of any proposed Subcontractor or third-party processor and Service Provider continues to use such Subcontractor or third-party processor to provide the Services, Hopper's sole and exclusive remedy shall be the right to: (i) terminate the SA to which this Rider is attached without further liability, obligation or penalty of either party, provided that Hopper has paid Service Provider all fees outlined in Exhibit A for use of the Services for the then-current Term (or Hopper shall pay all such fees due for the remainder of the then-current Term in connection with such termination); and (ii) to equitable relief, including injunctive relief and specific performance, as necessary to protect any Hopper Confidential Information (including Personally Identifiable Information) disclosed in violation of this Article 5.

Hopper may disclose Service Provider Confidential Information to Affiliates of Hopper if and to the extent necessary for Hopper and its Affiliates to exercise their respective rights or to comply with their respective obligations under the SA. Hopper may disclose Service Provider Confidential Information to third party service providers of Hopper and its Affiliates if and to the extent necessary for Hopper and its Affiliates to exercise their respective rights or to comply with their respective obligations under the SA, and provided that such third party service providers are bound by confidentiality obligations to Hopper substantially as protective as those described herein.

5.4. Ownership; License. Each party's Confidential Information shall remain the property of that party. Nothing contained in this Article 5 shall be construed as obligating a party to disclose its Confidential Information to the other party, or as granting to or conferring on a party, expressly or impliedly, any rights or license to the Confidential Information of the other party, and any such obligation or grant shall only be as provided by other provisions of the SA.

5.5. Remedies. Each party agrees that because of the unique nature of such Confidential Information, any breach of this Article 5 would cause the other party irreparable harm, and money damages and other remedies available at law in the event of a breach would not be adequate to compensate the other party for any such breach. Accordingly, each party agrees that (except for the

	specific remedy set forth in Article 5.3 which shall be Hopper's sole and exclusive remedy for any such breach of said Article) the other party shall be entitled, without the requirement of posting a bond or other security, to equitable relief, including injunctive relief and specific performance, as a remedy for any such breach. Such relief shall be in addition to, and not in lieu of, all other remedies available to the other party, whether under the SA, at law or in equity.

5.6	**Safeguarding**. Service Provider acknowledges that Hopper and/or its Affiliates is subject to the GLB Act, Title V, pursuant to which Hopper obtains certain undertakings from Service Provider with regard to the privacy, use and protection of Personally Identifiable Information. Therefore, notwithstanding anything to the contrary contained in the SA and in addition to (and not in substitution for) Service Provider's other obligations hereunder, and with respect to Service Provider's provision of the Services to Hopper: (A) Service Provider will protect and keep confidential all Personally Identifiable Information, in any form. During the Term, Service Provider will collect, maintain, use, disclose or otherwise Process Personally Identifiable Information in connection with the provision of the Services (i) solely on behalf of Hopper, (ii) only to the extent necessary to perform the obligations or perform the Services to Hopper under the SA, and (iii) only for the purpose for which such Personally Identifiable Information was disclosed to or obtained by Service Provider. Without limiting the generality of the foregoing, Service Provider is specifically prohibited from selling, renting, transferring or distributing Personally Identifiable Information and from retaining, using, making accessible or disclosing Personally Identifiable Information for a commercial purpose other than providing the Services as specified in the SA or in any manner outside of the direct business relationship between Service Provider and Hopper. The above restrictions on disclosure, etc. do not apply if Service Provider has obtained the express written consent of Hopper or, to the extent permitted by applicable laws, as necessary to comply with applicable laws, in which case Service Provider must notify Hopper promptly in writing before complying with such disclosure request. (B) Service Provider shall ensure that Service Provider Personnel shall not attempt to access, or allow access to, any Personally Identifiable Information that they are not permitted to access in connection with the provision of Services under the SA. (C) Service Provider acknowledges and agrees that its execution of this SA constitutes its certification that it understands the restrictions set forth in this Article 5.6 and will comply with them and all applicable laws, including GDPR, CCPA, PIPEDA, and any other similar state, provincial, or federal privacy law.

(D) Service Provider represents and warrants that it has, and warrants and covenants that for so long as it retains Personally Identifiable Information it will continue to have, adequate administrative, technical, and physical safeguards to (a) protect the security and confidentiality of such Personally Identifiable Information; (b) protect against any anticipated or reasonably likely threats or hazards to the security or integrity of such Personally Identifiable Information; (c) protect against unauthorized access to or use of such Personally Identifiable Information; (d) ensure the proper disposal of Personally Identifiable Information; and (e) without limiting the generality of items (a) through (d) preceding, comply with the requirements contained in Section 501(b) of the GLB Act, the CCPA, and the Interagency Guidelines Establishing Information Security Standards adopted by federal bank regulatory agencies, including the Office of the Comptroller of the Currency (OCC) and the Board of Governors of the Federal Reserve System. In addition to the foregoing, Service Provider represents and warrants that the manner in which it performs its obligations hereunder (including the manner in which it maintains, stores, backs up, transports, transmits or otherwise uses Personally Identifiable Information) will comply with any applicable state data security requirements covering information that, in whole or in part, is made up of Personally Identifiable Information, including, 201 CMR 17.00 et seq., ("Standards for the Protection of Personal Information of Residents of the Commonwealth").

(E) Service Provider shall immediately notify Hopper without undue delay (but no later than forty-eight (48) hours from Service Provider's actual knowledge) if (a) Service Provider discovers there (1) has been a material breach, or unauthorized intrusion or access, or (2) is a potentially material vulnerability, in each case, in the security safeguards required by this Section, including the security safeguards protecting Personally Identifiable Information in the possession of Service Provider, or (ii) the security of Personally Identifiable Information has been or may be compromised for any reason (including by access to Personally Identifiable Information by unauthorized Service Provider Personnel or the abuse of authorized access to Personally Identifiable Information by Service Provider Personnel) (each of the foregoing, a "**Security Incident**"). Such notification shall include the date and time of the Security Incident , what (if any) corrective action has been taken by Service Provider, what steps Service Provider has taken to isolate the Security Incident, and any additional details that may be necessary for Hopper to isolate the Security Incident or prevent any further adverse effect of the Security Incident. Service Provider shall promptly provide Hopper with any additional information that Hopper may request (e.g., for access logs), and promptly comply with any reasonable requests that Hopper may make (e.g., changing security credentials), in each case, relating to the Security Incident. Service Provider shall continue to promptly inform Hopper of any proposed corrective action that it plans to take with respect to the Security Incident and shall promptly take all corrective actions that are reasonably necessary to isolate the Security Incident and prevent further adverse effects. Upon receipt of notice of a Security Incident, Hopper may take all reasonable and appropriate steps to (aa) protect Personally Identifiable Information, (bb) execute its obligations under state or federal Security Incident requirements and (cc) to implement its data security breach response program, including by auditing Service Provider's security safeguards required under this Section and by auditing security and system log files from workstations and supporting servers containing or facilitating the flow of Personally Identifiable Information. Service Provider represents that it may, can and will,

following a Security Incident, cooperate with Hopper's efforts to expeditiously implement its data security breach response program. With respect to a Security Incident, except as required by any applicable legal or regulatory requirements, Service Provider shall not communicate with any third party (other than its contractors, insurers, accountants, attorneys and other confidential advisors who are assisting Service Provider in connection with such Security Incident or as may be required under the Payment Card Industry Data Security Standards or by any applicable charge card association rules or payment card network through which Spreedly Processes payment card transactions) regarding such Security Incident by making any direct or indirect reference to either the Services, or any data accessed, processed or stored on behalf of Hopper, in each case, without the prior written consent of Hopper; provided, however, any disclosure that may be required to meet legal or regulatory requirements shall be subject to Article 5 of this Rider. While it is the intention of the Parties that Hopper run its response program remotely, the Parties recognize that will not always be possible. For the avoidance of doubt, the term "Security Incident" as used herein shall include any data security event triggering response obligations under the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (see 70 Fed. Reg. 15736 (March 29, 2005)) or under state laws relating to data security breaches, including state law relating to the unauthorized access to or use of "personal information" or other similar terms.

(F) Service Provider shall not retain Personally Identifiable Information unless the retention is specifically provided for in the SA, Service Provider has a specific business purpose to retain it that is set forth in the SA, and the retention of such data is consistent with applicable laws. At Hopper's discretion, Service Provider shall destroy such Personally Identifiable Information or return it to Hopper, either of which shall be performed pursuant to Hopper's reasonable instructions: (a) during the Term promptly following the time at which such Personally Identifiable Information is no longer needed to provide the Services, or (b) within sixty (60) days after termination or expiration of the SA.

(G) Service Provider must notify Hopper in writing within five (5) Business Days of receipt of any request (whether received directly or indirectly by Service Provider) by any natural person, whose Personally Identifiable Information is Processed by Service Provider pursuant to this SA, to access, update, revise, correct, object to Processing, or delete Personally Identifiable Information (“Data Subject Request”). Service Provider will provide Hopper its reasonable assistance in responding to any such Data Subject Request in accordance with applicable laws.

