



**SHORT FORM SERVICES AGREEMENT
CONTRACT NO.**

CW192660

Between

BP International Limited

And

Spreedly, Inc.

Table of Contents

Contents	Page
1 Definitions and Interpretation	4
2 Term, Structure and Precedence	6
3 Scope of Services	7
4 Supplier Personnel Provisions and Use of Subcontractors	7
5 Customer Policies	9
6 Information Security	9
7 Regulatory Compliance and Anti-Corruption Undertakings	11
8 Taxes	12
9 Charges, Invoicing and Payment.....	13
10 Record Retention and Audit Rights.....	14
11 Intellectual Property Rights.....	15
12 Warranties and Representations	15
13 Insurance	16
14 Liability	17
15 Force Majeure.....	18
16 Confidentiality	18
17 Publicity and Public Announcements	19
18 Data Protection.....	20
19 Termination of the Global Agreement	21
20 Termination of the Release Order.....	21
21 Consequences of Termination.....	22
22 Exit Management Assistance.....	22
23 Third Party Rights	22
24 Notices	22
25 Miscellaneous.....	23
26 Dispute Escalation	23
27 Governing Law, Jurisdiction and Dispute Resolution	24

Schedule 1 Template Release Order.....26

Schedule 2 Service Description31

Schedule 3 Pricing and Financial Provisions39

Schedule 4 Policies.....41

Schedule 5 Special Conditions63

This Short Form Services Agreement (the “**Global Agreement**”) is effective as of June 1st 2021 (the “**Effective Date**”) between:

- (1) **BP INTERNATIONAL LIMITED**, a company incorporated in England and Wales (registered no. 00542515) having its registered office at Chertsey Road, Sunbury on Thames, Middlesex, TW16 7BP, United Kingdom (the “**Global Customer**”);
- (2) **Spredly, Inc.**, a company incorporated in the State of Delaware having its principal office at 300 Morris Street, Suite 400, Durham, North Carolina, USA 27701, (the “**Global Supplier**”)

Global Customer and Global Supplier may be referred to individually as a “**Party**” and collectively as the “**Parties**”.

Background:

The Global Customer and the Global Supplier have agreed to put in place the Global Agreement which creates a contractual framework for the supply of services relating to secure payment method storage and transaction proxying-services on the terms set out in this Global Agreement.

Now it is hereby agreed as follows:

1 Definitions and Interpretation

- 1.1** As used in the Global Agreement and any Release Orders the following terms and expressions have the meanings set out below:

“**Affiliate**” means:

- (a) with respect to the Applicable Customer: (i) BP p.l.c.; (ii) any legal entity directly or indirectly Controlled by BP p.l.c.; (iii) a firm, undertaking, joint venture, association, partnership, or other form of business organisation in or through which an entity referred to in (ii) above directly or indirectly operates or manages on behalf of itself and/or one or more third parties and in which it directly or indirectly has an ownership, production sharing, or other economic interest;
- (b) with respect to the Applicable Supplier: any legal entity directly or indirectly Controlled by its parent or ultimate holding company;

“**Applicable Customer**” means Global Customer when referring to the Global Agreement and the Customer (as defined in clause 2.5.1) when referring to a Release Order;

“**Applicable Supplier**” means Global Supplier when referring to the Global Agreement and the Supplier (as defined in clause 2.5.2) when referring to a Release Order;

“**AP System**” means any Applicable Customer’s (or its Affiliate’s) automated procurement system(s) as designated by the Applicable Customer (or its Affiliate);

“**Charges**” means the charges to be paid by the Applicable Customer or an Affiliate nominated by it for the relevant Services as set out in, or as calculated in accordance with Schedule 3 (Pricing and Financial Provisions) to the Global Agreement or Attachment 2 (Pricing and Financial Provisions) to the Release Order as appropriate;

“**Claims**” means all claims, suits, actions, damages, settlements, losses, liabilities and costs, including reasonable attorneys’ fees, incurred by the Customer Indemnified Parties;

“**Confidential Information**” means any and all information in the broadest sense in whatever form or medium (including but not limited to documentary, electronic or oral information) which is disclosed by or relates to either Party and is received or obtained by the other Party including Personal Data and any other information about its business affairs. The term “**Confidential Information**” shall include information of the

Applicable Customer's Affiliates and any third party information disclosed by the Applicable Customer to the Applicable Supplier;

"Control" means in relation to an organisation the power of a person to secure that the affairs of the relevant organisation are conducted in accordance with the wishes of that person, and **"Controlled"** shall be construed accordingly;

"Customer Data" means data or records of whatever nature and in whatever form relating to the business, clients, employees, operations or otherwise relating to the business of the Customer and/or any Affiliate of the Global Customer, whether subsisting before the Release Order Effective Date or as created or processed as part of, or in connection with, the Services;

"Customer Indemnified Parties" means the Applicable Customer, its Affiliates and the officers, directors, agents, employees and assigns of each;

"General Terms" means all of the clauses of the Global Agreement;

"Gross Negligence" means a degree of lack of care that exhibits a reckless or wilful disregard or indifference to consequences, being distinct from and more fundamental than failure to exercise proper care and skill;

"Industry Best Practice" means the exercise of that degree of skill, care, diligence, prudence, foresight and judgement which would reasonably be expected from skilled, experienced and market leading operators engaged in the provision of services similar to the Services;

"Initial Term" means for the purposes of the Global Agreement a period of 3 years from the Effective Date;

"Insolvency Event" means the event which occurs if a Party becomes unable to pay its debts as they fall due, enters into liquidation (except for the purposes of a solvent reorganisation), makes or proposes an arrangement with its creditors, becomes subject to an administration order or a receiver, trustee in bankruptcy, administrative receiver or the like is appointed over all or any of its assets or takes or suffers to be taken any similar action in consequence of a debt, ceases or threatens to cease trading or is dissolved, or any other equivalent procedure in any other jurisdiction with respect to that Party (including proceedings under Chapter 11 or 13 of the US Bankruptcy Code);

"Intellectual Property Rights" means rights, title and interests in materials, patents, trade marks, service marks, design rights, moral rights, domain names, trade or business names (whether registrable or otherwise), applications for any of the foregoing, copyright, databases, know-how, processes, trade secrets and other similar rights or obligations whether registrable or not (and which may subsist now or in the future) in any country or in any trans-border system of registration;

"Personal Data" means any information relating to an identified or identifiable natural person that is processed by the Supplier as a result of, or in connection with, the provision of the Services;

"Release Order" means the contract formed by an executed release order in the form of the Template Release Order (or, where an order is placed through the AP System, in a form that contains substantially the same information) and which refers to the Global Agreement;

"Release Order Effective Date" has the meaning set out in the Release Order;

"Service Commencement Date" has the meaning set out in the relevant Release Order;

"Service Levels" means the service levels (if any) identified as such in the Release Order;

"Services" means in relation to the Global Agreement any or all of the services as described in Schedule 2 (*Service Description*) and in relation to any Release Order as may be referred to or set out in Attachment 1 (*Service Description*) thereto;

“Supplier Personnel” means the personnel (including permanent and temporary employees, agents and contractors) used by or on behalf of the Applicable Supplier or its Affiliates to provide Services or otherwise fulfil the Applicable Supplier’s obligations;

“Template Release Order” means the template release order set out in Schedule 1 (Template Release Order); and

“Term” means the Initial Term and any term extension either pursuant to clause 2.1 or otherwise agreed to by the Parties in writing.

- 1.2** The Global Agreement and any Release Orders shall be interpreted in accordance with the following provisions: (i) the words **“include”** and **“including”** are to be construed without limitation and unless otherwise expressly stated; (ii) the words **“writing”** and **“written”** mean in documented form, whether electronic or hard copy, unless otherwise stated; and (iii) references to any laws shall include that law as amended from time to time.

