



SERVICE AGREEMENT

Part A: Parties

SPREEDLY

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

CUSTOMER

| | |
|---------------|------------------------------------------------------|
| Name: | Clearpay, S.A.U. |
| Address: | Torre Europa – Paseo de la Castellana 95 – Planta 11 |
| City/Country: | 28.046 Madrid, España |

PRIMARY SPREEDLY CONTACT

| | |
|--------|------------------------------|
| Name: | Watrice Woodridge |
| Title: | Enterprise Account Executive |
| Phone: | |
| Email: | watrice@spreedly.com |

PRIMARY CUSTOMER CONTACT

| | |
|--------|-----------------------------|
| Name: | Shannon Gilham |
| Title: | Senior Partnerships Manager |
| Phone: | +61 431 515 997 |
| Email: | Shannon.gilham@afterpay.com |

SPREEDLY FINANCE CONTACT

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

CUSTOMER BILLING CONTACT

| | |
|--------|----------------------------|
| Name: | Afterpay Touch Accounts |
| Phone: | |
| Email: | accounts@afterpaytouch.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. Spreedly offers the Account Updater program as an optional offering within the Service. If Customer opts-in to the Account Updater program, Customer agrees to pay all applicable fees associated with the Account Updater program and to conform to the specific Account Updater program terms and requirements set forth in **Exhibit D**.

- c. Customer shall comply with all laws, directives, rules and regulations (collectively, "**Laws**") applicable to its use of the Service and Spreadly 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 Spreadly authorization to share information with law enforcement about Customer, Customer's transactions and Customer's Spreadly account, in each case if Spreadly reasonably suspects that Customer's use of the Service has been for an unauthorized, illegal, or criminal purpose.
- d. Spreadly reserves the right to not store or submit any transaction Customer submits that Spreadly believes is in violation of this Agreement or applicable Law, any other Spreadly agreement, or otherwise exposes Customer or other Spreadly 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. Spreadly reserves all rights not expressly granted to Customer in this Agreement. The Service is protected by copyright, trade secret and other intellectual property laws. Spreadly 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 Spreadly products ("**Ideas**"). By submitting any Idea, Customer agrees that its disclosure is gratuitous, unsolicited and without restriction and will not place Spreadly under any fiduciary or other obligation, and that Spreadly 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, Spreadly 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 terminate unless the parties agree in writing to renew for an additional one (1) year period (a "**Renewal Term**" and, together with the Initial Term, the "**Term**"). In order to ensure that Customer will not experience any interruption in the Services, in the event of non-renewal of this Agreement, Customer's account shall revert to a month-to-month subscription plan at the then current pricing and terms (currently found at <https://www.spreadly.com/pricing>) unless Customer provides Spreadly with at least thirty (30) days notice prior to the expiration of this Agreement.
- 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 termination for any reason, Spreadly agrees to provide such support and services as may be reasonably required by Customer in the event Customer seeks to transition some or all of the Services received under this Agreement to a new provider including with respect to, but not by way of limitation, the transfer of tokens.

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. 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 **Error! Reference source not found.**, "**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, Spreadly's "Confidential Information" includes the source code for the Service and the methods, algorithms, structure and logic, technical infrastructure, techniques and processes used by Spreadly 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 **Error! Reference source not found.**; 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 **Error! Reference source not found.**, 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 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. 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, 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 \$30,000,000. 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 Spreadly's material breach of its security obligations set forth in Section 10.
- 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 any of the following: (i) any breach of Section 7 (Confidential Information); and/or (ii) Customer's material breach of its representations and warranties under the Agreement.
- 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. SUBJECT TO SECTION 14.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 14.b, UNDER NO CIRCUMSTANCES SHALL EITHER PARTY'S AGGREGATE LIABILITY TO FOR DIRECT DAMAGES RESULTING FROM EITHER PARTY'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 13 OR BREACHES OF ITS OBLIGATIONS UNDER SECTION 7 (CONFIDENTIAL INFORMATION) EXCEED THE GREATER OF: (i) \$2,000,000 OR (ii) TWO (2) TIMES 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.
- d. NOTWITHSTANDING THE FOREGOING, THE LIMITATIONS AND EXCLUSIONS OF LIABILITY IN SECTIONS 14.a, 14.b, AND 14.c DO NOT APPLY TO THE FRAUDULENT, CRIMINAL OR GROSSLY NEGLIGENT OR MORE CULPABLE ACTS OR OMISSIONS OF A PARTY.