(H) Without limiting the generality of the foregoing, Service Provider must, within five (5) Business Days of an applicable request from Hopper: (i) delete or destroy all copies of Personally Identifiable Information in any media relating to a particular natural person as directed by Hopper; and (ii) provide a copy of Personally Identifiable Information relating to a particular natural person (including information about the Processing of that Personally Identifiable Information) in a portable and readily useable format, as reasonably specified

	by Hopper. (I) To the extent that any Hopper Confidential Information (including data derived directly or indirectly from Hopper users) is used to improve Service Provider's underlying platform, such Confidential Information and data must be in an Aggregated and Deidentified format. At the termination or expiration of the SA, Service Provider agrees not to (i) make any effort to re-identify individual customers using any Hopper Confidential Information, (ii) make any effort to re-identify Aggregated and Deidentified data as originating from a financial institution, Hopper specifically, or Hopper users, (iii) use any Hopper Confidential Information to identify attributes or characteristics of Hopper's customers' credit card portfolio, or (iv) use any Hopper Confidential Information to identify attributes or characteristics of Hopper's customer portfolio. The phrase "Aggregated and Deidentified" means information that: (i) is aggregated and deidentified in such a manner that it cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual and does not reveal any customer Confidential Information; (ii) does not identify, nor make identifiable, Hopper as a source of the information or the proportion of information that can be attributed to Hopper versus Service Provider's other customers; and (iii) Service Provider warrants that it will not attempt to reverse engineer or otherwise use to reidentify an individual or Hopper. (J) The obligations set forth in this Article 5.6 shall survive termination of the SA.
5.7	At Hopper's request, Service Provider shall create and maintain flow diagram(s) indicating how Hopper Confidential Information flows through both the Service Provider network environment. Service Provider shall provide such flow diagram(s) upon Hopper's reasonable request.
5.8	**[Intentionally Omitted]**
6. Compliance with Laws and Policies	

6.1	**Compliance Generally**. Each party shall perform its obligations in a manner that complies with all applicable laws as and to the extent such laws apply or relate to each party, the provision or use of the Services, or any other act, activity or responsibility of such party hereunder. This requirement includes identifying and procuring required permits, certificates, approvals and inspections. In addition, Service Provider shall maintain commercially reasonable policies and procedures designed to promote compliance with its legal and contractual obligations. From time to time and with at least sixty (60) days advance notice, Hopper may provide Service Provider with policies and procedures or with changes to the same. Service Provider shall perform its legal and contractual obligations in a manner that complies with all of its policies and procedures, and those policies and procedures Hopper has provided to Service Provider, as amended from time to time with written notice to Service Provider at least sixty (60) prior to such amendments becoming effective. Service Provider shall maintain evidence of its compliance with applicable laws. If a charge of non-compliance with any applicable laws occurs, the party so charged shall promptly notify the other party of such charge. Service Provider shall reasonably cooperate with Hopper with respect to Hopper's efforts to comply with applicable laws, including implementing such measures as Hopper deems necessary or appropriate to effect such compliance. Provider shall also comply with the "Information Security Requirements" attached hereto as Schedule B. Notwithstanding the foregoing, if there is any breach of any term, condition or representation in this Article 6.1 by Service Provider, Hopper's sole and exclusive remedy shall be the right to terminate the SA to which this Rider is attached without further liability, obligation or penalty of either party, provided that Hopper has paid Service Provider all fees outlined in Exhibit A for use of the Services for the then-current Term (or Hopper shall pay all such fees due for the remainder of the then-current Term in connection with such termination).
6.2	**[Intentionally Omitted]**

6.3 **Compliance with Certain Applicable Laws and Policies**. Without limiting the generality of Article 6.1 (Compliance Generally):

(A) To the extent applicable to the Services and/or Service Provider, Service Provider is knowledgeable about the economic or trade sanctions or restrictions administered by the U.S. Government (including all Executive Orders and implementing regulations), such as those administered by the U.S. Department of the Treasury, Office of Foreign Assets Control ("OFAC") and will ensure that the Services are provided in a manner consistent with those sanctions and/or restrictions.

(B) Service Provider shall not assign to perform the Services any persons or entities identified on OFAC's Specially Designated Nationals and Blocked Persons List. So as to facilitate possible OFAC checks by Hopper, Service Provider, no more than fifteen (15) days prior to assignment to the Services, shall identify to Hopper the names, addresses and other identifying information of all Service Provider Personnel that Service Provider intends to assign to perform the Services.

(C) To the extent applicable to the Services, Service Provider is and shall continue to remain knowledgeable about, and shall remain in full compliance with, all anti-money laundering requirements and legal obligations regarding combating terrorist financing contained in the Bank Secrecy Act, the USA PATRIOT Act and all implementing regulations. Service Provider shall perform the Services in full compliance with such laws, including the performance of any procedures identified in any work order. Service Provider has and shall continue to implement effective oversight and monitoring procedures to detect and investigate misuse or misappropriation of any Hopper assets, systems, funds or information by Service Provider Personnel. Service Provider shall promptly (not to exceed three (3) Business Days following discovery) report any such misuse or misappropriation to Hopper.

(D) Service Provider shall comply with all applicable laws protecting the confidential material, information and privacy rights of Hopper, its Affiliates and/or their customers and consumers, including Title V, Subtitle A of the GLB Act; the CCPA and any other similar state privacy law; and the Economic Espionage Act, 18 USC §1831 et. seq.).

(E) To the extent applicable to the Services and/or Service Provider, Service Provider is and shall continue to be knowledgeable about, and shall perform the Services in full compliance with, applicable laws governing telephone calling and telemarketing activities in the applicable jurisdictions where the Services include such activities, including the Telephone Consumer Protection Act, 47 U.S.C. § 227 et seq. and its implementing regulations as administered by the Federal Communications Commission, the Telemarketing Sales Rule, 16 C.F.R. § 310.1 et seq., and any applicable state versions of the foregoing.

(F) The Parties acknowledge that certain items, including computers, electronic components, telecommunications equipment, Software and technical data, which may be provided hereunder, and certain transactions which may be undertaken hereunder, may be subject to export controls under applicable laws. Service Provider agrees that it shall not export or re-export any such items or any direct product thereof or undertake any transaction in violation of any such export controls. Without limiting the generality of this Article 6.3, to the extent within Service Provider's control, Service Provider shall be responsible for, and shall coordinate and oversee, compliance with such applicable laws in

respect of such items exported, re-exported, trans-shipped or imported hereunder. As provided in this Section, Service Provider shall reasonably cooperate with Hopper with respect to Hopper's efforts to comply with any such applicable laws, including implementing such export control measures as Hopper deems necessary to effect such compliance. Service Provider will perform the Services under the SA in compliance with such laws, Executive Orders and regulations.

(G) **UDAAP**. To the extent applicable to the Services and/or Service Provider, Service Provider is and shall continue to be knowledgeable about, and shall remain in full compliance with, applicable laws governing unfair, deceptive, or abusive acts and practices in connection with any transaction with a consumer, including, Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) and Section 1031 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, 12 U.S.C. § 5531, administered by the Consumer Financial Protection Bureau.

(H) Service Provider shall perform the Services in full compliance with such laws and any requirements, standards or procedures identified in any work order. Service Provider shall retain evidence of its compliance with such laws and procedures.

6.4	**Anti-Bribery and Anticorruption**. (A) Service Provider (and its officers, directors and employees, and any third parties acting on Service Provider's behalf, at its direction or under its control in connection with the Services), and the Services being directly or indirectly provided by Service Provider, shall comply with all applicable laws relating to bribery and corruption, including: (i) the U.S. Foreign Corrupt Practices Act ("FCPA"), (ii) the U.K. Bribery Act 2010, (iii) Canada's Corruption of Foreign Public Officials Act, and (iv) the antibribery and anticorruption laws of any country outside of the United States from which Service Provider will perform the Services (collectively, the "ABAC Laws"). (B) Neither Service Provider nor any of its officers, directors, employees, or any third parties acting on Service Provider's behalf, at its direction or under its control in connection with the Services, has paid, offered, funded, approved or otherwise facilitated, promised or provided anything of value to any person in order to improperly influence them in the performance of their legal or contractual duties in connection with Service Provider's provision of the Services, nor will they do so during the performance of the Services. (C) If Service Provider learns of or has reason to know of any payment, offer or agreement relating to the Services that is contemplated or that has occurred and represents or could represent a violation of an ABAC Law, Service Provider shall immediately notify Hopper in writing. (D) Hopper shall be permitted to take reasonable steps to avoid, mitigate or investigate an actual or potential violation of the ABAC Laws, including by: (i) performing due diligence on Service Provider, and (ii) upon Hopper forming reasonable suspicion that a violation of this provision or of an ABAC Law has or is at risk of occurring, reviewing Service Provider's books and records, or performing other audits or reviews of Service Provider upon reasonable notice. Service Provider agrees to cooperate with Hopper as it exercises its rights hereunder. (E) Service Provider shall disclose to Hopper the name, address and any other relevant identifying information of any person or entity holding or that at any point during provision of the Services acquires any ownership interest in Service Provider, or that otherwise has or that at any point during provision of the Services acquires any ability to control Service Provider, that Service Provider knows (or through reasonable diligence should know) is (i) a "foreign official" as that term is construed under the FCPA, or (ii) owned or controlled by or affiliated with any non- U.S. government or instrumentality of a non-U.S. government. (F) **ABAC Certification**. Service Provider acknowledges that it has received and reviewed a copy of the Foreign Corrupt Practices Act (FCPA) General Description provided in Schedule A, and has received, reviewed and executed the Hopper Anti-Bribery and Anticorruption (ABAC) Compliance Certification provided in Schedule A. Service Provider agrees that it will execute the certification in Schedule A on an annual basis, or at such other intervals as Hopper may request.

6.5 **Workplace Laws**. Without limiting the generality of Article 6.1 (Compliance Generally), Service Provider, in providing Services, shall:

(A) Comply with all applicable federal, state and local employment and employee benefits laws, regulations and orders. In addition, Service Provider will perform all work under the SA in full compliance with the provisions of the Federal Occupational Safety and Health Act of 1970 (the "1970 Act"), and with any rules and regulations promulgated pursuant to the 1970 Act and any similar state and local laws.

(B) Comply with all applicable provisions of Sections 6, 7, and 12 of the Fair Labor Standards Act, 29 USC §§201 - 219, as amended ("FLSA"), and agrees that there will be no violations by Service Provider of the "hot goods" or "hot cargo" provisions of such FLSA involving restrictions on use of underage individuals by Service Provider.

(C) Employ workers on the basis of their ability to do the job, not on the basis of their personal characteristics. Service Provider shall not discriminate against any employee or applicant for employment because of race, color, religion, disability, sex, national origin, age, veteran status, genetic information or any other unlawful criterion and shall comply with all applicable laws against discrimination and all applicable rules, regulations and orders issued thereunder or in implementation thereof. Hopper is a federal contractor and as such, but only if applicable, the Equal Opportunity Clauses set forth in 41 C.F.R. §§ 60-1.4(a), 60-300.5(a), and 60-741.5(a), as well as the employee notice found at 29 C.F.R. Part 471, Appendix A to Subpart A are incorporated by reference herein. Hopper and Service Provider shall abide by the requirements of 41 CFR 60-300.5(a) and 41 CFR 60-741.5(a). These regulations prohibit discrimination against qualified individuals on the basis of protected veteran status or disability, and require affirmative action by covered prime contractors and subcontractors to employ and advance in employment qualified protected veterans and individuals with disabilities.

(D) Furnish Service Provider Personnel with safe and healthy working conditions, adequate medical facilities, fire exits and safety equipment, well-lit and comfortable workstations and clean restrooms. Service Provider shall comply with all applicable laws governing occupational health and safety and, in addition to any such legal requirements, shall adequately train its employees to perform their jobs safely.

(E) Not use child labor. As used in this clause "child" means an individual that is younger than either: (i) fifteen (15) years of age or (ii) the minimum legal age requirement to work in the applicable location;

(F) Only employ individuals whose presence is voluntary and not use forced, indentured, involuntary, prison, or uncompensated labor under any circumstances; and

(G) Not use corporal punishment or other forms of physical or mental coercion as a means to discipline employees.