2 Term, Structure and Precedence

- 2.1** The Global Agreement shall commence on the Effective Date and shall continue for the Term unless terminated in accordance with its terms. The Applicable Customer may at any time prior to expiry of the Initial Term extend the Global Agreement by up to one (1) year by serving notice in writing on the Global Supplier.
- 2.2** If there is any conflict or ambiguity between any of the sections of the Global Agreement, the sections shall be applied in the following order of precedence: Schedule 5 (*Special Conditions*); then the General Terms; then the remaining Schedules; and then any other document referred to in the Global Agreement.
- 2.3** If the Global Customer or any of its Affiliates requires the Global Supplier or any of its Affiliates to provide any Services, the Global Supplier shall procure that the relevant Supplier Affiliate shall complete and execute a Release Order. The Global Supplier shall procure that each of its Affiliates which enters into a Release Order shall comply with its obligations under the relevant Release Order.
- 2.4** The General Terms other than clauses 2.1, 2.2, 2.3 and 19 (*Termination of the Global Agreement*) and Schedules 4 (*Policies*) and 5 (*Special Conditions*), as amended at any time and from time to time, shall be incorporated into and shall form part of the Release Orders entered into pursuant to clause 2.3 above, and shall be read as one with such Release Orders, subject to any agreed changes as set out in Attachment 3 (*Special Conditions*) to the relevant Release Order.
- 2.5** Each Release Order shall constitute and be constructed as a separate agreement. For the purpose of interpreting and construing the Release Order only:
- 2.5.1** references to the **“Customer”** shall mean the Global Customer or its Affiliate which executed the relevant Release Order;
- 2.5.2** references to the **“Supplier”** shall mean the Global Supplier or its Affiliate which executed the relevant Release Order including all assigned Supplier Personnel;
- 2.5.3** references to a **“Party”** shall individually refer to the Customer and Supplier which executed the relevant Release Order and **“Parties”** shall be construed accordingly;
- 2.5.4** references to the **“Services”** shall be to the Services as set out or referred to in Attachment 1 (Service Description) to the relevant Release Order;

- 2.5.5 references to the “**Term**” shall be to the Term as referenced in the relevant Release Order;
 - 2.5.6 references to the “**Charges**” shall be to the Charges as set out or referred to in Attachment 2 (Pricing and Financial Provisions) to the relevant Release Order; and
 - 2.5.7 any terms and conditions in the General Terms or the incorporated Schedules which within their meaning are applicable only to the Global Agreement or the Global Customer or Global Supplier (in their capacity as Parties to the Global Agreement) shall not apply.
- 2.6 If any provision contained in these General Terms or the incorporated Schedules is expressly varied for a Release Order, such varied terms shall apply to that Release Order only and shall not apply to other Release Orders or the Global Agreement. In interpreting Release Orders, if there is any conflict or ambiguity between any of the sections of the Release Order, the sections shall be applied in the following order of precedence: Attachment 3 (*Special Conditions*) to the Release Order; then Schedule 5 (*Special Conditions*) to the Global Agreement; then the General Terms; then the completed Release Order and Attachments 1 (*Service Description*) and 2 (*Pricing and Financial Provisions*) to the Release Order; then the remaining Schedules; and then any other document referred to in the Release Order.
- 2.7 For the purposes of the Global Agreement and the Release Orders: “**execute**” shall mean either written signature or electronic execution through the AP System or any Customer designated e-signature system. The Global Supplier shall, when required by the Applicable Customer, procure that its Affiliates use the AP System in accordance with any AP System processes, guidance, documentation and training provided. Where the AP System refers to “**Orders**” (or anything analogous to an Order), for the purposes of the Global Agreement, Orders shall mean Release Order.
- 2.8 The Global Customer shall not be liable for the actions or omissions of its Affiliates under any Release Order.
- 2.9 The Global Agreement does not create any financial commitments from the Global Customer or its Affiliates to the Global Supplier or its Affiliates and unless specifically stated otherwise therein nothing in any Release Order shall be construed as requiring the Applicable Customer to order any particular volume of Services or that the Applicable Supplier is engaged on an exclusive basis.

3 Scope of Services

- 3.1 From the relevant Service Commencement Date, the Supplier shall provide the Services and meet any applicable Service Levels in each case in accordance with the terms of the applicable Release Order. In addition to the Services, and except where specifically stated otherwise in a Release Order, the Applicable Supplier shall, at its cost, provide all activities, functions, responsibilities and obligations for the proper provision of, ancillary to or customarily included as part of the Services.
- 3.2 The Services and any deliverables provided under a Release Order may be subject to acceptance by the Customer pursuant to any acceptance process and acceptance criteria set out in or referred to in the Release Order.

4 Supplier Personnel Provisions and Use of Subcontractors

- 4.1 The Supplier shall ensure, to the extent that it is within its reasonable control, that any key personnel (who may be identified as such in a Release Order) are, and remain actively involved

in, supplying and performing the Services. The Supplier shall ensure that any replacements are properly briefed and all appropriate handover and training is provided at no additional cost to the Customer.

- 4.2** Upon the Customer's request, the Supplier shall remove or replace Supplier Personnel (i) immediately in the case of misconduct or security risk or (ii) upon five (5) working days prior written notice in all other cases. The Supplier will ensure that an adequate handover of responsibilities takes place.
- 4.3** Supplier Personnel shall not be entitled to participate in any of Customer's employee benefits. Supplier shall be responsible for all employer obligations towards all of its employees and agents under any and all applicable laws.
- 4.4** The Applicable Supplier shall not, without the Applicable Customer's prior written consent, subcontract or delegate any of its rights or obligations under the Global Agreement or any Release Orders. The Applicable Supplier shall ensure that Supplier Personnel and its subcontractors fully comply with the terms and conditions of the Global Agreement or any Release Orders and the Applicable Supplier shall remain fully liable for all acts and omissions thereof.
- 4.5** The Supplier shall indemnify and hold harmless the Customer Indemnified Parties against all Claims arising from or relating to any employment allegations or employment claims brought against the Customer Indemnified Parties by any of the Supplier Personnel.
- 4.6** The Applicable Supplier undertakes and warrants to the Applicable Customer that, in relation to Supplier Personnel, it will, prior to involvement in providing any of the Services or access to BP information or systems (whichever is the earlier):
 - 4.6.1** carry out such vetting checks as may be consistent with Industry Best Practice, except to the extent prohibited by Applicable Law, and that such checks shall include but not be limited to the verification of identity; right to work; employment and education history for Seven (7) years; relevant qualifications; criminal record check; and checks against recognised counter-terrorism databases including, the 'Interpol's Most Wanted List' and the 'FBI Most Wanted Terrorists List';
 - 4.6.2** conduct at no cost to the Applicable Customer such additional vetting as may be required (i) by the laws of the jurisdiction in which the relevant Services are to be provided; (ii) the local policies or procedures adopted by the Affiliates of the Applicable Customer which are receiving the benefit of the Services and (iii) by the Applicable Customer acting reasonably; and
 - 4.6.3** upon request provide written details to the Applicable Customer of the steps it has taken pursuant to clause 4.6.1 above.
- 4.7** Neither the Global Agreement nor any Release Order creates an employer/employee relationship, a partnership or agency of any kind, an association or trust between the applicable Parties, each Party being individually responsible only for its obligations as set out in the Global Agreement or relevant Release Order and the Parties agree that their relationship is one of independent contractors.
- 4.8** **Unless exempt, Applicable Supplier and its subcontractors shall abide by the requirements of 41 CFR §§ 60-1.4(a) (for women and minorities), 60-300.5(a) (for protected veterans) and 60-741.5(a) (for individuals with disabilities). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, sex, or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and**

advance in employment individuals without regard to race, color, religion, sex, national origin, protected veteran status or disability. In addition, if applicable, the provisions of 41 CFR § 61-300.10 (veterans' employment reports) and provisions of 29 CFR Part 471, Appendix A to Subpart A (posting notice of employee rights) are incorporated by reference as terms and conditions herein and are binding on Applicable Supplier and its subcontractors.

5 Customer Policies

- 5.1** Without limiting any of the Applicable Supplier's other obligations the Applicable Supplier shall, and shall procure that the Supplier Personnel shall, at all times in performing their obligations under the Global Agreement and each applicable Release Order:
- 5.1.1** act consistently with the applicable principles of the Customer's Code of Conduct set out at www.bp.com, as amended from time to time;
- 5.1.2** conduct its business in a manner that respects the rights and dignity of all people and internationally recognized human rights and act consistently with the applicable principles of Customer's Business and Human Rights policy set out at www.bp.com, as amended from time to time, including without limitation:
- (i) not employing, engaging or otherwise using forced labour, trafficked labour or exploitative child labour; nor engaging in or condoning abusive or inhumane treatment of workers;
 - (ii) providing equal opportunities, avoiding discrimination and respecting freedom of association of workers, in each case within the relevant national legal framework; and
 - (iii) mitigating or avoiding adverse human rights impacts to communities arising from Applicable Supplier's activities to the extent practicable.
- 5.2** The Applicable Supplier shall, and shall ensure the Supplier Personnel shall, in relation to all aspects of health, safety, security and environmental management, observe and comply with the Applicable Customer's relevant health, safety, security and environmental management policies in force from time to time. If the Applicable Customer reasonably believes that the Applicable Supplier is failing to comply with this obligation then, in addition to its other rights and remedies herein, at law or in equity, it may require the Applicable Supplier to review such non-compliance and to explain what steps it plans to take in order to remedy the non-compliance.