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

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

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

18. Survival. Sections 3.a (Ownership), 4.c (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.

DocuSigned by:
By: Justin Benson
Name: Justin Benson
Title: CEO
Date: 5/26/2021

Clearpay, S.A.U.

DocuSigned by:
By: David Katz
Name: David Katz
Title: Chief Product Officer
Date: 5/25/2021

EXHIBIT A**PRICING**

The initial term of this agreement is 12 months. Customer shall pay Spreadly 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 |
| Enterprise Platform Fee: | \$200,000 |
| Enterprise Assurance Agreement & SLAs | Included |
| Existing Spreadly Endpoints | Unlimited |
| PCI Compliant Card Storage Limit | Unlimited |
| Add New Standard PMD Endpoints | Included |
| API Usage Fee: | \$150,000 |
| Included API Calls | 150,000,000 |
| Cost per API Call | \$0.0010 |
| Total Base Annual Fee | \$350,000 |

The API Usage Fee in the table above includes an initial allotment of 150,000,000 API calls.

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 the contract rate of \$0.0010 per API call for the remainder of the contract term.

Customer may also or instead elect to purchase additional blocks of 10,000,000 API calls at the contract rate of \$0.0010 per API call 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

The above pricing is contingent on contract execution on or before May 28, 2021.

Enterprise Account Management

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

Payment Terms

Base Annual Fee. Customer will pay the Base Annual Fee for the Initial Term, and each Renewal Term, quarterly, with each payment equal to 25% of the Base Annual Fee for the then-current Contract Year. The first payment of \$87,500.00 is due and payable in full within 30 days of the Effective Date. Each subsequent quarterly payment shall be invoiced prior to the next quarterly billing date, and shall be due and payable in full within 30 days.

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 Spreadly is legally obligated to collect applicable taxes, such taxes shall be invoiced to and paid by Customer, unless Customer provides Spreadly 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 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.

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
 Spreadly, 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 99.95%, 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. For the purposes of this definition, the Transaction Processing Service will be deemed unavailable if the the average API response time is greater than three seconds based on the global server-side response time threshold excluding delays resulting from third-party connections (e.g. downstream gateways).
- 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 99.99% but greater than or equal to 99.95% | 5% of 1/12 th of Base Annual Fee |
| Less than 99.95% but greater than or equal to 99.90% | 10% of 1/12 th of Base Annual Fee |
| Less than 99.90% but greater than or equal to 99.80% | 15% of 1/12 th of Base Annual Fee |
| Less than 99.80% | 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.

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**ACCOUNT UPDATER SERVICE REQUIREMENTS**

If Customer elects to participate in to Spreedly's Account Updater program, Customer agrees to conform to the following requirements:

1. Merchant Qualification

- Merchants designated by Visa as high-risk (High-Risk Acquirer Program with a condition of RED or higher) or on the MasterCard Alert to Control High-risk Merchants (MATCH) system may not participate in Account Updater.
- Third-party payment portfolios must not contain more than 20 percent High-Risk Merchant activity.
- Merchant must not be under any special conditions imposed by Visa Corporate Risk Management.
- Merchants must have been in business a minimum of six months.
- Over the course of six months, the merchant must have at least 1,000 transactions a month or an average of 5,000 transactions over three months.
- The merchant must maintain a chargeback ratio of less than 3 percent.
- Merchants must meet the following risk management criteria:
 - Must not be engaged in business categorized by the following merchant category codes: 5962, 5966, 5967, or 7995.
 - Must not have sales transactions that are predominantly Quasi-Cash, Account Funding, or any combination thereof.

