



SERVICE AGREEMENT

Part A: Parties

SPREEDLY		CUSTOMER	
Name:	Spreedly, Inc.	Name:	SUEZ North America, Inc.
Address:	733 Foster Street, Suite 100	Address:	461 From Rd, Suite 400
City/State:	Durham, NC 27701	City/State:	Paramus, NJ 07652
PRIMARY SPREEDLY CONTACT		PRIMARY CUSTOMER CONTACT	
Name:	Shawn Curtis	Name:	Douwe Busschops
Title:	Senior Enterprise Account Executive	Title:	Director Customer Experience
Phone:	888-727-7750	Phone:	201-634-4255
Email:	shawn@spreedly.com	Email:	douwe.busschops@suez.com

Part B: Terms

1. This Service Agreement (including its exhibits, the "**Agreement**") is effective as of the last date of signing below ("**Effective Date**") and is between Spreedly, Inc. ("**Spreedly**"), and the customer listed above (the "**Customer**"). Except as otherwise provided herein, this Agreement is subject to the Spreedly Privacy Policy ("**Privacy Policy**"), which is incorporated herein by reference, and which can be viewed at <https://spreedly.com/>. To the extent that any term in the Privacy Policy conflicts with the terms of this Agreement or any inconsistency between the Privacy Policy and this Agreement exists, the terms of this Agreement shall prevail.
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.
 - 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. Spreedly shall immediately notify Customer of any instance where it does not store or submit Customer transaction under this Subsection 2.d.
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 Spreadly, 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 one (1) year from the Effective Date (the "**Initial Term**"). Thereafter, this Agreement shall automatically renew for successive one year periods (each, a "**Renewal Term**" and, together with the Initial Term, the "**Term**") unless either party has provided written notice of its intent to not renew this Agreement not less than sixty (60) days prior to the expiration of the then-current Initial or Renewal Term.
- b. Either party may terminate this Agreement, by written notice to the other party effective as of the date specified in such notice, if the other party materially breaches this Agreement and such breach: (i) cannot be cured; or (ii) being capable of cure, remains uncured thirty (30) days after the breaching party receives written notice thereof. Without limiting the foregoing, in the event of a breach that gives rise to the right by Spreadly to terminate this Agreement, Spreadly 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. Spreadly's exercise of its right to suspend performance shall be without prejudice to Spreadly's right to terminate this Agreement upon written notice to Customer.
- c. Upon termination of this Agreement, (i) Spreadly 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 Spreadly trademarks and immediately remove any Spreadly 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).
- d. In the event of a breach that gives rise to the right by Customer to terminate this Agreement, Spreadly shall provide transition services to Customer.

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 Spreadly 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. Spreadly will charge Customer the fees outlined on Exhibit A for use of the Services.

7. Confidential Information.

- a. For the purposes of this Agreement, "**Confidential Information**" means any and all technical and non-technical information, whether in graphic, electronic, written or oral form, disclosed by either Spreadly or the Customer, including the Spreadly API or any API owned or otherwise controlled by the Customer, any ideas, techniques, drawings, designs, descriptions, specifications, works of authorship, 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 each of the parties, 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, Personal Information, sales and merchandising, marketing plans of or related to Spreadly or the Customer and information either party provides to the other regarding or belonging to third parties, whether or not labeled or marked as "Confidential," "Proprietary" or with a similar proprietary legend, and which may also be disclosed verbally. "Confidential Information" does not include any information which: (i) now or hereafter enters the public domain through no breach of an obligation of confidentiality or other fault of a party; (ii) the receiving party independently knows free of any obligation of confidentiality at the time of receiving such information; (iii) a third party hereafter furnishes to the receiving party without restriction on disclosure and without breach of any confidentiality obligations; or (iv) employees or agents of a receiving party have independently developed without any use of or reference to any Confidential Information and without breaching this Agreement.
- b. Each party shall: (i) only disclose 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 Confidential Information to any third party, except as permitted herein; (iii) protect and safeguard any and all Confidential Information using the same standard of care as it uses to protect and

safeguard its own confidential and/or proprietary information, but in no event less than a reasonable standard of care; (iv) use such Confidential Information only to the extent required for the purposes of this Agreement; (v) not reproduce Confidential Information in any form except as required for the purposes of this Agreement; (vi) not reverse-engineer, decompile, or disassemble any software or devices disclosed by the other party; (vii) not directly or indirectly export or transmit any Confidential Information to any country to which such export or transmission is restricted by regulation or statute; and (viii) promptly provide the other party with notice upon discovery of any loss or unauthorized disclosure of the Confidential Information. Each party shall be liable for any failure of its Representatives to abide by the provisions of this Agreement as if such failure was the act or omission of such party.