6 Information Security

- 6.1** The Applicable Supplier shall implement and maintain appropriate:
- 6.1.1** technical and organisational measures; and
- 6.1.2** adequate security programmes and procedures,
- to ensure a level of security appropriate to the risk, and to prevent any accidental, unauthorised or unlawful access to, processing, destruction, loss, alteration, damage or disclosure of the Applicable Customer's Confidential Information and protect the Applicable Supplier's IT systems used to provide the Services in accordance with applicable laws and Industry Best Practice.
- 6.2** The Applicable Supplier shall ensure that the measures outlined in clause 6.1 above include:
- 6.2.1** boundary firewalls and internet gateways to protect the Applicable Supplier networks and IT systems from the internet and other external networks;

- 6.2.2 secure configuration of the Applicable Supplier networks, IT systems, applications and devices, including encryption of portable devices and removable media and the encryption of Personal Data;
 - 6.2.3 physical and logical access controls that restrict access to only authorised users to the extent required to perform the required Services;
 - 6.2.4 malware protection software that is designed to prevent the introduction of malware into the Applicable Supplier IT systems, networks and devices;
 - 6.2.5 patch management practices to identify, assess and apply applicable security patches to the Applicable Supplier's IT systems, applications and devices; and
 - 6.2.6 training and awareness for Supplier Personnel in information security and the handling of Customer's Confidential Information in accordance with the terms of this Agreement.
- 6.3 The Applicable Supplier shall implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing of Personal Data.
- 6.4 The Applicable Supplier shall:
- 6.4.1 investigate all (i) accidental, unauthorised or unlawful access to, processing, destruction, loss, alteration, damage or disclosure of Customer's Confidential Information and/or any cyber-attacks on the Applicable Supplier's IT systems ("**Security Incidents**"); and (ii) suspected Security Incidents; and
 - 6.4.2 notify the Applicable Customer without undue delay, via soc@bp.com, of any Security Incident.
- 6.5 If an incident referred to in clause 6.4 occurs due to the Applicable Supplier's act or omission, the Applicable Supplier shall, at its own cost, provide all necessary assistance as requested by the Applicable Customer, including with notifications that may be required under applicable law.
- 6.6 PCI-DSS. Supplier 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:
- 6.6.1 Supplier 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 MasterCard, VISA, American Express, Discover, JCB or any other credit card brand or payment card network for or through which Supplier processes payment card transactions (the "**Card Associations**").
 - 6.6.2 Supplier represents and warrants that it validates its PCI-DSS compliance as required by the applicable Card Associations, and, as of the effective date of this Agreement, Supplier 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, Supplier 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 Annual 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 and that it has passed its most recent scan.

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

7 Regulatory Compliance and Anti-Corruption Undertakings

7.1 Compliance with Laws

- 7.1.1** The Applicable Supplier shall throughout the Term comply with:
- (i) all applicable export control, trade sanctions and other foreign trade control laws, rules and regulations including those of the territories where Services are to be performed and the US Export Administration Regulations (the "**Trade Restrictions**");
 - (ii) all applicable anti-bribery and corruption and anti-money laundering laws, rules, regulations or equivalent of the UK, the US and all locations where Services are provided including, the UK Bribery Act 2010 and the Foreign Corrupt Practices Act 1977 of the United States of America (regardless of whether the Applicable Supplier is otherwise subject to those laws); and
 - (iii) all other laws at all times relating to the performance of its obligations hereunder.
- 7.1.2** The Applicable Supplier shall obtain and maintain throughout the Term, at its own cost, all the consents, licences and permissions it may require and which are necessary to enable the performance of its obligations under the Global Agreement and each Release Order.
- 7.1.3** The Applicable Supplier shall ensure that Supplier Personnel attend such training, including on the Customer's Code of Conduct, as directed by the Applicable Customer from time to time.

7.2 Trade Restrictions

- 7.2.1** The Applicable Supplier represents and warrants that it, its Affiliates, subcontractors and Supplier Personnel are not persons who are identified from time to time by any government or legal authority as a person with whom trade or financial dealings and transactions by either the Applicable Supplier or Applicable Customer and/or its Affiliates are prohibited or restricted.
- 7.2.2** Failure to comply with the Trade Restrictions shall constitute a material breach of the Global Agreement and each Release Order.

7.3 Anti-Bribery and Corruption

- 7.3.1** The Applicable Supplier acknowledges that the Global Customer has a zero tolerance policy towards bribery and corruption including towards facilitation payments and grease payments.

- 7.3.2** The Applicable Supplier agrees, undertakes and confirms that it, its Affiliates and Supplier Personnel have not and will not make, offer, promise to make or authorise the making to any person or solicit, accept or agree to accept from any person, either directly or indirectly, anything of value including without limitation gifts or entertainment, facilitation payments or grease payments, in order to obtain, influence, induce or reward any improper advantage in connection with the Global Agreement or any Release Order or where to do so would breach any applicable anti-corruption or anti-money laundering laws or regulations (the “**Anti-Corruption Obligation**”).
- 7.3.3** The Applicable Supplier shall on an on-going basis:
- (i) notify the Applicable Customer in writing promptly upon discovery of any actual or suspected breach of the Anti-Corruption Obligation; and
 - (ii) inform all Supplier Personnel that they are required to act in accordance with the Anti-Corruption Obligation.
- 7.3.4** The Applicable Supplier shall, throughout the Term and for at least one (1) year following its expiration or termination:
- (i) upon reasonable notice, but not more than annually, permit the Applicable Customer or its duly appointed third party representatives to reasonably inspect, audit and make copies of any, books and records maintained in connection with the Services provided to such Applicable Customer under the Global Agreement and/or Release Order, such inspection to be carried out as expediently as possible and at Applicable Customer's sole expense; and
 - (ii) upon request cooperate and provide all reasonable assistance to enable the Applicable Customer to ensure and monitor compliance with the Anti-Corruption Obligation.

8 Taxes

- 8.1** All Charges for Services are exclusive of any applicable federal, state, provincial, local sales, use, excise, business, service, consumption, goods and services and value added taxes and other similar taxes (“**Sales Taxes**”) which shall be charged in addition at the appropriate rate and in accordance with applicable law at the time of supply.
- 8.2** If the Customer provides the Supplier with a duly authorised domestic U.S. exemption or direct pay certificate in respect of Sales Taxes, then the Supplier will exempt the Customer from payment of Sales Taxes, effective on the date that the Supplier receives the certificate.
- 8.3** If the Supplier has incorrectly determined the amount of Sales Taxes, then the Supplier shall correct the invoice in accordance with applicable law and provide the Customer with a valid tax invoice or credit note as appropriate. The Supplier will repay to the Customer any amount overpaid and the Customer will pay to the Supplier any amount underpaid within thirty (30) days of the Customer having been notified or becoming aware of the overpayment or underpayment and (in a case where the Customer is required to make a payment) subject to the receipt of a valid tax invoice from the Supplier.
- 8.4** Any amount paid by the Customer as reimbursement for (or calculated by reference to) any costs or expenses incurred by the Supplier, shall be calculated net of any credit allowed by any tax authority for Sales Tax purposes in respect of the same (“**Input Tax Credits**”) to which the Supplier is entitled, except where the relevant applicable law does not so permit.
- 8.5** The Customer will pay the Charges exclusive of any required tax, withholding or deduction imposed in the country of payment at the applicable rates at the time payment is made (“**Withholding Tax**”). Customer shall be liable for payment of all such Withholding Taxes, however designated, levied or based on Customer's use of the Services and shall account to

the relevant tax authority for such Withholding Tax in which event Customer shall (i) pay to Supplier such additional amount as is necessary so that Supplier receives, after such deduction or withholding (including any withholding with respect to this additional amount), an amount equal to the amount that Supplier would have received if such deduction or withholding had not been made and (ii) deliver to Supplier within thirty (30) days after the date of such payment an official receipt of the relevant taxing authority showing that Customer paid to such taxing authority the full amount of the tax required to be deducted or withheld. Supplier shall take reasonable administrative actions, if possible, to lawfully mitigate or to help recover on behalf of Customer any withholding taxes, if and only if none of the foregoing actions would operate to prejudice Customer with respect to its tax liability or otherwise.

- 8.6** The Supplier and its subcontractors are deemed to have taken into account, in their rates and Charges, all applicable taxes other than Sales Taxes. Each Party will be solely responsible for its own income, corporate, employment and property taxes.
- 8.7** [Intentionally Omitted]
- 8.8** The Applicable Supplier shall supply to the Applicable Customer such Tax information (including supporting documents) connected with the supply of the Services as may be reasonably requested by the Applicable Customer from time to time.
- 8.9** The Applicable Supplier shall immediately inform the Applicable Customer of any change in its Tax status where relevant to the supply of Services. For the avoidance of doubt the Applicable Customer shall be under no obligation to compensate the Applicable Supplier for additional Taxes arising as a consequence thereof.
- 8.10** For the avoidance of doubt, Sales Taxes attributable to any supplies, equipment and tools used by Supplier or its subcontractors in the performance of Services shall be paid by Supplier and its subcontractors and shall be included in all Charges for Services.

9 Charges, Invoicing and Payment

- 9.1** In consideration of the Applicable Supplier carrying out all of its obligations under the Global Agreement and the Release Order the Applicable Customer shall pay the Charges to the Applicable Supplier in accordance with this clause, Schedule 3 (*Pricing and Financial Provisions*) to the Global Agreement and Attachment 2 (Pricing and Financial Provisions) to the Release Order (as applicable).
- 9.2** The Applicable Customer is not liable to pay any amount (including the Charges) in respect of services required to remedy the Applicable Supplier's failure to perform the Services.
- 9.3** Supplier Personnel who are promoted to a higher personnel grade during the Term shall continue to be charged for at the rate applicable to the Supplier Personnel's initial grade.
- 9.4** Subject to clause 9.8, the Customer shall instigate payment of all valid and undisputed invoices submitted by the Supplier (or generated by the AP System) not later than thirty (30) days after the date on which the Supplier's valid invoice was correctly received by the Customer pursuant to clause 9.6. The Customer will make payment of valid and processed invoices on its next regularly scheduled payment run, which could be up to four (4) days later. Payments will not be considered late provided that the Customer makes payment of the funds on or before thirty (30) days after the Customer receives the valid invoice. If a Party is late in paying an undisputed invoice, and the Late Payment of Commercial Debts (Interest) Act 1998 or equivalent legislation would otherwise apply, the sums under such invoice will accrue interest from the date on which

the invoice was due at a rate equal to two (2) per cent per annum over the base rate of the Bank of England from time to time and this shall constitute a substantial remedy for late payment.