6.6	**[Intentionally Omitted]**
7. Representations, Warranties and Covenants	
7.1	**Adequate Internal Controls**. Service Provider represents, warrants and covenants that it has and shall continue to have effective enterprise governance practices and adequate internal controls over the Services to ensure Service Provider is being managed in conformity with industry standards and regulatory guidelines and recommendations. In addition, Service Provider will maintain appropriate policies and procedures to ensure that the financial incentives and penalties Service Provider uses to reward Service Provider Personnel performance will be consistent with and in support of Hopper's commitment to comply with applicable laws and regulatory guidance.
7.2	**[Intentionally Omitted]**.
7.3	**Employment Laws**. Service Provider represents, warrants and covenants that it is in compliance with, and will comply with all applicable laws regarding employment and employee benefits-related laws, regulations and obligations, including those regarding any applicable compensation and wages (including applicable overtime and hourly pay) and/or its/their payment; employee benefits, required insurance (including unemployment and workers compensation), accommodation and leave, employment authorization (including form I-9 compliance), immigration laws and the withholding or payment of employment taxes. Service Provider further represents, warrants and covenants that it does not and 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. If applicable, the Equal Opportunity Clauses set forth in 41 C.F.R. §§ 60-1.4(a), 60-250.5(a), 60-300.5(a) and 60-741.5(a) are incorporated by reference herein.
7.4	**Personnel Requirements**. Service Provider represents, warrants and covenants that Service Provider Personnel are authorized and will remain authorized to work in each of the locations where they are providing the Services; and that Service Provider and its subcontractors have complied with all obligations under applicable laws regarding immigration and work authorization. Service Provider shall bear all financial responsibility for all matters relating to Service Provider obtaining any visa, immigration, naturalization or other similar authorizations and requirements under applicable laws pertaining to visas, immigration, naturalization and other similar authorizations.
7.5	**Work Standards**. Service Provider warrants and covenants that the Professional Services shall be rendered with promptness and diligence and shall be executed in a workmanlike manner, in accordance with the practices and high professional and accepted industry standards used in well-managed operations performing similar services similar. Service Provider warrants and covenants that it shall use adequate staffing with suitable training, education, experience and skills to perform the Professional Services.

7.6	**Non-Infringement**. Service Provider represents, warrants and covenants that it does not and has not infringed or misappropriated any Intellectual Property Rights of any third party, that Hopper's receipt and use of the Services do not infringe or misappropriate any Intellectual Property Rights of any third party, and that it shall perform its responsibilities under the SA in a manner that does not infringe or constitute an infringement or misappropriation of any Intellectual Property Rights of any third party. Service Provider further represents and warrants that as of the Effective Date, there is no proceeding pending, or, to Service Provider's knowledge, threatened, that alleges that any of the Services or Service Provider's manner of performing the Services infringe or constitute an infringement or misappropriation of any Intellectual Property Rights of any third party.
7.7	**Software Ownership or Use**. Service Provider represents and warrants that it is either the owner of, or authorized to use, and covenants that during the Term it shall be either the owner of or authorized to use, the software provided by Service Provider or used to perform the Services, including any software developed by Service Provider as part of the Services. To the extent Service provider and Hopper enter into a statement of work whereby Service Provider shall provide deliverables to Hopper that are work product, and such work product is expressly specified as "Deliverables" in such statement of work and generated by Service Provider exclusively on Hopper's behalf in the performance of the SA, then Service Provider represents, warrants and covenants that any such work product provided to or licensed to Hopper hereunder does not and will not incorporate into it Software that is subject to an open source or "copyleft" license, or license having similar licensing or distribution models or terms, if such license: (i) creates or purports to create obligations of use with respect to any such Work; (ii) grants or purports to grant to any third party any rights to such work product; or (iii) requires disclosure or furnishing of source code for any portion of such work product to any third party. In the event that Service Provider wishes to incorporate into any work product provided to or Hopper Software that is subject to an open source or "copyleft" license, or license having similar licensing or distribution models or terms, and at least one of the foregoing obligations, Service Provider agrees to request, in writing, Hopper's prior written approval. Hopper may approve, condition or reject its approval in its sole discretion. With respect to such work product provided to Hopper, if applicable, Service Provider represents, warrants and covenants that Service Provider has complied with the requirements of any open source or "copyleft" license, or license having similar licensing or distribution models or terms.
7.8	**Authorization and Other Contracts**. Each Party represents and warrants to the other that: 1. It has the requisite corporate power and authority to enter into the SA and to carry out the transactions contemplated by the SA; 2. The execution, delivery and performance of the SA and the consummation of the transactions contemplated by the SA have been duly authorized by the requisite corporate action on the part of such Party and will not constitute a violation of any judgment, order or decree; 3. The execution, delivery and performance of the SA and the consummation of the transactions contemplated by the SA will not constitute a material default under any material contract by which the Party or any of its material assets are bound, or an event that would, with notice or lapse of time or both, constitute such a default; and 4. There is no proceeding pending or, to the knowledge of the Party, threatened that challenges

	or may have a material adverse effect on the SA or the transactions contemplated by the SA.
7.9	**Viruses**. Service Provider warrants and covenants that it shall use commercially reasonable efforts to avoid the coding or introduction of computer viruses into the systems used to provide the Services. In the event that a virus is found to have been introduced into Hopper systems through Service Provider or the Services, Service Provider shall use commercially reasonable efforts, at no additional charge, to assist Hopper remove the virus, reduce the effects of the virus and, if the virus causes a loss of operational efficiency or data, to assist Hopper, at no additional charge or cost, to the same extent in order to mitigate such losses and restore the data. In the event that a virus is found to have been introduced into Service Provider systems used to provide the Services, Service Provider shall remedy the effects of the virus and, if the virus causes a loss of operational efficiency or loss of data, mitigate and restore such losses, at no additional cost or charge to Hopper.
7.8	**[Intentionally Omitted]**.
8. Insurance	

8.1	**Insurance Coverage**. Service Provider represents that as of the Effective Date it has, and agrees that it shall maintain in force during the Term, at least the following insurance coverages: 1. Worker's compensation insurance and other similar social insurance in accordance with the laws of the country, state, province or territory exercising jurisdiction over the employee with minimum limits required by law; 2. Employer's liability insurance, including coverage for occupational injury, illness and disease, with minimum limits per employee and per event of $1,000,000; 3. Commercial general liability insurance, including products liability, completed operations, premises operations, personal injury, advertising liability and contractual and broad form property damage liability coverages, on an occurrence basis, with a minimum per occurrence combined single limit of $1,000,000 and a minimum aggregate combined single limit of $2,000,000; 4. Comprehensive automotive liability insurance covering use of all owned, nonowned and hired automobiles used to perform the Services or on Hopper's property for purposes related to the Services for bodily injury, property damage, uninsured motorist and underinsured motorist liability with a minimum combined single limit per accident of $1,000,000 or the minimum limit required by law, whichever limit is greater; 5. Excess or umbrella liability insurance with a minimum limit of $5,000,000 in excess of the insurance coverage described in Sections (2), (3), and (4), above; 6. Crime and fidelity insurance, including blanket coverage for computer fraud, for loss or damage arising out of or in connection with any fraudulent or dishonest acts, including wrongful conversion of (i) Hopper's, or any of its Affiliates', property, (ii) the property of any customers or patrons of such persons or (iii) the property and funds of others in Service Provider's possession, care, custody or control, committed by Service Provider's employees, agents or subcontractors, acting alone or in collusion with others, with a minimum limit per event of $5,000,000. This coverage shall be endorsed to name Hopper and its subsidiaries as loss payees; 7. Professional liability insurance for errors and omissions covering liability for loss or damage due to an act, error, omission, or negligence, with a minimum limit per event of $10,000,000; 8. Cyber/E-commerce liability covering liability arising from or out of the Services provided under the SA with limits not less than $15,000,000 per occurrence. Coverage shall include, but not be limited to, the following: Internet and network liability (providing protection against liability for system attacks; denial or loss of service; introduction, implantation, or spread of malicious software code; and unauthorized access and use), infringement of privacy or intellectual property rights, internet advertising and content offenses, defamation, errors or omissions in software and/or systems development, implementation and maintenance, and privacy liability (providing protection against liability for the failure to protect, or wrongful disclosure of, private or confidential information); 9. Property insurance, including extra expense and business income coverage, for all risks of physical loss of or damage to buildings, business personal property or other property that is in the possession, care, custody or control of Service Provider pursuant to the SA. Such insurance shall have a minimum limit adequate to cover risks on a replacement costs basis; and

10. Electronic data processing insurance providing coverage for all risks of loss or damage to equipment, data, media and valuable papers that are in the possession, care, custody or control of Service Provider pursuant to the SA. Such insurance shall include extra expense and business income coverage and have a minimum limit adequate to cover such risks on a replacement costs basis.

8.2	**Insurance Provisions.** 1. At Hopper's reasonable request, To the fullest extent allowed by its insurers, Service Provider shall cause its insurers to waive all rights of subrogation against Hopper, and its officers, directors and employees and any insured-versus-insured exclusion regarding Hopper. 2. The amounts of insurance required above may be satisfied by Service Provider purchasing primary coverage in the amounts specified or by Service Provider buying a separate excess umbrella liability policy together with lower limit primary underlying coverage. The structure of the coverage is at Service Provider's option, so long as the total amount of insurance meets Hopper's requirements. 3. The insurance under Section 8.1, above, shall be primary, and all coverage shall be non-contributing with respect to any other insurance or self-insurance that may be maintained by Hopper. 4. The insurance coverage under Sections 8.1(1), (2), (3), (4) and (5) shall be written on an occurrence form basis. If any other coverage is written on a claims made basis, it shall have a retroactive date no later than the Effective Date and, notwithstanding the termination of the SA, either directly or through 'tail' coverage shall be maintained for a period of at least two (2) years following completion of the Term, or it shall allow for reporting of claims until the later of two (2) years after the Term or the period of the applicable limitations of actions has expired. 5. At Hopper's reasonable request, Service Provider shall cause its insurers to name Hopper, its subsidiaries and their respective directors, officers, employees, agents, successors, and permitted assigns, as Additional Insureds on the insurance coverages under Sections 8.1 (2), (3), (4) and (5). 6. Service Provider shall cause its insurers to issue certificates of insurance evidencing that the coverages and policy endorsements required under the SA are maintained in force. Service Provider shall require its insurers to provide Hopper not less than thirty (30) days' written notice prior to any adverse modification, cancellation, or non-renewal of the Workers' Compensation, Commercial General Liability and Crime and Fidelity policies. For all other policies, Service Provider shall provide Hopper not less than thirty (30) days' written notice prior to any adverse modification, cancellation or non-renewal. The insurers selected by Service Provider shall be of good standing and authorized to conduct business in the jurisdictions in which Services are to be performed. When the policy is issued each such insurer shall have at least an A.M. Best rating of A- IX and replacement coverage shall be sought if the insurer's rating goes below AVIII. 7. At Hopper's reasonable request, Service Provider shall assure that it maintains insurance coverages as specified in this Section 8.1 naming Hopper as an additional insured or loss payee where relevant. 8. In the case of loss or damage or other event that requires notice or other action under the terms of any insurance coverage specified in this Section 8.1, Service Provider shall be solely responsible to take such action. Service Provider shall provide Hopper with contemporaneous notice and with such other information as Hopper may request regarding the event. 9. Service Provider's obligation to maintain insurance coverage shall be in addition to, and not in substitution for, Service Provider's other obligations hereunder and Service Provider's