- c. Notwithstanding the foregoing, either party may disclose Confidential Information (i) to the extent required by a court of competent jurisdiction or other governmental authority or otherwise as required by applicable Laws; or (ii) on a "need-to-know" basis and under an obligation of confidentiality to its legal counsel, accountants, banks and other financing sources and their advisors, or to a Qualified Security Assessor ("**QSA**") for the purpose of assessing compliance with the Payment Card Industry Data Security Standards ("**PCI-DSS**").
 - d. All Confidential Information (including all copies thereof) shall remain the property of the disclosing party. Upon the request of the disclosing party, the receiving party shall either (a) return such materials to the disclosing party; or (b) certify in writing as to the destruction thereof.
8. References to Relationship. Any press release, public announcement or media communication regarding this Agreement may only be made with the written approval of both Parties.
9. PCI-DSS. Spreadly 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. Spreadly 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 Spreadly 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. Spreadly 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, Spreadly 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, Spreadly 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 has passed its most recent scan.
 - c. Spreadly 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. Spreadly agrees to supply Customer with evidence of its most recent Annual Assessment prior to or upon execution of this Agreement. Thereafter, Spreadly shall annually supply to Customer, or make available on www.spreadly.com, evidence of Spreadly'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. Spreadly 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 Spreadly supports third-party vaulting (a "**Supported TPV Endpoint**") as set forth at: <https://docs.spreadly.com/guides/third-party-vaulting/>. For any endpoint that is not a Supported TPV Endpoint, Customer may request that Spreadly 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. Spreadly 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 relevant storage fees determined in accordance with Exhibit A of this Agreement.