- 9.5** In relation to any Release Order or any other agreement entered into by the Parties, the Customer's obligations to pay the Charges shall not be affected by any set-off, counterclaim, recoupment, defence or other claim, right or action that the Customer may have against Supplier.
- 9.6** The Supplier shall submit invoices using the AP System (if any). If there is no such designated AP System, then receipts and invoices should be generated and submitted using a manual process designated by the Customer. If the Supplier submits receipts and invoices outside of the designated process then they may be rejected by the Customer. The Supplier should then resubmit receipts and invoices using the correct process.
- 9.7** All amounts due under the Release Order must be invoiced by the Supplier within twelve (12) months of the date on which the Supplier is first entitled to invoice such sums. The Supplier irrevocably waives the right to payment of any sums not invoiced within this period.
- 9.8** If the Customer reasonably and in good faith disputes its obligation to pay part or all of an invoice submitted by the Supplier under the Release Order (the "**Disputed Invoice**"), then the dispute escalation process set out in clause 26 (*Dispute Escalation*) shall apply. Upon the Customer's request, the Supplier shall rescind the Disputed Invoice and resubmit a new invoice for the undisputed portion of the Disputed Invoice, which the Customer shall pay as required herein. Upon settlement by the Parties of any dispute related to a Disputed Invoice, the Supplier shall submit an invoice to the Customer for the balance of any additional Charges agreed as due and the Customer shall make the appropriate payment as required herein. The Customer's failure to pay the Disputed Invoice will be deemed not to be a breach of the Release Order and the Supplier shall continue to perform its obligations under the Release Order notwithstanding any dispute related to invoices.
- 9.9** [Intentionally Omitted]

10 Record Retention and Audit Rights

- 10.1** Subject to clause 16.3, the Applicable Supplier shall maintain and retain:

- 10.1.1** records required by applicable law; and
- 10.1.2** accurate books, records accounts, and adequate supporting information relating to the Charges for a period of three (3) years after completion of the relevant Service, or such longer period as any applicable law may require.

The Applicable Supplier shall grant to the Applicable Customer (and to its representatives) the right of access to any documents, , Supplier Personnel, and any other relevant information, , in order to demonstrate compliance with, and to audit the Applicable Supplier's performance of, its obligations under the Global Agreement or relevant Release Order and the Charges and taxes charged to the Customer. Such audit, conducted no more than one time per calendar year, shall be after reasonable advance notice. The Applicable Supplier shall have the right to exclude from such audit any of its competitively sensitive data.

- 10.2** In the event that an audit establishes that the Customer has been overcharged for the provision of any Services the Supplier shall promptly refund the amount of any such overcharge.

11 Intellectual Property Rights

11.1 All Intellectual Property Rights belonging to a Party, subcontractor or third party prior to the Effective Date or the Release Order Effective Date or created other than in the provision of the Services ("**Pre-existing Intellectual Property Rights**") will remain vested in that Party, subcontractor or third party (as applicable) and shall not be assigned hereunder. Pre-existing Intellectual Property Rights must not be used by the other Party for any purpose except (i) with the owning Party's prior written consent or (ii) as expressly permitted by the Global Agreement or the Release Order.

11.2 Intentionally omitted.

11.2.1 The Supplier shall indemnify and hold harmless the Customer Indemnified Parties against all Claims arising from or relating to a claim of infringement of an Intellectual Property Right however arising as a result of or in connection with the provision, use or receipt of the Services or any Supplier Pre-existing Intellectual Property Rights, provided that the Customer (i) notifies Supplier in writing promptly after notice of any potential Claim (sufficient for Supplier to respond without prejudice); (ii) permits Supplier to defend, compromise or settle the Claim at its sole discretion and (iii) provides all reasonable and necessary cooperation to Supplier. If an infringement claim threatens the Customer's continued use of any of the Services, Supplier may, in its sole discretion: (a) substitute substantially functionally similar services; (b) procure for Customer the right to continue using the Services; or if (a) and (b) are not commercially reasonable, (c) terminate the Agreement and refund to Customer the fees paid by Customer for the portion of the Term that was paid by Customer but not rendered by Supplier. The foregoing indemnification obligation of Supplier shall not apply:

11.2.2 if the Services are modified by any party other than Supplier, but solely to the extent the alleged infringement is caused by such modification;

11.2.3 if the Services are combined with products or processes not specified in the Documentation or provided by Supplier, but solely to the extent the alleged infringement is caused by such combination;;

11.2.4 to any unauthorized use of the Services;

11.2.5 or

if Customer settles or makes any admissions with respect to a claim without Supplier's prior written consent.

THIS SECTION 11.2 SETS FORTH SUPPLIER'S SOLE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT.

12 Warranties and Representations

12.1 Each Party warrants, represents and undertakes that:

12.1.1 the Global Agreement and/or Release Order is executed by its duly authorised representative and once duly executed will constitute its legal, valid and binding obligations;

12.1.2 there are no actions, suits or proceedings or regulatory investigations pending, or to that Party's knowledge, threatened against that Party or any of its Affiliates that might adversely affect the ability of the Party to meet and carry out its obligations under the Global Agreement and/or Release Order; and

12.1.3 as at the Release Order Effective Date it has not and is not reasonably likely to suffer an Insolvency Event.

12.2 The Applicable Supplier warrants, represents and undertakes to the Applicable Customer that:

- 12.2.1** the Services and all obligations under the Release Order shall be performed with all due reasonable care and skill, in accordance with the Policies, Industry Best Practice and applicable law;
- 12.2.2** it has the requisite competitive alliances, and financial and physical resources necessary to provide and to fully perform the Services;
- 12.2.3** it will use an adequate number of personnel with appropriate skills and training who are appropriately experienced, qualified and competent to perform the Services and undertake the tasks assigned to them in connection with the Release Order and such personnel will perform the Services and such tasks assigned to them in a timely manner;
- 12.2.4** the Services, including the iOS and Android SDKs that are in "beta"-status as of the effective date of this Agreement, will conform in all material respects to the specifications, functions, descriptions, standards, and criteria set forth in the Service documentation. Customer's sole and exclusive remedy for any breach of this warranty shall be, at no additional charge to Customer, for Spreadly to use commercially reasonable efforts to correct the non-conformity. Except as provided in the documentation, Spreadly does not warrant that the Service will meet Customer's requirements or operate in combination with any other service providers, or that the Service's operation will be uninterrupted or error-free. Spreadly does not make and will not be liable for any warranties other than those expressly included in this Agreement.
- 12.2.5** it shall maintain throughout the Term business continuity and disaster recovery plans in accordance with Industry Best Practice.

12.3 Customer represents and warrants to Supplier that:

- 12.3.1** Customer 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;
- 12.3.2** Customer 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:
 - (i) The terms of service of the payment gateways, merchant service providers and/or API endpoints Customer connects with on the Service;
 - (ii) 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;
 - (iii) PCI-DSS and PA-DSS, as applicable; and
 - (iv) Any regulatory body or agency having jurisdiction over the subject matter hereof.