	liability to Hopper for any breach of an obligation under the SA which is subject to insurance hereunder shall not be limited to the amount of coverage required hereunder.
8.3	**Risk of Loss**. Each Party shall be responsible for risk of loss of, and damage to, any equipment, software or other materials in its possession or under its control.
8.4	For Service Provider's breach of any term, condition, representation or warranty condition in this Article 8 (Insurance), Hopper's sole and exclusive remedy shall be the right to terminate the SA to which this Rider is attached without further liability, obligation or penalty of either party, provided that Hopper has paid Service Provider all fees outlined in Exhibit A for use of the Services for the then-current Term (or Hopper shall pay all such fees due for the remainder of the then-current Term in connection with such termination).
9. Indemnities	
9.1	**Indemnity by Service Provider**. Service Provider shall indemnify, defend and hold harmless Hopper and its Affiliates and their respective officers, directors, employees, agents, successors and assigns from and against any and all claims, suits and/or proceedings brought by third parties and resulting losses, judgments, costs, awards, expenses (including reasonable attorneys' fees, expert witness fees and costs of settlement) and liability of any kind (collectively, "Losses") arising from, in connection with, or based on allegations whenever made of, any of the following: 1. Any third-party claim of infringement or misappropriation of any Intellectual Property Rights, alleged to have occurred because of systems or other resources provided by Service Provider to Hopper, or based upon performance or receipt of the Services; provided that Service Provider's obligations under this Section shall not apply to any claims based upon: (A) any materials, software or other information that have been altered by Hopper or any party other than Service Provider; (B) the combination of the Services with any items not provided, required or approved by Service Provider, in writing. 2. Any third-party claim against Hopper arising out of, or in connection with, amounts owed by Service Provider, in whole or in part, or for which Service Provider is otherwise responsible (e.g., pass-through expenses, taxes, Losses arising from claims against Hopper that Service Provider Personnel are alleged to be employees or co-employees of Hopper, etc.); 3. Any third-party claim arising out of, or in connection with, Service Provider's breach of its obligations under Article 5 of this Rider; 4. Any third-party claim, demand, charge, action, cause of action, or other proceeding resulting from an act or omission of Service Provider in its capacity as an employer of a person; 5. Any third-party claim arising out of, or in connection with, any fraudulent or dishonest acts committed by Service Provider's employees, agents or subcontractors, acting alone or in collusion with others, including wrongful conversion of: (i) Hopper's, or any of its Affiliates', property, (ii) the property of any customers or patrons of such persons and (iii) the property of others in Service Provider's possession, care, custody or control; 6. Any third-party claim arising out of, or in connection with, Service Provider's breach of any applicable bank, credit and charge card association rules, as any of the foregoing may be amended from time to time,

	except in each case to the extent of Hopper's gross negligence, bad faith or willful misconduct (including Hopper's breach of Service Provider's Acceptable Use Policy).
9.2	**Indemnity by Hopper**. Hopper agrees to indemnify, defend and hold harmless Service Provider and its Affiliates and their respective officers, directors, employees, agents, successors and assigns from any and all Losses and threatened Losses arising from, in connection with, or based on allegations whenever made: (i) of any third party claim of infringement or misappropriation of any Intellectual Property Rights resulting from any Hopper Confidential Information provided to Service Provider by Hopper; or (ii) any claim relating to the acts, omissions, statements or representations of Hopper or its employees solely and directly in connection with any promotional or marketing by Hopper of the Services, except in each case to the extent of Service Provider's gross negligence, bad faith or willful misconduct.
9.3	**Additional Indemnities**. Each Party agrees to indemnify, defend and hold harmless the other, and its Affiliates, officers, directors, employees, agents, successors, and assigns, from any and all Losses and threatened Losses arising from, in connection with, or based on allegations whenever made of, any of the following: 1. the death or bodily injury of any agent, employee, customer, business invitee, or business visitor or other person caused by the indemnifying Party's tortious conduct; and 2. the damage, loss or destruction of any real or tangible personal property caused by the indemnifying Party's tortious conduct

9.4	**Indemnification Requirements and Procedures.** With respect to any claim that is the subject of indemnification under these Sections 9.1 through 9.3, the following requirements and procedures shall apply: 1. When Requirement to Defend Arises. Each Party's obligation to defend the other party is triggered as soon as an allegation is made against such party by a third party involving any of the above indemnification requirements. 2. Notice. Promptly after receipt by any entity entitled to indemnification under Sections 9.1 through 9.3 of notice of the assertion or the commencement of any action, proceeding or other claim by a third party for which the indemnitee will seek indemnification pursuant to any such Section, the indemnitee shall promptly notify the indemnitor of such claim in writing. No failure to so notify an indemnitor shall relieve it of its obligations under the SA, except as otherwise provided elsewhere in this Section 9, and to the extent that the indemnitor can demonstrate material prejudice to its ability to defend the claim attributable to such failure. Within fifteen (15) days after receipt of notice from the indemnitee relating to any claim, but no later than ten (10) days before the date on which any filing is due responding to a third party action, proceeding or other claim, the indemnitor shall notify the indemnitee in writing if the indemnitor acknowledges its indemnification obligation and elects to assume control of the defense and settlement of that claim (a "Notice of Election"). 3. Procedure Following Notice of Election. If the indemnitor delivers a Notice of Election relating to any claim within the required notice period, the indemnitor shall be entitled to have sole control over the defense and settlement of such claim; provided that (i) the indemnitee shall be entitled to participate in the defense of such claim and to employ counsel at its own expense to assist in the handling of such claim; and (ii) the indemnitor shall obtain the prior written approval of the indemnitee before entering into any settlement of such claim or ceasing to defend against such claim. After the indemnitor has delivered a Notice of Election relating to any claim in accordance with the preceding paragraph (and, in fact, diligently defends the claim), the indemnitor shall not be liable to the indemnitee for any legal expenses incurred by the indemnitee in connection with the defense of that claim. In addition, the indemnitor shall not be required to indemnify the indemnitee for any amount paid or payable by the indemnitee in the settlement of any claim for which the indemnitor has delivered a timely Notice of Election if such amount was agreed to without the consent of the indemnitor. 4. Procedure When No Notice of Election Is Delivered. If the indemnitor does not deliver a Notice of Election relating to a claim, or otherwise fails to acknowledge its indemnification obligation or to assume the defense of a claim, within the required notice period or fails to diligently defend the claim, the indemnitee may defend the claim in such manner as it may deem appropriate, at the cost, expense, and risk of the indemnitor, including payment of any judgment or award and the costs of settlement or compromise of the claim. The indemnitor shall promptly reimburse the indemnitee for all such costs and expenses, including payment of any judgment or award and the costs of settlement or compromise of the claim. If it is determined that the indemnitor failed to defend a claim for which it was liable, the indemnitor shall not be entitled to challenge the amount of any settlement or compromise paid by the indemnitee. 5. Failure to Defend in a Timely Fashion. If the indemnitor does not provide a defense to the indemnitee within a timely manner following receipt of the Notice of Election described in Section 9.3 above, and the indemnitee retains counsel to file responsive pleadings or other

filings to protect or advance the indemnitee's interests against any third party claim, the indemnitor shall be required to reimburse the indemnitee for its attorneys' fees and costs expended prior to the date on which the indemnitor agreed to defend the indemnitee, subject to Section 9.4.

9.5	**Infringement Remedies**. If any intellectual property used by Service Provider to provide the Services or included in the Services becomes, or in Service Provider's reasonable opinion is likely to become, the subject of an infringement or misappropriation claim or proceeding, in addition to indemnifying Hopper as provided in this Section 9.1 and to the other rights Hopper may have under the SA, Service Provider shall: 1. promptly secure the right at Service Provider's expense to continue using the intellectual property; 2. if this cannot be accomplished with commercially reasonable efforts, then at Service Provider's expense, replace or modify the Services to make it non-infringing or without misappropriation, provided that any such replacement or modification will not materially degrade the performance or quality of the affected component of the Services, or 3. if neither of the foregoing can be accomplished by Service Provider with commercially reasonable efforts, and only in such event, remove the intellectual property from the Services, in which case the charges shall be equitably adjusted to reflect such removal (and if in Hopper's reasonable opinion such removal is material to all or any portion of the remaining Services, Hopper may terminate such portion of the affected Services or the entire SA, as the case may be, without liability).
9.6	**Subrogation**. If an indemnitor is obligated to indemnify an indemnitee pursuant to this Article 9, the indemnitor shall, upon fulfillment of its obligations with respect to indemnification, including payment in full of all amounts due pursuant to its indemnification obligations, be subrogated to the rights of the indemnitee with respect to the claims to which such indemnification relates.

SCHEDULE A:
ANTI-BRIBERY AND ANTICORRUPTION CERTIFICATION MATERIALS

U.S. FOREIGN CORRUPT PRACTICES ACT (FCPA) GENERAL DESCRIPTION

_____

I. FCPA Liability

The U.S. Foreign Corrupt Practices Act of 1977 ("FCPA") prohibits U.S. companies, and their agents and employees, from corruptly giving, offering, promising or authorizing the provision of anything of value to foreign (non-U.S.) officials or foreign political parties, officials or candidates, for the purpose of influencing them in order to gain or maintain business or some competitive business advantage.

The FCPA also prohibits misrepresentations in a publicly-traded company's books and records and requires that the company's books, records and accounts be maintained in reasonable detail to accurately represent all transactions and payments. This includes maintaining an adequate system of internal financial controls.