- g. Per PCI-DSS Spreadly shall adhere to minimum encryption standards prescribed for all Customer data at rest or in motion.
 - h. Spreadly shall not store CVV numbers permanently.
10. Security. Without limiting the requirements of this Agreement, Spreadly 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, Spreadly represents and warrants the following:
- a. Spreadly 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. Spreadly's information security program satisfies the requirements of all data security Laws applicable to Spreadly, 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. Spreadly 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 Spreadly Personnel with access to Customer Confidential Information are provided appropriate information security and privacy training to ensure their compliance with Spreadly's obligations and restrictions under this Agreement, with applicable Laws and with Spreadly'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 Spreadly 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 Spreadly in Processing such information or otherwise providing services under this Agreement.
 - b. If there is a Breach of Security, Spreadly 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. Spreadly 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. Spreadly shall not inform any third party of any Breach of Security, except other affected Spreadly customers or as may be required by applicable Law, without first obtaining Customer's prior written consent, which shall not be unreasonably withheld.
12. Insurance. At all times during the Term, Spreadly shall maintain (i) commercial general liability insurance with at least \$1,000,000 per occurrence and (ii) “errors and omission” (tech and cyber coverage) insurance in an amount not less than \$10,000,000. Upon Customer's request, Spreadly shall provide Customer with a copy of such policy or policies or a certificate of insurance evidencing the same.
13. Indemnification.
- a. Spreadly 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 Spreadly of Section 7 (Confidential Information), Section 9 (PCI-DSS) or Section 10 (Security); or (iii) any Breach of Security that is caused by by Spreadly's breach of its security obligations set forth in Section 10; (iv) Spreadly's violations of the terms of this Agreement.
- b. Customer shall indemnify, defend and hold harmless Spreadly against any loss or damage that Spreadly 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 violation of 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 13.a or 13.b. The party seeking indemnification (the "**Indemnitee**") shall cooperate with the other party (the "**Indemnitor**") at the Indemnitor's sole cost and expense. The Indemnitor shall promptly assume control of the defense and investigation of such Claim and shall employ counsel of its choice to handle and defend the same, at the Indemnitor's sole cost and expense. The Indemnitee's failure to perform any obligations under this Section 13.c will not relieve the Indemnitor of its obligations under this Section 13 except to the extent that the Indemnitor can demonstrate that it has been materially prejudiced as a result of such failure. The Indemnitee may participate in and observe the proceedings at its own cost and expense with counsel of its own choosing. The Indemnitor shall not enter into any settlement that imposes any liability or obligation on the Indemnitee without the Indemnitee's prior written consent.
14. Limitation of Liability.
- a. IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY LOST PROFITS, OR ANY INDIRECT, EXEMPLARY, PUNITIVE, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF BUSINESS PROFITS) ARISING OUT OF OR RELATING TO THIS AGREEMENT, HOWEVER CAUSED, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- b. EXCEPT FOR A PARTY'S INDEMNIFICATION OBLIGATIONS IN SECTION 13 AND FOR A BREACH OF THE CONFIDENTIALITY OBLIGATIONS IN SECTION 7 ABOVE 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 SPREADLY BY CUSTOMER UNDER THIS AGREEMENT DURING THE TWELVE MONTH PERIOD IMMEDIATELY PRECEDING SUCH CLAIM.
- c. NOTWITHSTANDING THE FOREGOING, THE LIMITATIONS AND EXCLUSIONS OF LIABILITY IN SECTIONS 14.a AND 14.b DO NOT APPLY TO THE FRAUDULENT, CRIMINAL OR NEGLIGENT OR MORE CULPABLE ACTS OR OMISSIONS OF A PARTY.
15. Assignment. The parties' rights and obligations under this Agreement will bind and inure to the benefit of their respective successors and permitted assigns. Neither party shall assign or delegate its obligations under this Agreement either in whole or in part without the prior written consent of the other party; provided, however, that either party may assign this Agreement in its entirety, without the other party's consent, to an entity that acquires all or substantially all of the business or assets of the assigning party relating to the subject matter of this Agreement, whether by merger, reorganization, acquisition, sale or otherwise.
16. Notices. Any notices required to be delivered in writing hereunder shall be sent to the party's address set forth in Part A and shall be deemed delivered when (i) by personal delivery (when actually delivered); (ii) by overnight courier (upon written verification of receipt); or (iii) by certified or registered mail, return receipt requested (upon verification of receipt). Either party may change its address at any time by giving written notice of the change to the other party.
17. Force Majeure. Neither party will be liable for failure or delay in performance due to causes beyond its reasonable control, including without limitation acts of God, terrorism, war, riots, fire, earthquake, flood or failure of internet or communications infrastructure. Notwithstanding the foregoing, if any force majeure event lasts more than thirty (30) days, Customer will have the right to terminate the Agreement.
18. Survival. Sections 3.a (Ownership), 4.c (Effect of Termination), 7 (Confidential Information), 13 (Indemnification), 14 (Limitation of Liability), 18 (Survival) and 19 (Miscellaneous) will survive expiration or termination of this Agreement.
19. Miscellaneous. This Agreement shall be governed by the Laws of the State of Delaware (without regard to its choice of law provisions). 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 parties are independent contractors and this Agreement does not create an agency, partnership, joint venture, employee/employer or other similar relationship between them. The failure to require performance of any provision shall not affect a party's right to require performance at any time thereafter, nor shall a waiver of any breach or default of this Agreement constitute a waiver of any subsequent breach or default or a waiver of the provision itself.

[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.

By:

Name: Justin Benson
Title: CEO
Date: April 4, 2019

SUEZ North America, Inc.

By:

Name: Michael Salas
Title: SVP, Chief Information Digital Officer
Date: April 4, 2019


 Digitally signed by Michael Salas
DN: cn=Michael Salas, o=SUEZ,
ou=Exec,
email=Michael.Salas@suez.com, c=US
Date: 2019.04.04 08:44:49 -0400

EXHIBIT A

PRICING

The initial term of this agreement is 12 months. Customer shall pay Spreadly a total fee of \$77,000 for the first 12 months of service. For each subsequent 12 months of service, Customer shall pay Spreadly \$105,000 for the Base Annual Fee, which shall entitle Customer to the following for the duration of the Term:

SUEZ North America, Inc. - Enterprise Pricing Table		
	Year 1	Subsequent Years
Enterprise Platform Fee	\$65,000	\$75,000
Tier 1 Enterprise Platform Fee	\$75,000	\$75,000
Year 1 Discount	-\$10,000	\$0
Enterprise Assurance Agreement & SLAs	included	included
Existing Spreadly Endpoints	unlimited	unlimited
PCI Compliant Card Storage Limit	unlimited	unlimited
Add New Standard PMD Endpoints	included	included
API Usage Fee	\$12,000	\$30,000
Included Non-Partner API Calls	2,000,000	5,000,000
Included Partner API Calls	unlimited	unlimited
Cost per API Call	\$0.0060	\$0.0060
Total Base Annual Fee	\$77,000	\$105,000

Spreadly will apply a one-time \$2,000 discount to the API Usage Fee for the Initial Term if this Agreement is executed and becomes effective on or before April 3, 2019. In this case total Year 1 Fees owed will be \$75,000.

API Usage Fees

The API Usage Fee in the table above includes an initial allotment of 2,000,000 API calls. The following API calls made to partner gateways will not be counted against that allotment as long as partner remains in good standing in the Spreadly gateway partner program:

- A Purchase API call against the partner gateway
- A Capture API call against the partner gateway
- A Refund API call against the partner gateway
- A Void API call against the partner gateway
- An Authorization API call against the partner gateway

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

- If the overage first occurs in Months 1 through 10: billed at \$0.012 per API call for the remainder of the contract term.
- If the overage first occurs in Month 11 or 12: billed at \$0.009 per additional API call for the remainder of the contract term.

Enterprise Account Management

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

Payment

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

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

Total fees owed under this contract:

- Year 1: \$77,000
- Year 1 (if this Agreement is executed and becomes effective on or before April 3, 2019): \$75,000

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

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

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

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

EXHIBIT B

SUPPORT; SERVICE LEVEL AGREEMENT

Service Level Agreement

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

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

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

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

Service Credits may not be redeemed for cash and shall be applied to Customer's next applicable payment of Base Annual Fee. The issuance of Service Credits sets forth Spreadly's sole obligation and liability and Spreadly's sole remedy for any Service Level Failure.

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

Support

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

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

Category	Definition	Spreadly Acknowledgement Time	Resolution
Low	End-user or Customer complaint that requires investigation by Spreadly (including bugs not impacting API uptime)	Up to 48 hours	Next update

Category	Definition	Speedly Acknowledgement Time	Resolution
Serious	Customer's use of Transaction Processing Service is severely impaired due to Speedly-side issue	Up to 4 hours	Within 3 days
Critical	Transaction Processing Service is unavailable due to Speedly-side issue	Up to 60 minutes	Within 1 day

Speedly 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

Information Security Requirements Exhibit

This Information Security Requirements Exhibit ("IS Exhibit") is by and between Spreadly, Inc. ("Vendor") and SUEZ North America, Inc. ("SUEZ") and is attached to this Enterprise Services Agreement ("Agreement") and is effective as of the execution date of this Agreement. To perform the services described in the Agreement, SUEZ may grant Vendor access to or use of Confidential Information (as defined in the Agreement), systems and technology of SUEZ (together "SUEZ Systems"), and Vendor agrees to abide by the terms of this IS Exhibit in connection with its access to or use of SUEZ Systems and access to or use of Confidential Information of SUEZ.

1. MONITORING, REVIEW AND AUDITS:

- 1.1 Vendor shall maintain external monitoring and review requirements in accordance with Section 9 of this Agreement.
- 1.2 Vendor shall permit audits in accordance with Section 8 of the Spreadly Partner GDPR Annex, included as part of this Agreement.
- 1.3 Independent, third-party reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of Vendor's established policies, standards, procedures, and compliance obligations. Third-party security assessments being performed shall include vulnerability scans, penetration tests, policy reviews at least on an annual basis, or more frequently. ASV Scan Report Attestation of Compliance is available at <https://www.spreadly.com/pci>, and updated on a quarterly basis in accordance with PCI DSS Requirement 11.2.2 and the ASV Program Guide.