13 Insurance

- 13.1** The Supplier shall take out and maintain throughout the term of the Release Order and for a period of one (1) year afterwards insurance policies with a reputable third party insurance company with a credit rating of not less than "A" from Standard & Poor (or an equivalent rating from another reputable ratings agency approved by the Customer) which are appropriate to its level of obligation and liability under the Release Order including all insurances required to be maintained by applicable law and with the following minimum insurance cover:

- 13.1.1 public and product (commercial general) liability insurance (or the closest local equivalent(s)) in respect of loss or injury to persons or damage to tangible property with a limit of not less than **\$1 million** per occurrence;
 - 13.1.2 tech and cyber (errors and omissions) insurance (or the closest local equivalent(s)) in respect of its undertakings and obligations under the Release Order with a minimum level of cover of **\$5 million** per occurrence; and
 - 13.1.3 employer's liability insurance and (where required) workers compensation insurance (or the closest local equivalent(s)) with a minimum level of cover of **\$1 million** for any one occurrence.
- 13.2 [Intentionally Omitted]
- 13.3 Intentionally Omitted] [

14 Liability

- 14.1 Exclusion of Damages. SUBJECT TO CLAUSE 14.4 (EXCEPTIONS), BUT OTHERWISE NOTWITHSTANDING ANY OTHER PROVISION OF THE GLOBAL AGREEMENT OR RELEVANT RELEASE ORDER (AS THE CONTEXT REQUIRES), NO PARTY SHALL BE LIABLE TO THE OTHER PARTY, WHETHER IN CONTRACT, IN TORT (INCLUDING NEGLIGENCE), UNDER WARRANTY, UNDER STATUTE OR OTHERWISE FOR OR IN RESPECT OF ANY INDIRECT OR CONSEQUENTIAL LOSSES OF WHATEVER NATURE NOR FOR ANY LOSS OF PROFIT OR REVENUE.
- 14.2 General Liability Cap.
- 14.2.1 Customer. SUBJECT TO CLAUSE 14.4 (EXCEPTIONS), THE LIABILITY, WHETHER IN CONTRACT, IN TORT (INCLUDING NEGLIGENCE), UNDER WARRANTY, STATUTE OR OTHERWISE, OF THE CUSTOMER IN CONNECTION WITH ANY CLAIM OR SERIES OF RELATED CLAIMS SHALL BE LIMITED TO THE GREATER OF (A) AN AMOUNT EQUAL TO THE TOTAL CHARGES PAID OR PAYABLE UNDER ALL RELEASE ORDERS ENTERED INTO IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRIOR TO THE DATE ON WHICH THE CUSTOMER RECEIVES WRITTEN NOTICE OF SUCH CLAIM OR THE FIRST OF A SERIES OF RELATED CLAIMS; and (B) \$1,000,000.
- 14.2.2 Supplier. SUBJECT TO CLAUSE 14.4 (EXCEPTIONS), THE LIABILITY, WHETHER IN CONTRACT, IN TORT (INCLUDING NEGLIGENCE), UNDER WARRANTY, STATUTE OR OTHERWISE, OF THE SUPPLIER IN CONNECTION WITH ANY CLAIM OR SERIES OF RELATED CLAIMS SHALL BE LIMITED TO THE GREATER OF (A) AN AMOUNT EQUAL TO THE TOTAL CHARGES PAID OR PAYABLE UNDER ALL RELEASE ORDERS ENTERED INTO IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRIOR TO THE DATE ON WHICH THE SUPPLIER RECEIVES WRITTEN NOTICE OF SUCH CLAIM OR THE FIRST OF A SERIES OF RELATED CLAIMS; and (B) \$1,000,000.
- 14.3 Special Liability Cap. SUBJECT TO CLAUSE 14.4 (EXCEPTIONS), NOTWITHSTANDING THE LIMITS IN CLAUSE 14.2, EACH PARTY'S AGGREGATE LIABILITY FOR LIABILITIES RESULTING FROM: (1) BREACH OF THE APPLICABLE SUPPLIER'S SECURITY, PRIVACY AND/OR DATA PROCESSING OBLIGATIONS SPECIFIED IN CLAUSE 6 (INFORMATION SECURITY); CLAUSE 18 (DATA PROTECTION); OR SCHEDULE 4 SECTION E (INFORMATION SECURITY REQUIREMENTS FOR SUPPLIERS); (2) A PARTY'S BREACH OF CLAUSE 16 (CONFIDENTIALITY); (3) SUPPLIER'S INDEMNIFICATION OBLIGATIONS HEREIN (EXCLUDING IP INFRINGEMENT); SHALL NOT EXCEED \$2,500,000. THE SPECIAL LIABILITY CAP SHALL APPLY SOLELY TO THE CLAIMS DESCRIBED IN THIS CLAUSE 14.3.

FOR AVOIDANCE OF DOUBT, THE PARTIES AGREE THAT DIRECT DAMAGES THAT ARE RECOVERABLE UNDER THIS CLAUSE 14.3 SHALL INCLUDE THE FOLLOWING LIABILITIES: (i) ANY REASONABLE COSTS AND/OR EXPENSES ACTUALLY INCURRED BY CUSTOMER IN CONNECTION WITH FULFILLING LEGALLY REQUIRED OBLIGATIONS RESULTING FROM A SECURITY INCIDENT THAT IS CAUSED BY SUPPLIER'S MATERIAL BREACH OF ITS SECURITY OBLIGATIONS SET FORTH IN CLAUSE 6 AND SCHEDULE 4 SECTION E (E.G., SENDING NOTICES TO AFFECTED END USERS, FORENSIC INVESTIGATION EXPENSES, AND THE COST OF PROVIDING LEGALLY REQUIRED MONITORING SERVICES TO AFFECTED END USERS); AND (iv) ANY FINES, PENALTIES, NON-COMPLIANCE FEES OR SIMILAR AMOUNTS ASSESSED OR IMPOSED BY A GOVERNMENTAL AUTHORITY OR CARD ASSOCIATION IN CONNECTION WITH AN INFORMATION SECURITY INCIDENT THAT IS CAUSED BY SERVICE PROVIDER'S MATERIAL BREACH OF ITS SECURITY OBLIGATION SET FORTH IN CLAUSE 6 AND SCHEDULE 4 SECTION E.

14.4 Exceptions. The limits on liability set out Clause 14.2 and Clause 14.3 shall not apply in respect of:

- 14.4.1 any liability for death or personal injury resulting from a Party's negligence;
- 14.4.2 any liability for Gross Negligence, fraud or any liability to the extent which it cannot be lawfully excluded;
- 14.4.3 the obligation on the Customer to pay undisputed Charges that have become due;
- 14.4.4 [Intentionally Omitted];
- 14.4.5 [Intentionally Omitted] ;
- 14.4.6 [Intentionally Omitted];
- 14.4.7 [Intentionally Omitted]
- 14.4.8 [Intentionally Omitted].
- 14.4.9 Supplier's indemnification and defence obligations in connection with infringement claims under Clause 11.2.

15 Force Majeure

Neither Party shall be liable to the other for failure to comply with its obligations in the Release Order to the extent that such failure is caused by war, armed conflict, actual or threatened terrorist attack, nuclear, chemical or biological contamination, fire or any natural disaster. If such a Force Majeure event continues for a period longer than thirty (30) days, the non-affected Party shall have the right to immediately terminate the Release Order. Nothing herein shall relieve the Supplier of its obligation to have proper business continuity and disaster recovery plans in place.

16 Confidentiality

- 16.1 Subject to clause 16.2, each Party shall treat as strictly confidential and not disclose to any third party nor use any Confidential Information of the other Party.
- 16.2 The provisions of clause 16.1 shall not prohibit disclosure or use of Confidential Information if and to the extent:

- 16.2.1 necessary for the performance of obligations or the exercise of rights under the Global Agreement and/or the Release Order;
- 16.2.2 where the receiving Party is the Applicable Customer, that disclosure is by the Applicable Customer to: (i) its Affiliates; or (ii) any third party providing services to the Applicable Customer or its Affiliates that are related to the Services; or (iii) any replacement supplier or potential replacement supplier, for the re-tendering or transfer of the Services;
- 16.2.3 required by law, or regulatory authority;
- 16.2.4 made to the professional advisers of a Party;
- 16.2.5 it becomes publicly available except as a result of a breach of an obligation of confidentiality;
- 16.2.6 the original disclosing Party has given prior written approval to the disclosure;
- 16.2.7 the Confidential Information is independently developed by the receiving Party without violating its obligations under this clause or the disclosing Party's proprietary rights; or
- 16.2.8 the Confidential Information is already in the possession of the receiving Party and is not subject to an obligation of confidentiality or a restriction on use,

provided that: (i) except where prohibited by applicable law, prior to disclosure of any Confidential Information pursuant to clause 16.2.3, the receiving Party shall promptly notify the disclosing Party of such requirement with a view to providing the disclosing Party with the opportunity to contest such disclosure or otherwise to agree the timing and content of such disclosure; and (ii) prior to the disclosure of any Confidential Information pursuant to clauses 16.2.1, 16.2.2 and 16.2.4, the receiving Party ensures that third parties undertake to comply with confidentiality provisions no less stringent than the provisions of this clause.

- 16.3 In the event of the termination or expiration of the Global Agreement or the Release Order, each Party shall return to the other Party (or, at the disclosing Party's option, destroy) all Confidential Information of the disclosing Party and all copies thereof, provided that each Party shall be entitled to retain one copy of the Confidential Information to the extent required to comply with applicable law or to the extent such Confidential Information is necessary to receive the benefit of any continuing right provided under the Global Agreement or applicable Release Order.

- 16.4 The confidentiality obligations under this clause shall survive for three (3) years after termination or expiry of the Global Agreement or the Release Order.
- 16.5 Under no circumstances will the Supplier deny (or place unreasonable conditions on) the Customer or its Affiliates access to the Customer Confidential Information, including any data created as a result of the Services.