In addition to prohibiting corrupt payments offered or made directly to foreign officials, the FCPA also forbids offering or paying anything of value to any person or entity (including intermediary third-parties) when it is known that all or part of the payment will be transmitted to a foreign official for one of the improper purposes mentioned above. Under the FCPA, a person is deemed to have acted "knowingly," and may therefore be held liable, when the payment is made or offered either with actual knowledge or in conscious disregard of circumstances that should have reasonably alerted them to the high probability of improper conduct. For this reason, it is vital that any "red flags" that arise in connection with a transaction involving business outside the United States be promptly resolved.

A corrupt act does not have to succeed in order to violate the law. An FCPA violation has occurred once an offer, promise or authorization for a corrupt payment has been made.

A "*Foreign Official"* for purposes of the FCPA means any:

- Non-U.S. government official (elected or otherwise) (including municipal, provincial, central, federal or any other level of government);
- Officer or employee of a foreign government or any department, agency, ministry or instrumentality thereof (including executive, legislative, judicial, regulatory or military);
- Person acting in an official capacity on behalf of a foreign government or any department, agency, ministry or instrumentality thereof;
- Officer or employee of a company or business owned or controlled in whole or in part by a foreign government;
- Officer or employee of a public international organization such as the United Nations or World Bank;
- Member of a royal family; or
- Foreign political party, member, or official thereof, or candidate for foreign political office.

The term also includes the children, spouse or other close relatives of a Foreign Official.

Anything of value" for purposes of the FCPA includes cash and cash equivalents such as unauthorized travel expenses, vacations, gifts, services and lavish entertainment.

II. Parent-Subsidiary Considerations

A U.S. parent company can be held liable for the extraterritorial acts of its foreign subsidiaries when it authorizes, directs or controls those acts. This includes instances where the parent company was willfully blind to or recklessly disregarded the conduct at issue. Accordingly, almost any amount of effective control over a subsidiary's activities puts a parent company at risk of FCPA liability for those activities. The DOJ and SEC, which share FCPA enforcement authority, take the position that U.S. companies can be held liable for the actions of their foreign subsidiaries under several other indirect theories, including:

- Unitary enterprise controlled by the parent (a.k.a., "alter ego," typically applied to majority or wholly- owned subsidiaries operating as part of a single group);
- Ratification or acquiescence (acceptance or retention of an illicit benefit where the company knows or should have known that the subsidiary's conduct was illegal); and
- Agency (vicarious responsibility for the acts of one's agents).

Subsidiary-based liability can turn on the level of ownership and/or the level of control the parent has over the subsidiary. Even mere equity ownership may be sufficient to create FCPA liability in certain circumstances, even if the equity stakeholder does not exert day-to-day operational control over the company. Relevant control considerations could include authority to appoint board members, company official presence on the board, ability to veto proposed acts, power to appoint senior executives and influence over company financial decisions.

III. Red Flags

If any of the following arise in connection with a current or proposed international transaction or activity, it indicates a potential compliance issue that must be resolved before proceeding:

Transaction Structure, Payments and Documents

- Questionable or unjustified transaction structures. Involvement of unnecessary or unqualified parties.
- Payment terms outside the normal course for the particular market or type of transaction, such as:
    - Payments requested in cash, upfront or to third parties outside the transaction.
    - Requests for unusually large commissions, retainers, fees, bonuses or other payments.
    - Payments through multiple layers of entities.
- Documentation problems, such as questionable, false or poorly documented invoices or requests for reimbursement.
- Actions or transactions occurring outside normal processes.
- Transactions that result in payments, margins or discounts that are unusually high, out of line with industry or market standards, appear unreasonable, or that otherwise lack justification, documentation or explanation.
- Any payment required to "get the business," or where there is a suggestion that the payment is being dictated by an outside party.

Reputation and Rumor

- Rumors regarding unethical or suspicious conduct by someone involved in the transaction.
- News or social media accounts indicating potentially unethical, criminal or otherwise improper conduct by someone involved in the transaction.

Questionable Government Connections

- Involvement of persons related to or otherwise closely connected to government officials or political parties.
- Political contributions or payments to a government official. Questionable requests, such as:

- Using the services of a specific partner, agent, consultant or representative at the suggestion of a government official.
    - Requests for increases in commission during the course of active negotiations involving government officials.
    - Any other abnormal activity within or relating to the transaction should also be considered a red flag.

IV. Conclusion

The FCPA applies to a U.S. company's operations worldwide, its employees and all persons and entities, wherever located, acting on behalf of the company. Companies and their individual officers, directors, employees and third parties found to have violated the FCPA can face substantial penalties. This risk is heightened by an aggressive enforcement environment, where federal law enforcement currently considers the investigation and prosecution of FCPA violations to be a significant priority.

CAPITAL ONE ANTI-BRIBERY AND ANTICORRUPTION (ABAC) COMPLIANCE CERTIFICATIONS

Spreedly Inc

The U.S. Foreign Corrupt Practices Act of 1977 ("FCPA") prohibits U.S. companies, and their agents and employees, from corruptly giving, offering, promising or authorizing the provision of anything of value to foreign (non-U.S.) officials or foreign political parties, officials or candidates, for the purpose of influencing them in order to gain or maintain business or some competitive business advantage.

The FCPA also prohibits misrepresentations in a publicly-traded company's books and records and requires that the company's books, records and accounts be maintained in reasonable detail to accurately represent all transactions and payments.

In addition to prohibiting corrupt payments offered or made directly to foreign officials, the FCPA also forbids offering or paying anything of value to any person or entity (including intermediary third-parties) when it is known that all or part of the payment will be transmitted to a foreign official for one of improper purposes mentioned above. Under the FCPA, a person is deemed to have acted "knowingly," and may therefore be held liable, when the payment is made or offered either with actual knowledge or in conscious disregard of circumstances that should have reasonably alerted them to the probability of improper conduct.

A corrupt act does not have to succeed in order to violate the law. An FCPA violation has occurred once an offer, promise or authorization for a corrupt payment has been made.

Numerous non-U.S. countries have enacted laws similar to the FCPA, and there are both U.S. and non-U.S. laws that prohibit both the bribery of government officials and the bribery of commercial parties. Such laws of particular relevance include the UK Bribery Act 2010 ("UK Bribery Act") and Canada's Corruption of Foreign Public Officials Act ("CFPOA").

The FCPA applies to Capital One operations worldwide, its employees and to all persons and entities, wherever located, acting on behalf of Capital One. Similar anti-bribery and anticorruption laws, including the UK Bribery Act and CFPOA, may also apply, depending of the facts and circumstances. Companies and individuals that violate the FCPA or other anti-bribery and anticorruption laws may be subject to fines and criminal penalties. Individual officers, directors, employees and third parties found to have willfully violated the FCPA may be fined and imprisoned for up to five years for each violation.

I hereby acknowledge having received and reviewed the U.S. Foreign Corrupt Practices Act (FCPA) General Description, as well as a copy of the U.S. Department of Justice's and U.S. Securities and Exchange Commission's Joint *A Resource Guide to the U.S. Foreign Corrupt Practices Act*. I further certify that I understand and will abide by the restrictions of the FCPA and any other applicable U.S. or non-U.S. anti-bribery and anticorruption laws.

IN WITNESS WHEREOF, the undersigned has executed this Certificate as of the 25th day of May, 2021.

DocuSigned by:
Justin Benson
6793B5D8B8EC48E...

Justin Benson
CEO
Spreedly Inc.

SCHEDULE B:
INFORMATION SECURITY REQUIREMENTS

1. DATA SECURITY

1.01 Service Provider shall provide industry standard encryption of Hopper Confidential Information in transit over public or leased circuits.

1.02 Service Provider shall provide industry standard encryption of Hopper Confidential Information at rest on local desktops, laptops, mobile devices, shared drives and removable media. Hopper Confidential Information shall not be stored on public facing systems that do not fall under the administrative control or compliance monitoring processes of the Service Provider.

1.03 Service Provider shall create, implement and maintain logical and/or physical data segregation that meets or exceeds industry standards to ensure Hopper Confidential Information is not viewable by unauthorized users.

1.04 If credit card data is made available to Service Provider as part of the Services, Service Provider shall encrypt at rest the full Primary Account Number (PAN) on all end-point storage devices located without limitation in laptops, servers, thumb drives and mobile devices.

1.05 Service Provider shall create, implement and maintain Data Loss Prevention (DLP) technology with related monitoring and response procedures that meets or exceeds industry standards.

1.06 Service Provider shall create, implement and maintain technical controls designed to prevent the unauthorized bulk export of Hopper Confidential Information outside of Service Provider's network.

1.07 Supplier shall create, implement and maintain filtering standards that meet or exceed industry standards and that, prevent the unintended download of malicious software from known hacking sites and suspicious emails.

1.08 Service Provider shall create, implement and maintain a process to monitor and detect unauthorized access to, misuse or misappropriation of, or fraudulent activity, involving Hopper Confidential Information that meets or exceeds industry standards.

1.09 Service Provider shall notify Hopper, promptly upon initial detection of any Confidential Information Violation related to the Services and in no event later than forty-eight (48) hours after the initial detection of the suspected Violation.

1.10 Service Provider shall create and maintain flow diagram(s) indicating how Hopper Confidential Information flows through both the Service Provider network environment as well as the network environment of any Approved Subcontractor. Service Provider shall provide such flow diagram(s) upon Hopper's reasonable request.

2. DATA SECURITY - PCI DSS

2.01 To the extent applicable to the Services and/or Service Provider, Service Provider shall create, implement and maintain the required level of Payment Card Industry Data Security Standard (PCI DSS) compliance and attestation established by the PCI Security Standards Council, and shall promptly provide related documentation upon Hopper's reasonable request. As required by the PCI DSS, such documentation shall include the definition of responsibilities for meeting applicable PCI DSS requirements specific to each service provided by Service Provider, including the definition of how these responsibilities are shared between Service Provider and Hopper.

3. DATA INTEGRITY AND MANAGEMENT

3.01 Service Provider shall create, implement and maintain for all business data elements provided to Hopper a data dictionary that meets or exceeds industry standards. Characteristics of the data dictionary shall include without limitation the business name, description and valid values of each data element. Service Provider

3.02 [Intentionally Omitted]

3.03 Service Provider shall remediate both self-identified and Hopper-identified data integrity issues. Service Provider shall provide integrity and remediation reports for Hopper Data: (i) upon occurrence of any data integrity failures; (ii) once per quarter on data where Service Provider provides the system of record; and (iii) upon Hopper's reasonable request.

3.04 Service Provider shall make available to Hopper, a digital copy of any conversation data and customer records, at Hopper's sole cost pursuant to an SOW between the parties.