2. SECURITY

- 2.1 **General.** Vendor will implement and maintain a comprehensive written information security program ("Information Security Program"), which contains appropriate administrative, technical and organizational safeguards that: (a) ensure the security, integrity, availability, resilience and confidentiality of SUEZ Confidential Information; (b) protect SUEZ Confidential Information against Security Incidents (defined below); and (c) meet or exceed industry best practices and requirements under applicable law. Without limiting the generality of this Section 2.1, Vendor will ensure that its Information Security Program meets the requirements of meets the compliance requirements as set forward by PCI-DSS and applicable data protection and privacy laws, including the following obligations:
 - 2.1.1 Vendor shall notify SUEZ of all Service Locations at the time of this Agreement. All SUEZ services will be provided from the U.S.A. Vendor shall provide commercially reasonable written-notice to SUEZ of any new Service Locations.
 - 2.1.2 Maintain separate and distinct development and production databases to ensure that production information is not accidentally altered or destroyed.
 - 2.1.3 Production data may not be used for testing purposes without the prior written approval of the Information Security Department (ISD) of SUEZ. In such cases, where production data must be used to complete development testing, such data must be sanitized to the satisfaction of the SUEZ ISD.
 - 2.1.4 Vendor will maintain, for a period of at least 180 days (or such longer period as may be required by law or contract) detailed log files concerning all activity on Vendor's systems including, without limitation:
 - 2.1.4.1 All sessions established
 - 2.1.4.2 Information related to the reception of specific information from a user or another system
 - 2.1.4.3 Failed user authentication attempts
 - 2.1.4.4 Unauthorized attempts to access resources (software, data, processes, etc.)
 - 2.1.4.5 Administrator actions
 - 2.1.4.6 Events generated (e.g., commands issued) to make changes in security profiles, permission levels, application security configurations, and/or system resources.
 - 2.1.4.7 Vendor must protect all log files against unauthorized access, modification, or deletion.
 - 2.1.5 Vendor shall adhere to the *principle of least privilege* and *need to know* basis principles by limiting personnel working on SUEZ projects or in providing services to SUEZ. Vendor shall restrict access for each system used to provide services under this Agreement to those Vendor staff members with a job-related need to access the system.
 - 2.1.6 Vendor shall cooperate fully (including but not limited to making appropriate personnel, system logs, or other resources available) with SUEZ, its regulators, any law enforcement personnel and any judicial or governmental agency in the investigation of any actual or suspected threat and in any necessary remediation and/or resolution actions.
 - 2.1.7 Vendor will test, on at least a quarterly basis or at the interval established by industry best practice, the implementation of its information security measures through the use of network, system, and application vulnerability scanning tools and/or penetration testing.
 - 2.1.8 If SUEZ requests that Vendor implement or maintain safety and security procedures in addition to those stated herein, Vendor shall implement or maintain such reasonable procedures at Vendor's expense.
 - 2.1.9 Vendor shall bear all costs it incurs in complying with this IS Exhibit.
- 2.2 **Network and Communications Security.** Vendor shall:
 - 2.2.1 Vendor must deploy a defense-in-depth approach to security, relying on layers of security measures to provide a high-level of security confidence. All security monitoring systems including, but not limited to, firewalls and intrusion detection systems must be monitored 24 hours per day, 365 days per year.
 - 2.2.2 Configure its firewalls, network routers, switches, load balancers, name servers, mail servers, and all other network components in a manner that meets or exceeds industry best practices.
 - 2.2.3 Without limiting Section 3 below, if an incident takes place that involves the systems, employees or software used to provide services to SUEZ, Vendor will provide SUEZ, within five days of the closure of the incident, with a written report describing the incident, actions taken during the response, and plans for future actions to prevent a similar incident from occurring in the future.

2.3 Infrastructure Platforms, Services, and Operations Security. Vendor shall:

- 2.3.1 Ensure all infrastructure platforms, authentication mechanisms, and services (operating systems, web servers, database servers, firewalls, routers, etc.) used to provide services under this Agreement are configured and utilized according to industry best practices.
- 2.3.2 Ensure that all remote administrative access to production systems is performed over encrypted connections (i.e., SSH, SCP, SSL-enabled web-management interfaces, and VPN solutions).