17 Publicity and Public Announcements

- 17.1 Applicable Supplier shall not without the Applicable Customer's prior written approval: (i) make any public announcement relating to the Global Agreement or any Release Order; nor (ii) use Customer or its Affiliates' trademarks, logos or names. This does not affect any announcement or circular required by applicable law or any authority or the rules of any recognised stock exchange, but the Applicable Supplier shall consult with the Applicable Customer so far as is reasonably practicable before complying with such obligation.
- 17.2 [Intentionally Omitted]

18 Data Protection

- 18.1** “**Data Controller**” means the person which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; “**Data Processor**” means the person which processes Personal Data on behalf of the Data Controller; and “**processing**” means any operation(s) performed upon Personal Data such as collection, recording, storage, adaptation, use, disclosure by transmission or otherwise making available.
- 18.2** The Supplier acknowledges that the Customer is the Data Controller in respect of any Personal Data that the Supplier processes on the Customer’s behalf in the course of providing the Services and that the Supplier is a Data Processor of such data.
- 18.3** The nature and purpose of the processing of Personal Data by the Supplier where Supplier acts as a Data Processor is the performance of the Services pursuant to this Global Agreement. The categories of data subjects whose Personal Data will be processed in the course of providing the Services, and the types of such Personal Data which will be processed, are as set out in Schedule 2 (*Service Description*) to this Global Agreement.
- 18.4** The processing of Personal Data shall continue only for the duration of the Global Agreement, save to the extent required by applicable law, or regulatory authority.
- 18.5** The Supplier agrees that it shall (and shall procure that each of its Affiliates and subcontractors shall):
- 18.5.1** only carry out processing of Personal Data in accordance with the Customer’s instructions; and
 - 18.5.2** not process or permit the processing of Personal Data outside the European Economic Area except: (i) where no European Personal Data is being processed under the Agreement; or (ii) with the prior written consent of the Customer and, where such consent is granted, the Supplier undertakes to enter into a suitable agreement with the Customer and/or any relevant parties and/or adopt any necessary measures in order to ensure an adequate level of protection with respect to the privacy rights of individuals; “**European Personal Data**” in this sub-clause means Personal Data which comes within the scope of any of the laws and regulations of the European Union, the European Economic Area and their member states, and the United Kingdom applicable to the processing of Personal Data as amended from time to time; ***[Drafting Note: BP should ask the supplier if any information identifying individuals will be processed outside of the country of origin by either itself or any subcontractors. If so, refer to the Data Protection Section of the Wiki]***
 - 18.5.3** ensure that Supplier Personnel engaged in the processing of Personal Data shall treat as strictly confidential any Personal Data, and are bound under an appropriate obligation of confidentiality;
 - 18.5.4** at no additional cost, take such technical and organisational measures as may be appropriate to assist the Customer, insofar as this is possible, to comply with (i) the rights of individuals under applicable data protection laws, including subject access rights, the rights to rectify and erase Personal Data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data; and (ii) information or assessment notices served by any data protection authority;
 - 18.5.5** at no additional cost, assist the Customer in complying with its obligation, where applicable, to undertake a data protection impact assessment; and
 - 18.5.6** immediately inform the Customer if, in its opinion, an instruction as per clause 18.5.1 above infringes the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) or other European Union or Member State data protection provisions, in accordance with Article 28(3) of the General Data Protection Regulation.

19 Termination of the Global Agreement

- 19.1** Provided no Release Orders are in effect, the Global Customer may at any time terminate the Global Agreement for convenience by giving fourteen (14) days written notice to the Global Supplier.
- 19.2** [Intentionally Omitted].

20 Termination of the Release Order

- 20.1** Without prejudice to any other rights and remedies of the Customer under the Release Order, at law or in equity, the Customer may at any time terminate the Release Order in whole or in part by written notice to the Supplier, without any liability to the Supplier, if:
- 20.1.1** there is a material breach, or series of breaches (whether or not similar in nature) the combination of which constitutes a material breach by the Supplier of the Release Order and (if capable of remedy) the Supplier has failed to remedy the breach(es) within thirty (30) days after receipt of notice from the Customer giving full particulars of the breach(es) and requiring the breach(es) to be remedied;
 - 20.1.2** there is a material breach, or series of breaches (whether or not similar in nature), the combination of which constitutes a material breach by the Supplier of clause 16 (*Confidentiality*);
 - 20.1.3** the Supplier and/or Global Supplier or one of its officers or directors has been indicted for or involved in fraud or has been involved in financial irregularities; or
 - 20.1.4** There is a material breach of the provisions in clause 7 (*Regulatory Compliance and Anti-Corruption Undertakings*) or in clause 5.1.2 (*Customer's Business and Human Rights policy*).
 - 20.1.5** [Intentionally Omitted].
- 20.2** Customer may terminate a Release Order without cause at any time after the first 12 months from the applicable Release Order Effective Date, by providing no less than three (3) months prior written notice to Supplier with the termination effective as of the date set forth in such notice. In the event of early termination of a Release Order in accordance with this clause, the Supplier shall be entitled to fair compensation for stranded costs to be negotiated in good faith by the Parties but in no event less than the total Charges that would have been due to Supplier for the remainder of the then-current term (excluding any renewal terms which have not commenced) under the terminated Release Order.
- 20.3** The Supplier may at any time terminate the Release Order by written notice to the Customer if the undisputed Charges relating to the Release Order that are due and payable by the Customer remain unpaid for more than forty five (45) days after the due date of payment, provided that the Supplier:
- 20.3.1** has notified the Customer in writing if any Charges remain unpaid (excluding non-payment of any Disputed Invoices) promptly after the due date for payment and has specified the amount of payments due; and
 - 20.3.2** if it intends to serve such written notice, issues a warning notice in writing to the Customer specifying the amount of payments to be made no less than twenty (20) days before exercising its right to terminate the Release Order.
- 20.4** The Supplier shall not have the right to terminate or rescind the Release Order or accept any repudiation of the Release Order, except as set out in the Release Order.

21 Consequences of Termination

- 21.1** Neither termination nor expiry of the Global Agreement or the Release Order affects a Party's rights and obligations accrued at the time of termination or expiry.
- 21.2** The following clauses, each as incorporated into the Release Order (where the context requires), shall survive termination or expiry, in whole or in part, for any reason, of the Global Agreement or the Release Order: clauses 1 (*Definitions and Interpretation*), 6 (*Information Security*), 7.3 (*Anti-Bribery and Corruption*), 8 (*Taxes*), 10 (*Record Retention and Audit Rights*), 11 (*Intellectual Property Rights*), 12 (*Warranties and Representations*), 13 (*Insurance*), 14 (*Liability*), 16 (*Confidentiality*), 17 (*Publicity and Public Announcements*), 18 (*Data Protection*), 21 (*Consequences of Termination*), 22 (*Exit Management Assistance*), 23 (*Third Party Rights*), 24 (*Notices*), 25 (*Miscellaneous*), 26 (*Dispute Escalation*) and 27 (*Governing Law, Jurisdiction and Dispute Resolution*).

22 Exit Management Assistance

- 22.1** At Customer's request, Supplier shall provide all information and assistance necessary to ensure a smooth transition of the Services being from Supplier to another service provider of Customer's choosing ("**Transition Assistance**") for up to six (6) months following the applicable termination or expiration.
- 22.2** The Supplier shall provide the Transition Assistance on a time and materials basis, according to the Supplier's then applicable fees for professional services, and may include:
- 22.2.1** Developing a plan for orderly transition of the terminated Services;
- 22.2.2** Transferring of Customer Data from Supplier to Customer or other service provider on a format and manner requested by Customer;
- 22.2.3** Such other activities as the parties may agree.

23 Third Party Rights

- 23.1** The Applicable Supplier acknowledges that the Applicable Customer enters into the Global Agreement and the Release Orders for its own benefit and for the benefit of the Customer Indemnified Parties.
- 23.2** Where a Customer Indemnified Party suffers losses pursuant to the Global Agreement or the Release Order, the Parties agree that the Applicable Customer may on notice deem (and recover) such losses as if they were losses of the Applicable Customer.
- 23.3** Where the Contracts (Rights of Third Parties) Act 1999 applies, a person who is not a Party to the Global Agreement or the Release Order has no right to directly enforce any of its provisions.
- 23.4** The applicable Parties may by agreement amend the Global Agreement or the Release Order (as appropriate) without obtaining the consent of any third party notwithstanding that any such amendment may relate to any benefits conferred on such third party.