2. Customer Responsibilities. Customer must:

- Protect the security of the information sent to or received from Account Updater.
- Use the same standard of care to protect and prevent misappropriation or improper disclosure of the confidential information as is used to protect its own confidential information, but in no event less than reasonable care.
- Be in compliance with the network operating regulations.
- Have a valid business need to receive updated account information, including but not limited to:
 - Subscription services
 - Express checkout services
 - Membership (club) services
 - Recurring payment services
- Restrict access to Account Updater data to business need-to-know.
- Request an Account Update for every participating cardholder account in merchant's customer database at least once every 180 calendar days for merchants that bill daily, weekly, monthly, quarterly or bi-annually or at least once every 365 calendar days for merchants that bill annually.
- Submit inquiries only for those customer accounts with which Customer has existing customer relationships and have their account information on file.
- Ensure that information received from Account Updater is properly, completely, and accurately incorporated

3. Prohibited Activities. Customer must not:

- Request authorization on accounts that have returned a response of "Closed Account".
- Submit inquiries to Account Updater on behalf of any other entity.

If Customer has fraudulently misused Account Updater to obtain account updates, Customer will be removed from the Account Updater service.

4. Indemnification. Customer agrees to indemnify and hold Spreedly and its respective directors, officers, agents, and employees, harmless against any and all liability, costs, damages, and actions arising in connection with (a) Customer's use of Account Updater, confidential information, and/or any associated written materials, and/or (b) any breach of its obligations as stated herein. Customer acknowledges and agrees with the following:

- Account Updater contains confidential information of Spreedly and others that has been disclosed to the merchant or to which the merchant has been provided access.
- The merchant will not misappropriate confidential information of Spreedly.
- Account Updater contains Personal Data disclosed to Spreedly by Customer.

Customer acknowledges and agrees that any and all Confidential Transaction Data (as defined in the Card Network rules) or other Personal Data that Customer provides to the Card Networks in connection with use of Account Updater may be used by them for the purposes described in their respective rules and for purposes of providing the program and other services as requested by Customer. For purposes of clarity, Customer represents and warrants that it will be solely responsible for providing notice to and obtaining any necessary consent from cardholders in connection with the processing of Personal Data by the Card Networks for the above purposes. Customer also represents and warrants that it will be solely responsible for handling requests from cardholders to access, correct, block or delete their Personal Data in connection with the Account Updater.

5. Disclaimer. SPREEDLY DOES NOT REPRESENT OR WARRANT THAT ACCOUNT UPDATER IS FREE OF DEFECT AND/OR MISTAKE; AND IS PROVIDED ON AN "AS IS" BASIS, "WITH ALL FAULTS". SPREEDLY AND ITS ACCOUNT UPDATER COMPONENT SUPPLIERS DISCLAIM ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO: ACCOUNT UPDATER, CONFIDENTIAL INFORMATION AND/OR ANY ASSOCIATED WRITTEN MATERIALS; THEIR USABILITY, CONDITION, OR OPERATION; THEIR MERCHANTABILITY; THEIR FITNESS FOR ANY PARTICULAR PURPOSE; OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS. IN NO EVENT WILL SPREEDLY BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF INCOME, USE, OR INFORMATION, NOR ANY OTHER COST OR EXPENSE INCURRED BY A MERCHANT OR ANY THIRD PARTY ARISING FROM OR RELATED TO USE OR RECEIPT OF ACCOUNT UPDATER, WHETHER IN AN ACTION IN CONTRACT OR IN TORT, AND EVEN IF THE MERCHANT OR THIRD PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EACH MERCHANT ASSUMES THE ENTIRE RISK OF USE OR RECEIPT OF THE PROGRAM OR CONFIDENTIAL INFORMATION.

Only in the event the limitation of liability set forth in the immediately preceding paragraph is deemed by a court of competent jurisdiction to be contrary to applicable law, the total liability, in the aggregate, of Spreadly to Customer and anyone claiming by or through the Customer, for any claims, losses, costs, or damages, including attorneys' fees and costs and expert-witness fees and costs of any nature whatsoever or claims expenses resulting from or in any way related to Account Updater shall not exceed the total compensation received by Spreadly from the Customer for the use of Account Updater during the six months ending on the date that Spreadly was advised by the Customer of the Account Updater concern. It is intended that this limitation apply to any and all liability or cause of action however alleged or arising, to the fullest extent permitted by law, unless otherwise prohibited by law.