2.4 Application Security. Vendor shall:

- 2.4.1 Restrict access to only authenticated and authorized users to view, create, modify, or delete information managed by the application.
- 2.4.2 Require use of strong passwords to access SUEZ applications and systems.
- 2.4.3 Ensure web browser cookies that store SUEZ Confidential Information are encrypted using a public and widely accepted encryption algorithm. This encryption will be performed independently of any transport encryption such as Secure Sockets Layer. All other cookies must be opaque.
- 2.4.4 "Time out" and terminate the session after a reasonable period of user inactivity (not to exceed any mutually agreed upon period of time).
- 2.4.5 Terminate any active sessions interrupted by power failure, system "crash," network problem, or other anomaly, or when the connection is interrupted by the user.
- 2.4.6 Validate all input and output prior to use to avoid data-driven attacks such as "cross-site scripting" and "SQL injection."
- 2.4.7 Vendor agrees to adhere to secure coding standards, including SANS Top 25 Software Errors and OWASP Top 10.

2.5 Data Security. Vendor shall:

- 2.5.1 Transmit all highly confidential SUEZ information via some mechanism other than a Web browser, in accordance with industry best practice.
- 2.5.2 Encrypt all SUEZ Confidential Information in transit and at rest. Vendor shall first request written permission from SUEZ to store SUEZ Confidential Information on any portable or mobile device.

2.6 Physical Security. Vendor, or a third party utilized by the Vendor, shall:

- 2.6.1 Ensure that at each Service Location, to the extent shared environments exist with other businesses or customers for all WANS, LANS, network connections, dial-up connections, DASD or distributed systems, all access to SUEZ Confidential Information is in accordance with any written instructions provided by SUEZ.
- 2.6.2 Maintain all applicable workstations, computers, servers, and network equipment used to provide services under this Agreement ("Equipment") in secure facilities owned, operated, or contracted for by Vendor.
- 2.6.3 Maintain all applicable Equipment in an adequately secured computer room facility and tape library with access restricted to only Vendor staff and subcontractors.
- 2.6.4 Maintain a secure environment using appropriate logical and physical security controls, and continuously monitor access to these secure facilities, through the use of alarm systems, access controls, fire suppression, security guards, surveillance cameras, authorized entry systems, password protection of Equipment, staff egress searches, individual user identifications, or similar methods capable of recording entry and exit information.
- 2.6.5 Maintain all backup and archival media containing SUEZ Confidential Information, or other information used to provide services under this Agreement, in secure, environmentally-controlled storage areas owned, operated, or contracted for by Vendor.
- 2.6.6 Vendor shall: (a) ensure the reliability of personnel, including, to the extent permitted by applicable law, by performing and documenting appropriate background checks and screening (including criminal background checks) before personnel assignment and before access is granted to system or data on behalf of SUEZ; and (b) provide appropriate security training to personnel to ensure such personnel can comply with the obligations under applicable law, data and privacy standards. Vendor shall revoke access in the event of a subsequent criminal violation by personnel. Vendor shall periodically provide additional training to its personnel as may be appropriate to help ensure that Vendor's Information Security Program meets or exceeds industry best practices.
- 2.6.7 Dispose of SUEZ Confidential Information from any system or media no longer in use (or upon request) according to industry best practice. The approved methodology for the cleaning, destruction and sanitization will be dependent on the media used and may include degaussers, multi-pass encrypted wiping software and crosscut shredders. Upon completion of the cleaning, destruction and sanitization of SUEZ Confidential Information, Vendor will, on SUEZ request, provide a certificate of destruction confirming destruction and methods used.

2.7 Malicious Code and Virus Protection

- 2.7.1 Use the latest, at least industry standard, commercially available virus and malicious code detection and protection product(s) on all storage devices, workstations and servers used to provide services under this Agreement. Such products are to be updated on a frequently recurring basis specified by the Vendor's Service Location; and configured in a manner that causes automatic, on-access scanning of the default file types as specified by the antivirus vendor be active, and periodic scanning of system files; antivirus scanning shall not be disabled under any circumstances.
- 2.7.2 Vendor shall: (a) log vulnerability scan reports; (b) conduct periodic reviews of vulnerability scan reports over time; (c) use patch management and software update tools for the Vendor systems; (d) prioritize and remediate vulnerabilities by severity; and (e) use compensating controls if no patch or remediation is immediately available.
- 2.7.3 Vendor will implement best practices for data loss prevention to identify, monitor and protect SUEZ Confidential Information in use, in transit and at rest. Such data loss prevention processes and tools will include: (a) automated tools to identify or prevent attempts of data exfiltration; (b) the prohibition of, or secure and managed use of, portable devices; (c) use of certificate-based security; and (d) secure key management policies and procedures.