24 Notices

A notice under or in connection with the Global Agreement shall be in writing and in English. A notice shall be deemed given when delivered in person or five (5) days after proper mailing to the address set out below:

Customer: <i>BP International Limited</i>	Supplier: <i>Spreadly, Inc.</i>
Address: Procurement Contracts Administrator (UK) – Retail Technology Procurement BP ICBT, Chertsey Road, Sunbury on Thames, Middlesex. TW16 7LN. UK	Address: 300 Morris Street, Suite 400, Durham, North Carolina, USA 27701
For the attention of: <i>'Category Specialist – Retail Technology</i>	For the attention of: Nellie Vail VP of Finance and International Operations

25 Miscellaneous

- 25.1** If any provision in the Global Agreement or the Release Order is held to be illegal, invalid or unenforceable, in whole or in part, then such provision or part of it shall, to such extent be deemed not to form part of the Global Agreement or the Release Order and the legality, validity and enforceability of the remainder of the Global Agreement or the Release Order shall not be affected and shall continue in force and effect.
- 25.2** Save as expressly provided in the Global Agreement or the Release Order, no failure of a Party to exercise, and no delay by it in exercising any right, power or remedy in connection with the Global Agreement or Release Order shall operate as a waiver of such rights, nor shall any single or partial exercise of any rights preclude any further exercise of such right or any other right.
- 25.3** The Applicable Customer may assign, novate, assume or otherwise transfer the Global Agreement or the Release Order to its Affiliates or to any successor without the Applicable Supplier's consent and to any other person with the Applicable Supplier's prior written consent, which consent will not be unreasonably withheld or delayed. The Applicable Supplier shall not assign, novate, assume or otherwise transfer the Global Agreement or the Release Order to any person, except to its Affiliates, without the prior written consent of the Applicable Customer, which consent will not be unreasonably withheld or delayed. Any purported assignment other than in accordance with this clause is null, void and of no effect.
- 25.4** No amendment of the Global Agreement or Release Order shall be valid unless it is in writing and executed by or on behalf of each of the Parties to it.
- 25.5** The Global Agreement, its Schedules, the Policies and any other documents referred to in the Global Agreement constitute the entire agreement between the Parties with respect to the subject matter of the Global Agreement and (to the extent permissible by law) supersedes all prior representations or oral or written agreements between the Parties with respect to that subject matter, provided that neither Party is attempting to exclude any liability for fraudulent misrepresentations. No conflicting or additional terms or conditions endorsed on, delivered with or contained in any Applicable Supplier quotation, acknowledgement of order, delivery note, invoice or other Applicable Supplier document shall form part of the Global Agreement or of any Release Order and all such conflicting or additional terms are hereby rejected by the Applicable Customer. The Global Agreement may be entered into in any number of counterparts.

26 Dispute Escalation

- 26.1.1** The Parties shall attempt to resolve any issue in relation to the Global Agreement or the Release Order by first attempting informal resolution. Such discussions or correspondence shall be without prejudice to either Party's rights and remedies and any actions taken shall not constitute a waiver

thereof. Either Party may, at any time after having sought to resolve the issue informally, submit a written statement detailing the nature of the unresolved issue and the BP reference number of the Global Agreement and relevant Release Order(s) to their contract or account manager (a "Dispute Notice"). Following creation of a Dispute Notice the contract or account manager shall submit such Dispute Notice to the other Party and: the nominated contract manager or account manager of each Party shall meet to resolve the dispute, and if they cannot resolve the dispute within ten (10) working days of the dispute being referred to them; then

26.1.2 the dispute shall promptly be referred by either Party to, in the case of the Applicable Customer the VP Indirect Procurement or his delegate, and in the case of the Applicable Supplier the CEO or Managing Director or equivalent, or in either case any such persons who may be identified as authorised representatives in Schedule 2 (*Service Description*) of the Global Agreement as may be amended by Attachment 1 (*Service Description*) to a relevant Release Order.

26.2 If, within fourteen (14) working days of the dispute having been referred to the individuals specified in this clause, no agreement has been reached, each Party shall be free to pursue the rights granted to it by the Global Agreement or the Release Order, by law or in equity.

27 Governing Law, Jurisdiction and Dispute Resolution

27.1 Notwithstanding anything to the contrary in the Global Agreement or any Release Order, both Parties shall be entitled at any time to seek injunctive or other urgent relief in any court of competent jurisdiction.

27.2 The Global Agreement, the Release Order and any non-contractual obligations arising out of or in connection with them or their subject matter or formation, shall be governed by and construed in accordance with the laws of England and Wales.

27.3 Any dispute arising out of or connected with the Global Agreement or the Release Orders, which the parties have been unable to resolve pursuant to clause 26 (*Dispute Escalation*), including a dispute as to their validity or existence and/or this clause, shall be resolved by arbitration in London conducted in English by a single arbitrator pursuant to the LCIA Rules.

27.4 Where such disputes arise which, in the absolute discretion of the first arbitrator to be appointed in any of the disputes, are so closely connected that it is expedient for them to be resolved in the same proceedings, that arbitrator shall have the power to order that the proceedings to resolve such disputes shall be consolidated (whether or not proceedings to resolve those other disputes have yet been instituted), provided that no date for the final hearing of the first arbitration has been fixed.

27.5 Without prejudice to any other method of service permitted by law, the Applicable Supplier agrees that the documents which start any proceedings and any other documents required to be served in relation to those proceedings may be served on its related entity, Spreadly UK Limited at 5 The Green, Richmond, Surrey, United Kingdom TW9 1PL or at any address at which process may be served on it in accordance with applicable law. The Applicable Supplier shall inform the Applicable Customer, in writing, of any change in the name and/or address of the Agent within twenty eight (28) days of such change. Nothing herein shall affect the right to serve process in any other manner permitted by law.

EXECUTED by the Global Customer and the Global Supplier
SIGNED by

Andrew Jackson,
Retail Technology Category Leader

for and on behalf of BP International Limited

}

DocuSigned by:
Andrew Jackson
F7E82C13719043A...
28-May-21

SIGNED by
Justin Benson,
CEO

for and on behalf of Spreadly, Inc.

}

DocuSigned by:
Justin Benson
9624ED07D136401...
28-May-21

Schedule 1
Template Release Order

DATE: *[insert effective date for this Release Order]* or, if no such date is specified, the date on which the Release Order is executed by the last party to do so (the “**Release Order Effective Date**”).

BP reference number: *[Insert BP reference number. This number should be specific to this Release Order.];*

Description: *[Insert brief description of subject matter of the Release Order.].*

This Release Order is executed under an agreement (BP reference number [●]) *[insert BP reference number from relevant Global Agreement]* between *[insert names of Global Customer and Global Supplier]* dated *[insert date of the Global Agreement]* (the “**Global Agreement**”).

Parties:

- (1) *[INSERT NAME OF CUSTOMER]*, a company incorporated in [●] (registered no. [●]) having its registered office at [●] (the “**Customer**”); and
- (2) *[INSERT NAME OF SUPPLIER]*, a company incorporated in [●] (registered no. [●]) having its registered office at [●] (the “**Supplier**”).

- 1** This Release Order shall be constructed and interpreted in accordance with clauses 1 and 2 of the Global Agreement.
- 2** This Release Order incorporates the following Attachments: *[insert list of the Attachments (and any appendices) to the Release Order]*.
- 3** This Release Order shall take effect on the Release Order Effective Date and, subject to early termination shall expire *[[●] years/months]* later. The Customer may extend the Term of the Release Order by up to one (1) year. The Services shall commence on the Service Commencement Date specified in Attachment 1 (*Service Description*).
- 4** Each Party shall have the additional or varied rights and obligations given to it in Attachment 3 (*Special Conditions*).
- 5** A notice under or in connection with this Release Order shall be in writing and in English. A notice shall be deemed given when delivered in person or five (5) days after proper mailing to the postal address set out below:

Customer	Supplier
Postal Address: <i>[insert]</i>	Postal Address: <i>[insert]</i>
For the attention of: <i>[insert]</i>	For the attention of: <i>[insert]</i>
Telephone Number: <i>[insert]</i>	Telephone Number: <i>[insert]</i>
Email address: <i>[insert]</i>	Email address: <i>[insert]</i>

- 6** This Release Order and its Attachments, the General Terms, incorporated Schedules and any other documents referred to in the Release Order constitute the entire agreement between the Parties with respect to the subject matter of the Release Order and (to the extent permissible by law) supersedes all prior representations or oral or written agreements between the Parties with respect to that subject matter, provided that neither Party is attempting to exclude any liability

for fraudulent misrepresentations. No conflicting or additional terms or conditions endorsed on, delivered with or contained in any Supplier quotation, acknowledgement of order, delivery note, invoice or other Supplier document shall form part of the Release Order and all such conflicting or additional terms are hereby rejected by the Customer. The Release Order may be entered into in any number of counterparts.

EXECUTED by the Customer and the Supplier

SIGNED by *[print name and title]*

for and on behalf of *[insert relevant BP entity]*

}

SIGNED by [print name and title]

for and on behalf of [insert relevant Supplier entity]

}

Attachment 1 to the Release Order (Service Description)

[Drafting Note: Each Release Order will set out in Attachment 1 (Service Description) to the Release Order the specific Services that will apply to that Release Order. These could be the full catalogue of Services agreed under Schedule 2 (Service Description) to the Global Agreement or a part of those Services (as may be amended to reflect requirements of specific entities). Here the services could be referred to or copied or extracted as necessary from Schedule 2 (Service Description).]

Attachment 2 to the Release Order (Pricing and Financial Provisions)

[Drafting Note: Each Release Order will set out in Attachment 2 (Pricing and Financial provisions) to the Release Order the Charges that will apply to the Services under that Release Order. These will likely be the Charges agreed under Schedule 3 (Pricing and Financial provisions) to the Global Agreement as may be amended for the purposes of the specific Release Order. Here the charges could be referred to or copied or extracted as necessary from Schedule 3 (Pricing and Financial provisions).]

Attachment 3 to the Release Order (Special Conditions)

[Drafting Note: If any special conditions are required for an individual Release Order (for example to take account of a mandatory requirement of the local country in which the services are being provided) then those conditions should be listed below.]