3.05 For all Hopper Data, Service Provider shall create, implement and maintain a data retention and destruction program that meets or exceeds industry standards. Service Provider's process for data destruction shall include the creation of logs for all Hopper Data destroyed, which logs shall be made available for Hopper's review upon request.

3.06 [Intentionally Omitted]

4. DESKTOP, SERVER AND SYSTEM SECURITY

4.01 Service Provider shall create, implement and maintain system administration procedures that meet or exceed industry standards, including without limitation, system hardening, system and device patching (operating system and applications) and proper anti-virus installation as well as daily signature updates of same.

4.02 Service Provider shall create, implement and maintain security and system event logging procedures designed to meet or exceed industry standards in the detection, investigation and response to suspicious activity in a timely manner, including the retention of:

- Event logs for at least twelve (12) months for all its security devices, perimeter devices and policy enforcement points (including without limitation, firewalls, VPN servers and intrusion detection/protection systems).
- Network log-on records from authentication systems, including without limitation, domain controller logs (e.g., AD, LDAP, stand-alone local authentication controller, etc.) for at least one hundred twenty (120) days.
- Event logs for all other systems and applications for at least sixty (60) days.

4.03 Service Provider shall implement and maintain patch management procedures that meet or exceed industry standards and that require patches to be prioritized, tested and installed based upon criticality for all systems storing, transmitting and/or processing Hopper Confidential Information. Service Provider shall have the relevant patch installed within seven (7) days of patch release for vulnerabilities prioritized as 'critical' by the software/hardware vendor. Service Provider shall have the relevant patch installed within thirty (30) days of patch release for vulnerabilities rated as 'high' by the software/hardware vendor. Upon request, Service Provider shall provide Hopper a status of remediation efforts for zero-day or vulnerabilities determined to present material risk as identified at the sole discretion of Hopper.

4.04 Service Provider shall update and maintain change logs to document patch implementation activities including without limitation details regarding affected systems, patch identifiers, patch release dates and dates of implementation.

5. SYSTEM ACCESS MANAGEMENT PROCEDURES

5.01 Service Provider shall create, implement and maintain a logical system access provisioning process that meets or exceeds industry standards for all systems that access, process or store Hopper Confidential Information. Process documentation shall include procedures for proper segregation of access control roles, periodic management reviews for appropriateness of the current roles and timely access terminations.

5.02 The process shall specifically include operating standards for Privileged Users. A 'Privileged User' means a user who, by virtue of function and/or seniority, has been allocated access to systems that process Hopper Confidential Information that is significantly greater than that available to the majority of users.

5.03 Service Provider does not anticipate requiring logical access to Hopper systems, either hosted internally or outsourced to a third party, to perform the Services. If Service Provider requires such access, Service Provider shall provide Hopper with certain information for each Service Provider Personnel reasonably requested by Hopper to perform necessary due diligence and/or background checks in connection with requiring such access, taking into account the nature of the information that each Service Provider Personnel shall have access to and subject to such Service Provider Personnel's consent.

5.04 Service Provider shall notify Hopper promptly when system access for any Service Provider Personnel is no longer necessary to perform the Services. Hopper reserves the right to revoke system access for any Service Provider Personnel at any time, for any reason.

6. AUTHENTICATION

6.01 Service Provider shall create, implement and maintain password configuration and management procedures for all end user and system accounts related to the processing environment. Such procedures must follow recognized industry best practices in their configuration and management, including length and structure (commonly referred to as strong passwords), and passwords in accordance with the most recent NIST guidance.

7. INFORMATION SECURITY POLICY & GOVERNANCE

7.01 Service Provider shall create, implement and maintain an enterprise information security program that meets or exceeds industry standards and that includes without limitation, appropriate policies, governance structures, staffing, monitoring and assessment procedures. Service Provider's written program shall be approved by Service Provider's board of directors or similar governing body and at a minimum updated annually.

8. NETWORK SECURITY

8.01 Service Provider shall create, implement and maintain internal and external network security policies and procedures, including denial of service attack procedures where appropriate, all of which shall meet or exceed industry standards.

8.02 Service Provider shall actively monitor all systems for suspicious activity.

8.03 To the extent that it is commercially practicable, for Service Provider application(s) being provided to Hopper over the Internet, Service Provider shall provide access only to those IP addresses that are permitted to access the network.

8.04 Service Provider shall create, implement and maintain a network security assessment program in which network assessments are performed by Service Provider or by an external service provider on Service Provider's behalf to identify any vulnerabilities. The network shall be scanned for security vulnerabilities:

(i) at least annually and

(ii) after major hardware or software changes related to the Services.

8.05 Service Provider shall provide a summary report to Hopper defining remediation activities of any assessment findings that affect the delivery of the Services and an appropriate remediation strategy.

8.06 For Service Provider Personnel who require remote access to a network or system that protects, processes or stores Hopper Confidential Information, Service Provider shall create, implement and maintain remote access policies and procedures that meet or exceed industry standards. These policies and procedures shall include without limitation, a restriction of user access to Service Provider-owned devices, a minimum of two-factor authentication and retention for twelve (12) months of logs detailing all activity conducted during each user session.

8.07 Service Provider shall provide Hopper with the roles and responsibilities of all Service Provider Personnel who need remote access to Hopper owned or managed systems to perform the Services. Service Provider shall obtain Hopper's written approval prior to providing any Service Provider Personnel such access.

9. APPLICATION SECURITY & SOFTWARE DEVELOPMENT

9.01 Service Provider shall create, implement and maintain a software development lifecycle (SDLC) program that meets or exceeds industry standards for all software, applications, code, or web content to be presented on Hopper, or Service Provider websites, including but not limited to embedded scripts, or third party code (hereafter "Sensitive Applications") that support the engagement with Hopper or are provided as part of the Service. Service Provider shall build risk- based application security controls that includes without limitation, appropriate policies, governance structures, staffing and monitoring to manage the security of Sensitive Applications.

9.02 Service Provider shall create, implement, maintain and follow a documented set of secure coding standards, which are to be referenced for any internal development activities or maintenance coding.

9.03 Service Provider shall create, implement and maintain a formal dynamic application testing capability using a risk-based approach.

9.04 Service Provider shall engage qualified security representatives, either internal or external, to perform penetration testing of Sensitive Applications which shall include manual penetration testing.

9.05 [Intentionally Omitted]

9.06 Service Provider shall perform dynamic testing prior to Sensitive Applications being made available in production as well as after any material application upgrades or modifications.

9.07 Service Provider shall treat any information regarding identified application security vulnerabilities as Confidential Information

9.08 Service Provider shall evaluate and document the risk of each application security issue identified. Service Provider shall remediate identified application security issues utilizing a risk based approach within a reasonable timeframe in accordance with industry best practices.

9.09 Prior to formal closure of each, Service Provider shall re-test each Sensitive Application security issue to confirm remediation.

9.10 Service Provider shall report to Hopper any application security issues that will not be remediated prior to release to production.

10. HUMAN RESOURCE GOVERNANCE

10.01 Service Provider shall create, implement and maintain policies and procedures, which shall be documented and approved by its senior management, to support the hiring, termination, code of conduct, ethics and background screening of all Service Provider Personnel.

10.02 Service Provider shall create, implement and maintain a security awareness program for Service Provider Personnel, which provides initial education, on-going awareness and individual Service Provider Personnel acknowledgment of intent to comply with Service Provider's corporate security policies.

10.03 Service Provider shall create, implement and maintain a program to ensure Service Provider Personnel's physical access is revoked immediately upon termination or when access is no longer required.

10.04 Service Provider shall maintain a reporting mechanism to allow Service Provider Personnel to report any instance of questionable or unethical behavior, such as fraud and/or discriminatory behavior.

10.05 Service Provider shall ensure that all Service Provider Personnel performing End-Customer Facing Services or with access to Hopper Confidential Information are screened, to the extent permitted under law, in accordance with Hopper's requirements for Service Provider Personnel criminal background screening as provided or referenced herein, as well as industry best practices for performing criminal background screening.

Service Provider shall also ensure that no Service Provider Personnel that is deemed ineligible by Hopper to perform any End-Customer Facing Services or have access to Hopper Confidential Information.

10.06 Covered Personnel

Service Provider shall perform background screening as provided in this Section 10.06 for all Service Provider Personnel who have access to any funds, account, confidential or protected information or data, or computer systems of Hopper or any of its customers. These individuals include, but are not limited to:

- Persons with access to any Hopper computer system containing customer or account information.
- Persons with access to customer or company accounts, funds, or assets.
- Persons with access to any Hopper Confidential Information.

Screening Scope

Criminal history screening for these offenses must cover a period of no less than seven (7) years from the present, to the extent permitted by Applicable Laws, for all jurisdictions (domestic and international) in which the individual has resided, worked and/or attended school during that period.

Ineligibility Criteria:
Service Provider Personnel that are Covered Personnel must be excluded from engagement with Hopper if the employee has been convicted of a crime involving:

- theft, fraud, money laundering,
- breach of fiduciary duty,
- similar financial crime, or;
- as applicable, hate crime, or crimes involving violence,

which suggests that the employee poses a more than marginally greater level of risk than someone without a conviction to the safety and soundness of the human, intellectual, fiscal, or physical assets of Hopper, the confidentiality or security of data regarding its customers, Associates, or non-Associates, or the security of the financial accounts or assets of its customers, after an individualized assessment of the facts and circumstances of the conviction and individual.

10.07 New and/or Re-hired Service Provider Personnel: Service Provider shall conduct the above-described criminal background screening, for the purposes of determining eligibility, prior to the granting of access or assignment to Hopper. The criminal background screening shall be for the described period to the present (i.e. the current date or the date the screening was initiated).

11. PHYSICAL SECURITY

11.01 Service Provider shall create, implement and maintain physical security policies and procedures for all facilities that contain systems or personnel that provide the Services. Such policies and procedures shall include a process for managing, tracking and logging visitors to and within Service Provider's facility(s) and environment(s) where the Services are performed.

11.02 To the extent that it is commercially practicable, Service Provider shall create, implement and maintain a program of physical security monitoring and systems surveillance for all facilities that contain systems or personnel that provide Services to Hopper. This program shall include, but not be limited to, appropriate alarms, monitoring and response, access provisioning, CCTV cameras, access control points and visitor logging. This program shall cover the entry into Service Provider's facilities as well the overall internal operations. Service Provider shall retain all visual and other logging data for a minimum of: video; 30 days for Office/Professional worker space, 90 days for any PCI applicable operations (Data Center, Card Production/Embossing and/or Operations Centers), access and visitor logs (1 year). Service Provider does not have physical access control rights to our subcontracted data center, Amazon Web Services.