EXHIBIT E**Data Privacy Addendum and
Spredly Partner GDPR Annex****Compliance with the EU General Data Protection Regulation****Recitals:**

Spredly, 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.spredly.com/gdpr/subprocessors>. Controllers may receive notifications of new Subprocessors by emailing subprocessor@spredly.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.

Schedule 1 - Description of Processing of Personal Data to Facilitate Clearpay' Services

1 Description of the processing activities

Processing in connection with the provision of the Services.

2 Data subjects.

- (a) Customers and Website end-users.

3 Agreed purpose

The processing is necessary for the following.

- (a) To provide (or assess whether to provide) Clearpay services.
- (b) For customer / merchant support.
- (c) To process transactions and send notices about Data Subjects transactions.
- (d) To resolve Data Subjects disputes, collect fees, and troubleshoot problems.
- (e) To investigate and prevent Data Subjects potentially prohibited or illegal activities.
- (f) To enforce our rights against Data Subjects (debt recovery).

4 Categories of data

The Personal Data processed fall within the following categories.

- (a) Name, surnames, phone number, email address, business and residential address, location (country, city, state, billing / shipping address, mobile phone locator),
- (b) Bank account details; credit or debit card numbers.

5 Data Controller's specific instructions with regards to the processing of Personal Data:

Personal data is to be processed by the Processor(s) only for the purposes set out in this Schedule 1.

Schedule 2 – Security Measures Description

This document contains the technical and organizational security measures to be implemented by the Data Processor in the fulfilment of the Services that has agreed to provide by virtue of the Agreement.

1 Logical access control to systems that process Personal Data

At a minimum, the following security measures should be implemented where commercially reasonable:

(a) **Access control:**

- (i) Access to the systems after authentication of authorized personnel.
- (ii) Existence of an updated list of users with authorized access to the information systems.
- (iii) Access control based on roles and profiles, implemented in a manner consistent with the principle of least privilege, i.e., that users only access information that is essential to carry out their assigned functions.
- (iv) Prohibition of the use of anonymous or generic accounts, except in justified and limited situations.
- (v) Implementation of an access management system. Access administration should be centralized, and authorization for access should only be granted by authorized personnel, who alone can grant, alter or cancel access to the systems.
- (vi) In the event that external personnel have access to the resources, they shall be subject to the same security conditions and obligations as the company's own personnel.

(b) **Identification and authentication:**

- (i) Use of passwords with minimum security parameters (uppercase, lowercase, numbers, letters and special characters, minimum number of 6 characters, and expiration once a year), and keeping them unintelligible.
- (ii) Use of a procedure for assigning, distributing and storing passwords that guarantees their confidentiality and integrity.
- (iii) Automatic locking of the user's device after a period of inactivity. Identification and password required to restart its use.

(c) **Device management:**

- (i) Identification and inventory of the devices that process Personal Data, as well as the users that access them.
- (ii) Adoption of measures aimed at preventing subsequent access or recovery of the information contained in the devices once it is decided to dispose of them. To this end, they must be destroyed or erased by means of secure erasure systems. Devices containing personal data must be physically destroyed or, alternatively, the information stored in them must be destroyed, erased or overwritten using techniques that make it impossible to recover the original information, instead of using normal erasure or formatting.
- (iii) The distribution of devices containing personal data that pose a high risk to the rights and freedoms of data subjects shall be carried out after encrypting such data or using any other mechanism that ensures that such information is not accessible or manipulated during transport.

(d) **Backup and service availability.**

- (i) Documentation of the backup and recovery procedures, which always guarantee their reconstruction in the state in which they were at the time of the loss or destruction.
- (ii) Periodic backups, at least weekly, unless there has been no update of the data during that period.
- (iii) Periodic verification of the correct definition, operation, and application of the procedures for data backup and recovery.
- (iv) Ensure that systems are operational and that failures are properly reported. Accurate and complete records of backups performed should be retained.
- (v) Verification, at least every six months, of the correct definition, operation and application of the procedures for data backup and recovery.
- (vi) The backups should be stored in a remote location, at a sufficient distance to be spared from any damage that may be consequence of a disaster at the main site.