2.8 Business Continuity and Recovery. Vendor shall

- 2.8.1 Vendor shall ensure that systems and application architectures are redundant at all levels, including: Datacenter provisions (rack power sources, fiber paths), networking hardware, physical server hardware (power sources, RAM, CPUs, network interfaces, RAID/persistent storage drives), data storage systems and transaction processing systems.
- 2.8.2 Vendor will maintain a detailed, documented plan for responding to a prolonged disruption in services caused by power failure, system failure, natural disaster, or other unforeseen circumstances that includes processes and procedures for resuming operations within a commercially reasonable time for each Service Location ("**DR Plan**").
- 2.8.3 Report any deployment of the DR Plan to SUEZ within a commercially feasible amount of time from activation, and provide regular status updates at four-hour intervals (or at mutually agreed upon times throughout the day) for the duration of the recovery period.
- 2.8.4 Use commercially reasonable methodology, such as DOD or other mutually agreed data wiping standards, to purge and delete SUEZ Confidential Information upon request.

2.9 Laptops/Electronic Devices. Vendor shall:

- 2.9.1 Ensure that all computer terminals, laptops and other electronic devices displaying SUEZ Confidential Information will face away from common areas when possible.
- 2.9.2 While the current plans of Vendor and SUEZ do not anticipate the employment by Vendor of any laptops or other electrical devices connected to the SUEZ network, in the event that Vendor employs laptops, or any other electronic device connected to the SUEZ network, Vendor shall ensure that:
 - 2.9.2.1 no Vendor device shall be connected to a SUEZ network without the prior written consent and certification of the SUEZ Information Security department (as a condition of such certification, MAC and hostname information will be requested to unambiguously identify the device);
 - 2.9.2.2 such devices shall employ an operating system approved by SUEZ; such operating system shall be regularly updated;
 - 2.9.2.3 browsers, if present, will be current versions of software approved by SUEZ (currently Chrome or Microsoft Internet Explorer); such software shall be regularly updated; security settings shall not be lowered from the installed defaults.
- 2.9.3 Use strong encryption to protect all SUEZ Confidential Information. SUEZ may demand the removal from its premises of any Vendor device that does not comply with the foregoing, as well as the user of such device.
- 2.9.4 Vendor shall indemnify SUEZ and hold SUEZ harmless from any and all claims and damages attributable to the use of any Vendor device connected to SUEZ's networks.