11.03 To the extent that it is commercially practicable, Service Provider shall create, implement and maintain a process for managing, tracking and logging visitors to and within Service Provider's facility(s) and environment(s) where the Services are performed.

11.04 Service Provider shall create, implement and maintain a documented process for managing, tracking and logging the protection, retention and destruction (e.g. shredding) of Hopper Confidential Information, regardless of media or format.

12. BUSINESS CONTINUITY

12.01 A. Service Provider shall create, implement and maintain a Business Continuity Program (BCP) that meets or exceeds industry standards and that provides a formal framework and methodology, including without limitation, a business impact analysis and risk assessment process to identify and prioritize critical business functions.

B. Supplier shall utilize internal and/or independent auditors to perform regular audits, including as applicable, a review of the BCP, governance structure, business documentation requirements, recovery strategies, Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), testing strategy and frequency.

C. Service Provider shall provide Hopper with information determined in Service Provider's discretion to enable Hopper's BCP to work in concert with Service Provider's BCP.

D. Service Provider shall participate in Hopper's recovery testing and/or exercises as reasonably requested by Hopper, on no more than an annual basis.

E. Service Provider shall perform BCP testing at a minimum of once every twelve (12) months.

i. To the extent that it is commercially practicable, Service Provider shall permit Hopper to participate in Service Provider's BCP testing.

ii. Service Provider shall share the results of all such BCP testing upon Hopper's reasonable request.

12.02 A. Service Provider shall develop, for Hopper's review and approval, the appropriate Service Level Objectives (SLOs), Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) necessary to restore or reconstitute the Services.

B. Service Provider shall notify Hopper within twenty-four (24) hours of an event requiring implementation of Service Provider's BCP.

C. Service Provider shall implement its BCP as required to ensure Service

Provider continues to function through an operational interruption, and:

i. continues to provide the Services within twenty-four (24) hours (RTO); and

ii. maintains data that is no less than two (2) hours from point of outage (RPO).

13. DISASTER RECOVERY

13.01 A. Service Provider shall create, implement and maintain a Disaster Recovery Program (DRP) that meets or exceeds industry standards and that provides a formal framework and methodology, including without limitation, a business impact analysis and risk assessment process to identify and prioritize critical business functions.

B. Service Provider shall utilize internal and/or independent auditors to perform regular reviews of the DRP, governance structure, business documentation requirements, recovery strategies, Recovery Time Objectives (RTOs), testing strategy and frequency.

C. Service Provider shall provide Hopper with information determined in Service Provider's discretion to enable Hopper's DRP to work in concert with Service Provider's DRP.

D. Service Provider shall participate in Hopper's DRP testing and/or exercises as reasonably requested by Hopper, on no more than an annual basis.

E. Service Provider shall perform DRP testing no less frequently than once every twelve (12) months.

i. Service Provider shall permit Hopper to participate in Service Provider's DRP testing.

ii. Upon reasonable request, Service Provider shall share the results of all such testing with Hopper.

F. In the event of a business disruption affecting the Services, Service Provider shall retain for a minimum of ten (10) days any data or files needed for Hopper to recover its business operations, unless Hopper directs a longer period in a particular instance of disruption.

13.02 A. Service Provider shall develop, in concert with Hopper, the appropriate Service Level Objectives (SLOs), Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) necessary to restore or reconstitute the Services.

B. Service Provider shall notify Hopper within twenty-four (24) hours of an event requiring implementation of Service Provider's DRP.

C. Service Provider shall implement its Disaster Recovery Program as required to ensure Service Provider continues to function through an operation interruption, and:

i. continues to provide the Services within twenty-four (24) hours (RTO); and

ii. maintains data that is no less than two (2) hours from point of outage (RPO).

14. [Reserved]

15. CLOUD UTILIZATION

15.01 For all relationships where Service Provider is leveraging Cloud services, Service Provider shall create, implement, and maintain Cloud security practices which meet or exceed industry standard security expectations for the Cloud services utilized.

15.02 A. Service Provider shall create, implement and maintain a process to review with Hopper all physical locations, by country, where technology will be utilized to provide the Services.

B. Except where Supplier obtains Hopper's express prior written consent, the physical location of Supplier's data center where all Hopper Confidential Information is stored must be within the United States.

15.03 A. Upon written request no more than on an annual basis, Service Provider shall (i) promptly complete any reasonable data protection questionnaire provided by Hopper and (ii) provide a copy of its SOC2 report(s) which may be used for Hopper to perform a risk assessment. To the extent such proof or information is reasonably deemed insufficient and if Service Provider's proposed Cloud environment does not permit Hopper to reasonably perform an assessment of the risk of maintaining its data in such Cloud-based environment, Hopper may terminate the Services that will be provided in the Cloud-based environment, provided that Hopper has paid Service Provider all subscription fees for the Services set forth in the applicable Order for the then-current Subscription Term (or Hopper shall pay all such subscription fees due for the remainder of the then-current Subscription Term in connection with such termination).

B. [Intentionally Omitted]

15.04 A. All Hopper information shall be encrypted at rest in public, community, or hybrid Infrastructure as a Service (IaaS) Cloud environments. Confidential/Proprietary information shall be encrypted at rest in public, community, or hybrid Platform as a Service (PaaS) or Software as a Service (SaaS) Cloud environments.

B. During instances of data processing, Hopper Information may be decrypted; however, Hopper Information shall only persist temporarily in volatile memory. Immediately following completion of any data processing activity, Hopper Information shall be re- encrypted for storage to the extent that it is commercially practicable.

C. The encryption key management service (used to encrypt and decrypt information) must not be co-located with the Hopper Information.

D. Should Service Provider not support customer controlled key management, Service Provider shall only utilize encryption key management services which are auditable and which align with industry standards, including without limitation:

- The ability to expire, revoke, or destroy keys at the end of their useful life.
- Rotation of keys on a periodic basis.
- Secure back up of keys.
- Appropriate key algorithm, strength and length, with a minimum of 256 bit AES encryption.
- Keys are logically or physically separated from the Hopper Information.
- Access to keys is restricted to the minimum number of custodians and ensures separation of duties.
- Access to keys is logged and audited.

15.05 A. Service Provider shall create, implement and maintain a formal program to track and report end users with access to systems that support the Services.

B. [Intentionally Omitted]

C. For any Cloud service providers that will not agree to assessment rights, Service Provider shall ensure that appropriate independent audit testing occurs annually and the resulting reports (e.g. SSAE 16 SOC1, SOC2, PCI, etc.) are reviewed and subsequently shared with Hopper. Service Provider shall also identify any gaps to contractual requirements with Hopper and develop appropriate remediation plans.

D. Service Provider shall provide the details of the audit report review and the remediation plan to Hopper within thirty (30) days of issuance of the audit report by the Cloud service provider.

16. IT OPERATIONS

16.01 Service Provider shall establish, document and maintain processes and procedures to deliver the technical services to support its IT operations framework as described and set forth in this Exhibit ('Technical Support Services').

16.02 A. Service Provider shall provide Technical Support Services sufficient to meet or exceed

the Hopper requirements specified within this Exhibit.

B. Service Provider Personnel performing Technical Support Services shall have subject matter expertise and be fully trained in Incident identification and resolution.

C. Service Provider shall provide Technical Support Services by telephone, website access, direct connection and/or on-site visits as the situation requires, provided that Service Provider shall at all times comply with Hopper's policies and procedures regarding remote access.

D. Service Provider shall provide to Hopper all reasonably necessary toll-free telephone consultation requested in connection with Hopper's use and operation of any software, systems, services or any problems therewith.

16.03 A. Service Provider shall create, implement and maintain a change management program that meets or exceeds industry standards for all assets and systems that provide the Services. The program shall include without limitation, maintenance, patches, data formatting changes, new deployments of code or systems, or for any work to restore services as the result of an Incident. The program shall implement a division of roles and responsibilities and establish a process through which changes are tracked and approved.

B. Prior to using any new software or new equipment to provide the Services, Service Provider shall have verified that the item has been properly tested and installed, is operating in accordance with its specifications and is performing its intended function in a reliable manner. Service Provider shall maintain the ability to restore prior operational capabilities in all circumstances.

C. To the extent that it is commercially practicable, Service Provider shall not make material changes, including implementing a change in technology, without at least a 90-day prior written notification to Hopper, including:

i. a change adversely affecting the function or performance of the Services;

ii. a change which results in an increase to Hopper's charges under the Agreement;

iii. a change which affects the way in which Hopper conducts its business or operations;.

16.04 To the extent that it is commercially practicable, Service Provider shall create, implement and maintain a service level management program that meets or exceeds industry standards. Such program will ensure that a formal process framework is defined and process standards are in place for creating and maintaining service requirements, service definitions, SLAs and OLAs.

16.05 A. Service Provider shall create, implement and maintain a performance and capacity management process that meets or exceeds industry standards to plan, establish, monitor and review IT resource performance and capacity levels.

B. Service Provider shall ensure that proper monitoring and analysis are in place to identify workload trends which shall be used as input for periodic performance and capacity forecasting.

16.06 [Intentionally Omitted]

16.07 A. Service Provider shall create, implement and maintain a service desk function that meets or exceeds industry standards to register, communicate, dispatch and analyze all calls; report Incidents; initiate service requests; and respond to status information requests.

B. Service Provider shall implement monitoring and escalation procedures based on agreed upon service levels to classify and prioritize any reported issue as an Incident, a service request or an information request.

C. Service Provider shall provide Hopper with appropriate initial contact and escalation procedures for communicating with the service desk.

D. If Service Provider does not respond and begin to remedy an Incident within the Target Resolution Time, Service Provider shall meet with Hopper to discuss the issue and determine the best course of action for resolving the issue.

E. Service Provider shall resolve Low Severity Incidents according to mutually agreed upon priorities, but each Low Severity Incident involving software shall be resolved no later than the date of the next release of the applicable software.

16.08 A. Service Provider shall create, implement and maintain formal Problem management procedures including without limitation the investigation into the Root Cause of identified Incidents and the definition of solutions for identified IT operations Problems.

B. Service Provider shall record and track IT operational Problems that affect the Services delivered through resolution. Service Provider shall provide this information to Hopper upon request.

16.09 For material Changes to the Service and where commercially practicable, Service Provider shall notify Hopper (i) at least seven (7) days prior to implementation, and (ii) within two (2) days following completion of planned Changes to the Services. Where not commercially practicable, Service Provider will notify Hopper of all Changes to the Services via the changelog maintained at https://docs.spreedly.com/changelog/. Service Provider shall retain all change requests and change approvals for a minimum of thirteen (13) months and shall make the same available to Hopper upon request. Change notifications shall, at a minimum, include the following attributes:

- Change Number;
- Change Description;
- Change Risk (High, Med, or Low); and
- Planned Implementation Date.