- (vii) The controls applied to the media at the main site should be extended to the location of the backup copies.
- (e) **Development tests**
 - (i) Users should use different profiles for production and test systems, and it is recommended that menus display appropriate identification messages to reduce the risk of error.
 - (ii) No pre-implementation testing or modification of information systems with Personal Data shall be performed with real data. Dissociated data shall be used.
 - (iii) If this is necessary, the same security measures must be implemented as in the production environment, and a backup copy must have been made beforehand.
 - (iv) Segregation of IT test and production environments.
- (f) **Network security controls**
 - (i) Use of firewall, router and VPN-based access controls to protect private service networks and back-end servers.
 - (ii) Infrastructure security with ad-hoc monitoring.
 - (iii) Regular review of security risks by internal employees and external auditors.
 - (iv) Logging access to host servers, applications, databases, routers, switches, etc.
 - (v) The transmission of personal data through public or wireless electronic communications networks shall be carried out under secure protocols.
 - (vi) Sensitive personal data will be encrypted during transmission using security protocols by means of strong algorithms and encryption keys.
 - (vii) Limited existence of system administrators.
 - (viii) Setting up of mechanisms for recording actions on personal data or logging as well as reliable and flexible tools for the use of the resulting audit files.
 - (ix) Setting up of user code assignment policies by the organization that avoid simple data such as date of birth, first and last name, etc.

2 Physical access control to work centers and Personal Data processing areas.

At least one of the following security measures shall be implemented to prevent physical access to work centers and data processing centers:

- (a) Access control system.
- (b) Identity reader, magnetic card or chip card.
- (c) Provision of keys.
- (d) Door lock (automatic doors, etc.).
- (e) Alarm system, video and video surveillance monitors.
- (f) Registration of entrances and exits of the facilities.
- (g) Location of data centers in secure facilities that provide physical security, redundant power, and infrastructure redundancy.

3 Incident log

At a minimum, the following security measures should be implemented:

- (a) Procedure for notification and management of incidents affecting personal data.
- (b) Procedure for notification and management of security breaches, and their notification in due time and form to the Data Controller, in order to comply with the requirements of the regulations.
- (c) Maintenance of a record of incidents/breaches.

4 Training, functions, and duties.

At a minimum, the following security measures should be implemented:

- (a) The roles and duties of each of the persons with access to data and information systems must be documented and must be known by those involved.
- (b) The communication of these functions and responsibilities should be auditable and should include the penalties for non-compliance.
- (c) Training actions shall be carried out for employees and other persons with access to data, to ensure proper data processing in accordance with the requirements of the regulations.

5 Security measures for non-automated processing.

At a minimum, the following security measures should be implemented:

- (a) The archiving of documents should be carried out according to criteria that facilitate their consultation and location to guarantee the exercise of the rights of the interested parties.
- (b) Storage devices must be provided with mechanisms to prevent their opening.
- (c) Establish a clean desk policy in order to minimize the chances of unauthorized access to personal data.
- (d) During the review or processing of documents, the person in charge of them must be diligent and guard them to prevent unauthorized access.

6 Periodic verification of controls.

A process of regular verification, evaluation and assessment of the effectiveness of technical and organizational measures to ensure the security of the processing must be established, taking into account in particular the risks presented by the processing of the data.

Schedule 3 – Standard Contractual Clauses

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

Name of the data exporting organisation: Clearpay, S.A.U.

Address: Paseo de la Castellana 95, Torre Europa, Planta 11ª, 28.046 – Madrid (España)

Tel: n/a

Fax: n/a

Email: dpo@pagantis.com

(the data exporter)

Name of the data importing organisation: Spreedly, Inc.