3. Security Incident Reporting.

- 3.1 In the event of a conflict between Section 11 of this Agreement and this Section 3 of the IS Exhibit, the requirements of Section 11 of this Agreement shall take precedence.
- 3.2 Vendor shall develop, implement, document and maintain a Security Incident reporting process compliant with applicable law, data and privacy standards (hereinafter a "**SIRP**"). A "**Security Incident**" is:
 - 3.2.1 any breach of Vendor security policies or procedures relevant to this Agreement;
 - 3.2.2 any occurrence of virus or malicious code;
 - 3.2.3 any loss of or attempt to alter or destroy SUEZ Confidential Information;
 - 3.2.4 any actual or attempted (whether or not successful) unauthorized access, disclosure or use of a Service Location or SUEZ Systems or SUEZ Confidential Information.
- 3.3 The SIRP shall:
 - 3.3.1 provide an accurate and up-to-date list of Vendor and SUEZ personnel to be contacted in the event of an actual or suspected Security Incident,
 - 3.3.2 detail incident severity definitions consistent with applicable law, data and privacy standards, and
 - 3.3.3 set specific escalation procedures and timeframes for same based upon the breach severity level of the actual or suspected information Security Incident.
- 3.4 At a minimum, the SIRP must mandate that:
 - 3.4.1 all Vendor personnel notify their management immediately in the event that they become aware of any action which indicates that there has been or may be a Security Incident, and
 - 3.4.2 an officer of SUEZ must be contacted immediately by phone, and promptly thereafter in writing in accordance with Section 11.b of this Agreement.
- 3.5 If Vendor becomes aware of or reasonably suspects a Security Incident, Vendor shall immediately:
 - 3.5.1 notify SUEZ in accordance with the SIRP and cooperate with SUEZ to address and remedy the Security Incident; and
 - 3.5.2 take all steps necessary to remediate the Security Incident and not breach any laws and regulations in so doing; and
 - 3.5.3 make every commercially reasonable effort to allow an independent cyber forensics team to
 - 3.5.3.1 access and inspect the Equipment used by Vendor to provide the Vendor systems or services to SUEZ; and
 - 3.5.3.2 interview those personnel of Vendor who have knowledge of the Vendor systems or services provided to SUEZ to protect the interest of SUEZ or as otherwise permitted or required of SUEZ under applicable law, rule or regulation, and record and retain written or digital copies of such interviews.
 - 3.5.4 keep SUEZ reasonably informed of the progress of remediation activities and provide confirmation when the Security Incident has been fully corrected.
- 3.6 Notice to SUEZ of a Security Incident will include: (a) steps taken or planned to be taken by Vendor to remedy the Security Incident, (a) the nature of the Security Incident; (b) the categories and approximate numbers of any data subjects and Confidential Information records concerned; (c) any third-party investigations into such Security Incident; (d) the likely consequences of the Security Incident; and (e) any other information required by SUEZ to comply with its data breach notification requirements under applicable law. Notification will be via Speedly's public post-mortem.
- 3.7 In the event of a Security Incident, Vendor will be liable for any costs or expenses in accordance with Section 11 of this Agreement. Unless otherwise required by applicable law or regulation, in no event will Vendor serve any notice of or otherwise publicize a Security Incident without the prior written consent of Company.
- 3.8 Vendor shall provide to SUEZ copies of its Operational & Security Addendum for review on execution of the Agreement and each time thereafter such Addendum is updated.

3.9 If Vendor fails to promptly remediate any Security Incident, SUEZ may terminate this Agreement in accordance with Section 4 of this Agreement.

4. PERSONAL DATA.

See Spreadly Partner GDPR Annex in this Agreement.

5. REPRESENTATIONS AND WARRANTIES. Vendor represents and warrants to SUEZ that:

(a) any responses it provides to the Consensus Assessments Initiative Questionnaire (CAIQ v.3.0.1) provided to SUEZ, including any security questionnaire provided before the effective date of the Agreement, is accurate and correct, and Vendor's security measures will meet or exceed all practices described within any such questionnaire;

(b) it has not suffered any security incident that resulted in the loss, damage or unauthorized access, use or disclosure of confidential information (including personal data) of Vendor or any of its customers, or, if it has suffered any such incident, it has disclosed each such incident to SUEZ and taken appropriate measures to rectify such incident;

(c) it is not, and has not been, a party to any current, pending, threatened, or resolved enforcement action of any government or regulatory authority or agency, or any consent decree or settlement with any governmental or regulatory authority or agency or private person or entity regarding any such security incident or otherwise regarding data protection or information security; and

(d) it will not cause SUEZ to be in violation of any applicable data protection laws.

Spreadly Partner GDPR Annex
Compliance with the EU General Data Protection Regulation

Recitals:

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

The European General Data Protection Regulation (GDPR) imposes specific obligations on controllers 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 or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.”
 - (b) “Personal Data” has the meaning given to it in Article 4(1) of the GDPR: “any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person,” but only to the extent such personal data pertains to 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.spreadly.com/gdpr/subprocessors>. Controllers may receive notifications of new Subprocessors by emailing subprocessor@spreadly.com with the subject “Subscribe” and once subscribed in this manner that Controller will receive notification of new Subprocessors before those Subprocessors are authorized to process Personal Data on behalf of the Processor.

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

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 succcess@spreadly.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.

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

Spredly, Inc.

By:

Name:

Title:



Justin Benson

CEO

SUEZ North America, Inc.

By:

Name:

Title:



Digitally signed by Michael Salas
DN: cn=Michael Salas, o=SUEZ, ou=Exec,
email=michael.salas@suez.com, c=US
Date: 2019.04.04 08:48:40 -0400

Michael Salas

SVP, Chief Information Digital Officer