Service Provider shall notify Hopper

(i) at least seven (7) days prior to implementation, and

(ii) within two (2) days following completion of planned Changes to the Services. Service Provider shall retain all change requests and change approvals for a minimum of thirteen (13) months and shall make the same available to Hopper upon request. Change notifications shall, at a minimum, include the following attributes:

- Change Number;
- Change Description;
- Change Risk (High, Med, or Low); and
- Planned Implementation Date.

16.10 Service Provider shall provide Hopper with a method of monitoring the performance of the Services through the use of technical means.

16.11 A. For any High Severity Incident, Service Provider shall take all reasonable steps to supply a correction to Hopper as soon as possible. Such steps shall include without limitation the assignment of qualified, dedicated staff to work on the Incident until an acceptable correction is implemented. If Service Provider provides Hopper with a workaround deemed acceptable by Hopper for a High Severity Incident, Hopper may classify the Incident as restored. Work is expected to continue until the issue is fully resolved.

B. Upon detecting or being notified of a High Severity Incident, Service Provider shall:

i. Immediately assemble the appropriate personnel to analyze the Incident;

ii. Identify potential solutions and determine the best plan of action (which may include providing a temporary work-around acceptable to Hopper until a permanent correction can be provided);

iii. Immediately engage Hopper and allow active participation in the Incident management process provided that such participation shall not waive any other contractual rights Hopper may have; and

iv. Provide a dedicated representative to keep Hopper continuously informed of the Incident status via status.spreedly.com.

16.12 A. Service Provider shall provide a preliminary Root Cause Analysis (RCA) report for all High Severity Incidents within one (1) Business Day of the resolution of the Incident via status.spreedly.com. The preliminary report shall provide Hopper with:

i. Actions being taken to drive towards Root Cause remediation; and

ii. Actions being taken to prevent an Incident reoccurrence.

B. Service Provider shall provide final RCA reports for High Severity Incidents within five (5) Business Days of the resolution of each Incident via status.spreedly.com.

C. Service Provider shall provide final RCA reports for Trended Low Severity Incidents within ten (10) Business Days of Hopper's request via status.spreedly.com.

D. All RCA reports shall include:

- Incident Summary;
- Incident Details;
- Root Cause Description;
- Timeline of Events; and
- Response/Follow-up Actions to prevent Incident recurrence

16.13 A. Service Provider shall create, implement and maintain a Configuration Management program that meets or exceeds industry standards and which shall include a Configuration Management Database (CMDB) or similar central repository to track all relevant information on Configuration Items (CIs). Service Provider shall monitor and record all CI assets and changes to assets. Service Provider shall maintain a baseline of CIs for every system and service which will serve as a point-in-time reference.

B. Service Provider shall periodically review Configuration Items to verify and confirm the integrity of the current and historical configuration. Service Provider shall periodically review installed software

against the software usage policy to identify any personal or unlicensed software or any software instances in excess of current license agreements. Identified issues shall be logged and errors and deviations appropriately corrected.

16.14 Service Provider shall develop, implement, maintain and comply with a Procedures Manual for the Services or Product. Service Provider shall provide reasonable information to allow Hopper to develop processes that will work in concert with

Service Provider's processes. The Procedures Manual need not be unique to Hopper, and may consist of one or more existing product manuals or other documentation as appropriate to the Services. The Procedures Manual shall serve as the record of all steps necessary for the successful operation of the Services or Product as required by Hopper.

16.15 Service Provider shall make available to Hopper a report containing the following:

1. Changes: The changes completed during the previous month. Changes can be continuously monitored via https://docs.spreedly.com/changelog/. Each listed change shall include the following:

- Change Number;
- Change Description;
- Change Risk (e.g., High, Med, Low);
- Implementation Date; and
- Date Hopper was initially notified.

2. Incidents: All issues that caused downtime during the previous month. Incident reports are published via status.spreedly.com. Each listed incident shall include the following:

- Incident Number;
- Incident Description;
- Incident Severity;
- Incident Start Time;
- Incident Resolution Time; and
- Time Hopper was initially notified.

3. Capacity and Performance: To the extent that it is commercially reasonable, a monthly twelve (12) month forecast of capacity and performance. In lieu of such a report, Service Provider and Hopper may agree to incorporating Capacity and Performance reviews into at least quarterly business review meetings. These reports shall include the following:

- Capacity Monitors;
- Planned Capacity Allocated to Hopper; and
- Expected Capacity Utilization versus Planned Allocation.

17. ONGOING REMEDIATION OF RISK ASSESSMENT FINDINGS

As part of Hopper's Information Assurance and Security due diligence process, risk assessments of Service Providers services will be performed on an ongoing basis to evaluate the controls as described within this exhibit.

17.01 Service Provider agrees to remediate vulnerabilities detected during Hopper's risk assessments of Service Provider security and operational controls according to the following criteria:

A. For purposes of this section, vulnerabilities will be classified at the discretion of Hopper and validated by the Service Provider as follows:

(i) an "Extreme" or "High Finding" has a high probability of exposing Hopper Confidential Information to unauthorized viewing, modification, deletion or acquisition as well as attacks that could result in data corruption;

(ii) a "Medium Finding" involves a potential compromise or loss of Hopper Confidential Information which is possible based on the failure to observe security requirements specified in the Agreement; and

(iii) a "Low Finding" involves threats that:

(1) are considered extremely difficult for attackers to exploit;

(2) have a low probability of being exercised, and/or

(3) if exploited, are of minor consequence to the security of Hopper Confidential Information.

B. Extreme and High Findings

(i) Service Provider shall provide remediation plans within five (5) Business Days of receipt of the risk assessment report of findings.

(ii) Findings shall be remediated immediately unless otherwise agreed to in writing by both Parties.

(iii) Remediation of these findings is required prior to receipt of Hopper Information and the start of Services.

C. Medium Findings

(i) Service Provider shall provide remediation plans within ten (10) Business Days of receipt of the risk assessment report of findings.

(ii) Findings shall be remediated within ninety (90) days or as agreed to in writing by both Parties.

(iii) Remediation of these findings is required prior to receipt of Hopper Information

D. Low Findings

(i) Service Provider shall provide remediation plans within twenty (20) Business Days of receipt of the risk assessment report of findings.

(ii) Findings shall be remediated within one hundred eighty (180) days or as agreed to in writing by both Parties. Service Provider may elect, at its own discretion, to not remediate Low Risk Findings.

(ii) Remediation of these findings is not required prior to receipt of Hopper Confidential Information and the start of Services, unless otherwise directed by Hopper.

E. If Service Provider, despite its best efforts, is unable to correct a security vulnerability within the timeframes specified above, Hopper may, in its discretion and in writing, extend the timeframe for correction. If Service Provider is unable to correct the security vulnerability after this extended timeframe, Hopper may, without penalty of any kind, elect to immediately terminate

the Agreement and/or part or all of any or all Order Forms and SOWs without liability as of a date specified in the notice of termination.

18. APPENDIX

18.01 Definition of Cloud Services:

The use of the term 'cloud' suggests a different multi-tenant IT hosting environment than traditional IT hosted services environments (like mainframes or traditional application hosting providers). For the purposes of this Agreement, Hopper follows the National Institute of Standards and Technology (SP 800-145) to establish whether or not Service Provider is a public cloud service. Characteristics that identify a service as 'cloud' are:

- On-demand Self-Service: A consumer can unilaterally provision computing capabilities.
- Broad Network Access: Capabilities are available over the network and accessed through standard mechanisms that promote use by thin or thick client platforms, both mobile and fixed.
- Resource Pooling: The provider's computing resources are pooled to serve multiple consumers in a multi-tenant model, with resources dynamically assigned and reassigned

according to demand. Examples of resources include storage, processing, memory and network bandwidth.

- Rapid Elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.

- Measured Service: Cloud systems automatically control and optimize resource use by leveraging a metering capability appropriate to the type of service. Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of the utilized service. Further, third parties who are cloud providers offer different types of IT services within their cloud environment, with each having their own specific risk concerns. Third parties who utilize cloud service providers as part of the Services fall into one of these categories.

- There are three distinct Cloud Service Models:

A. SaaS - Software as a Service: The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.

B. PaaS - Platform as a Service: The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider.

C. IaaS - Infrastructure as a Service: The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

18.02 The following list of terms are defined as such for the purposes of this Exhibit. Terms not specifically defined in this Exhibit or elsewhere in the Agreement shall have the meanings commonly ascribed to them.

- 'Configuration Item' (CI) means a component of the IT Infrastructure, logical or physical, that is required to provide the services, systems or applications.

- 'Emergency Change' means any production change required to restore service as a result of an Incident.

- 'High Severity Incident' shall mean any Incident that results in the degradation of one or more critical business functions that is visible to external customers or impacts their experience with Hopper OR Causes immediate, high levels of impact to Hopper economics, operations, brand, reputation, legal or regulatory compliance.

- 'Incident' means any IT event that is not part of the standard operation of the

Services; and causes, or may cause, an interruption to, or a reduction in, the quality of the Services.

- 'Incident Resolution' means service restoration to minimize service disruption by restoring to agreed levels within the timeframes established in this Exhibit.

- 'Low Severity Incident' means any Incident that has a low to moderate level of impact on Hopper's customers, economics, operations or brand.

- 'Change' shall mean a scheduled change that has the potential to impact production.

- 'Problem' means a cause of one or more Incidents. The cause is usually not known at the time an Incident occurs. The Problem Management process is responsible for further investigation and tracking the implementation of preventative solutions.

- 'Procedures Manual' means the record of all steps necessary for the successful operation of the Services as well as a definition of roles, responsibilities and interactions for the Service Provider, Hopper and applicable Approved Subcontractors.

- 'Root Cause' means the underlying or original cause of an Incident or Problem.

- 'Target Resolution Time' means the timeframe in which Service Provider will make Commercially Reasonable Efforts to restore the Services.

- 'Trended Low Severity Incident' means two or more Low Severity Incidents that occur within a thirty (30) day period.

SCHEDULE C: LIST OF APPROVED SUBCONTRACTORS

SPREEDLY INC.

Name of Subcontractor	**Approval provided by Hopper in writing (Employee name)**	**Date**
All processors listed at: https://www.spreedly.com/gdpr-subprocessors	Joost Ouwerkerk	**25 MAY 2021**