Address: 300 Morris Street, Suite 400, Durham NC 27701

Tel: +1(888)727-7750

Fax: n/a

Email: security@spreedly.com

(the data importer)

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in 0.

1 Definitions

For the purposes of the Clauses:

- (a) **personal data, special categories of data, process/processing, controller, processor, data subject and supervisory authority** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) **the data exporter** means the controller who transfers the personal data;
- (c) **the data importer** means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) **the sub-processor** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) **the applicable data protection law** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) **technical and organisational security measures** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2 Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in 0 which forms an integral part of the Clauses.

3 Third-party beneficiary clause

- 3.1 The data subject can enforce against the data exporter this clause 3, clause 4(b) to clause 4(i), clause 5(a) to clause 5(e) and clause 5(g) to clause 5(j), clause 6.1 and clause 6.2, clause 7, clause 8.2 and clause 9 to clause 12 as third-party beneficiary.
- 3.2 The data subject can enforce against the data importer this clause 3.2, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2 and clause 9 to clause 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
- 3.3 The data subject can enforce against the sub-processor this clause 3.3, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2, and clause 9 to clause 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- 3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4 Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in **Error! Reference source not found.** to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any sub-processor pursuant to clause 5(b) and clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of **Error! Reference source not found.** and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

- (i) that, in the event of sub-processing, the processing activity is carried out in accordance with clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under the Clauses; and
- (j) that it will ensure compliance with clause 4(a) to clause 4(i).

5 Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in **Error! Reference source not found.** before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - (ii) any accidental or unauthorised access; and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of **Error! Reference source not found.** which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with clause 11; and
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6 Liability

- 6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in clause 3 or in clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
- 6.2 If a data subject is not able to bring a claim for compensation in accordance with clause 6.1 against the data exporter, arising out of a breach by the data importer or its sub-processor of any of their obligations referred to in clause 3 or in clause

11 because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

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

- 6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in clauses 6.1 and 6.2, arising out of a breach by the sub-processor of any of their obligations referred to in clause 3 or in clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7 Mediation and jurisdiction

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

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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

8 Cooperation with supervisory authorities

- 8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
- 8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
- 8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to clause 8.2. In such a case the data exporter shall be entitled to take the measures foreseen in clause 5(b).

9 Governing law

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

10 Variation of the contract

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

11 Sub-processing

- 11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
- 11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in clause 6.1 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in clause 11.1 shall be governed by the law of the Member State in which the data exporter is established.

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

12 Obligation after the termination of personal data processing services

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

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in clause 12.1.

On behalf of the data exporter

Name: David Katz

Position: Chief Product Officer

Address: c/o Torre Europa, Paseo de la Castellana, 95, Planta 11, 28046, Madrid

Signature

DocuSigned by:

FE141A12B71C486...

On behalf of the data importer

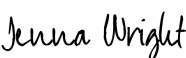
Name (written out in full) Jenna Hutt

Position Privacy Officer

Address 300 Morris Street, Suite 400, Durham NC 27701

Other information necessary in order for the contract to be binding (if any)

Signature

DocuSigned by:

302212D92EB44AD...

Annex A to the Standard Contractual Clauses

This Annex forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this 0.

Data exporter

The data exporter is (please specify briefly our activities relevant to transfer):

As detailed in Schedule 1 of the Exhibit E

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):

As detailed in Schedule 1 of the Exhibit E

Data subjects

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

As detailed in Schedule 1 of the Exhibit E

Categories of data

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

As detailed in Schedule 1 of the Exhibit E

Special categories of data (if appropriate)

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

As detailed in Schedule 1 of the Exhibit E

Processing operations

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

As detailed in Schedule 1 of the Exhibit E

DATA EXPORTER

Name: **Clearpay, S.A.U.**

Authorised signature:


DocuSigned by:

FE141A12B71C486...

DATA IMPORTER

Name: **Spreedly, Inc.**

Authorised signature:

DocuSigned by:

302212D92EB44AD...

Annex B to the Standard Contractual Clauses

This Annex forms part of the Clauses and must be completed and signed by the parties.

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

As detailed by the Data Importer in the Schedule 2 of the Exhibit E.