The Parties have agreed to the following Special Conditions, which are permitted modifications and/or supplements to the terms of the Release Order:

- 1** Modifications required in order for the Release Order to comply with applicable law in ***[INSERT COUNTRY OR COUNTRIES]*** but only to the extent required for compliance:

[Insert details, if any]

- 2** Modifications required in order for the Release Order to comply with the Customer's corporate governance policies and procedures but only to the extent required for compliance.

[Insert details, if any]

- 3** Modifications that have been specifically designated in the Schedules to the Global Agreement as matters that are to be agreed by the Supplier and the Customer in the Release Order.

[Insert details, if any]

- 4** Modifications required to reflect the nature of the particular services that are the subject of the Release Order.

[Insert details, if any]

Schedule 2A:
Operations and Service Levels

1 Services Description

The Supplier, Spreedly, provides software as a service to electronically 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 and/or third-party payment method receivers that Spreedly supports, and, where applicable, automatically update expired or lost credit cards.

Spreedly API. Spreedly's API-based Payments Orchestration platform (Spreedly's API) enables the Customer and its authorized affiliates, to tokenize End User payment instruments via Spreedly's iFrame payment form (or utilizing Spreedly's iOS and/or Android SDKs) in a centralized, PCI-DSS Level 1 certified token vault, and then use those tokens to process transactions with Customer's payment and fraud service provider(s) of choice. Spreedly's API provides one integration to 120+ gateways, payment processors, fraud service providers and alternate payment methods (APMs) globally. Through this single API connection, Customer can optimize and route transactions through gateways, processors and acquirers as needed based on a variety of factors and use cases. Additionally, Spreedly's API provides the ability for Customer to use its third-party vaulting services, enabling Customer to send and receive Cardholder Data from third party vaults (e.g., another payment gateway or tokenization service).

Supplier will (i) monitor whether the Services are available in accordance with reasonable and customary Industry Best Practices and (ii) provide notification to Supplier of known material problems with the Services that are likely to impair the normal functioning of the Services.

2 Services Availability

Service Availability (as defined below) for the Services shall be ninety-nine point nine-nine percent (99.99%). If the Supplier fails, or is likely to fail, to fulfil any of the Supplier's responsibilities in relation to Services Key Performance Indicators (as detailed in this Schedule), then the Supplier shall arrange, at the Supplier's own cost and expense, such additional Resources as are necessary to fulfil the relevant obligation by the relevant date (where applicable) or as soon as practicable thereafter.

(i) **"Service Availability"** means that the services are up and running, accessible by Customer and its end users, without interruption or undue delay and is calculated as set forth in Table 1 below.

Table 1 – Service Availability Definition

Service Availability shall be calculated using the formulas shown below	
Planned Service Availability	Available Time in Month minus Excluded Downtime
Actual Service Availability	Planned Service Availability minus Downtime
Service Availability Level (%)	Actual Service Availability divided by the Planned Service Availability x 100

(ii) **"Excluded Downtime"** means: (a) Scheduled Maintenance (as defined below); (b) Emergency Maintenance (as defined below); (c) reasons of force majeure (as described in the Agreement); (d) issues attributable to a Customer application, Customer components or Customer Data; (e) issues attributable to the public internet, private line or VPN connection to the physical site location of the Services; (f) issues attributable to Customer or any other third party-managed hardware, software, computer systems and/or services that interface with the Services; (g) issues

arising from acts or omissions of Customer, its employees, agents, and/or Customer end users in breach of this Agreement; or (h) network intrusions or denial of service attacks; (i) or any downtime resulting from outages of third party connections or utilities or other reasons beyond Supplier’s control will be excluded from any such calculation.

(iii) **“Scheduled Maintenance”** means: A maintenance event not to exceed one hundred twenty (120) minutes that meets the following criteria:

- (1) Supplier has scheduled the event by notice to Customer and its Affiliates delivered by email no less than ten (10) working days beforehand; and
- (2) Supplier notifies Customer and its Affiliates via email immediately prior to and after the Scheduled Maintenance is performed, or as soon as practicable if the Scheduled Maintenance is postponed or cancelled, and
- (3) The Downtime for each single Scheduled Maintenance event shall not exceed one hundred twenty (120) minutes, and Supplier will work diligently to minimise the duration of each scheduled Downtime.

During Scheduled Maintenance Supplier’s platform may not respond to transaction messages and it is Customer’s or its Affiliate’s responsibility to recognise the appropriate response code and convey this message to the Customer User accordingly detect this situation and queue messages during such Scheduled Maintenance. Customer or its Affiliates is/are solely responsible for notifying Customer Users of the unavailability of the Services due to Scheduled Maintenance.

(iv) **“Emergency Maintenance”** means a maintenance event that: (a) Supplier reasonably determines to be necessary to cure or prevent a condition that might result in a Level I or Level II incident, and (b) Supplier notifies Customer or its Affiliates, of as soon as practical, including the expected duration.

Supplier shall take all commercially reasonable steps in accordance with customary industry practice to prevent, or minimise the duration of, any interruption of Services availability due to Emergency Maintenance. Warnings of Emergency Maintenance activities shall be disseminated to the First Contact at Customer identified below by means of electronic mail and other appropriate and available methods. Customer shall be solely responsible for notifying Customer Users of the unavailability of the Services due to Emergency Maintenance.

(v) **“Downtime”** means that Supplier’s Services are unable to transmit or receive data to or from the Internet as defined by its inability to respond to internal “ping” requests.

3 Services Key Performance Indicators

Supplier will use its best efforts ensure that during each month the following functionality of the Services shall meet or exceed the following key performance indicators. If the Supplier fails, or is likely to fail, to fulfil any of the Supplier’s responsibilities in relation to Services Key Performance Indicators, then the Supplier shall arrange, at the Supplier’s own cost and expense, such additional Resources as are necessary to fulfil the relevant obligation by the relevant date (where applicable) or as soon as practicable thereafter.

- (i) Latency Performance Indicators are set forth in Table 2.

Table 2 – Latency Performance

Service	Description	Target Latency Performance Indicator
---------	-------------	--------------------------------------

Transaction	Provides ability to receive, process and send payment related transactions.	Transactions processed and sent by Services to applicable telecommunications provider within 2 seconds 99% of time, and within 10 seconds or less 99.90% of time within any 24 hour period.
-------------	---	---

(ii) Transaction Latency Performance Indicators are conditional upon each of Customer and its Affiliate and the relevant payment processors, financial institutions, merchants and/or relevant telecommunications provider sending the correct transaction messages.

(iii) Any latency resulting from outages of third-party connections or utilities or other reasons beyond Supplier's control will be excluded from any such calculation.

4 Conditions Precedent to Service Levels.

(i) Supplier shall not be responsible for a failure to achieve a Service Level set forth in this Schedule that is caused by (a) deployment of the Services on other than as directed in the applicable documentation, (b) a failure by Customer or its Affiliates to properly implement, operate and maintain in accordance with the applicable documentation of any Services and any other Supplier-supplied APIs, web services, SDKs, interfaces, specifications or integration points that are within Customer or its Affiliate's control or any failure by Customer or its Affiliate to follow the then current Supplier APIs, documentation and specifications as delivered by Supplier to Customer or its Affiliate, or (c) a failure of Customer or its Affiliate's systems (to include those third parties operating as a service provider to Customer or its Affiliates, such as telecommunications providers, payment processors, financial institutions, payment networks and others) or a failure by Customer or its Affiliates to properly operate, maintain and ensure compatibility of Customer or its Affiliates provided hardware, software, and services that interface or interoperate with the Services or are otherwise required for the provision of the Services.

(ii) Customer or its Affiliates shall notify Supplier in writing at least two

(2) Working days before a scheduled maintenance of Customer or its Affiliates' systems that may impact the Services provided by Supplier. Customer or its Affiliates shall give notification of internal changes, which could affect the Supplier Services.

5 Remedies

(i) In the event Supplier fails to meet the Service Availability as set forth below, it shall be a material breach of Suppliers obligations under the Agreement:

(a) Supplier fails to meet the Services Availability Service Level set forth in Section 2 above in any three (3) months during a rolling twelve (12) month period; and/or

(b) a Downtime event for the Services continues for a period of more than five (5) calendar days; and/or

(c) Supplier fails to meet the Latency Performance Indicators set forth in Table 3 across all transactions, calculated in aggregate over a calendar month, for more than three (3) continuous months.

(ii) If any one or more of the foregoing material contract breach events described in Section 5(i) above occurs, Customer or its Affiliates may, without limitation and in addition to all other rights and remedies, whether under equity or law, shall:

(a) have the right to claim from the Supplier or its relevant Affiliates and the Supplier a credit equal to a percentage of the annual fees as set forth in the following Table 2A (each a "Service Credit").

- (b) also have the right to terminate the Agreement or any applicable Release Order, without further liability to Supplier and/or its Affiliates (except for Services rendered prior to the termination date) upon providing to Supplier and/or its Affiliates not less than thirty (30) calendar days prior written notice of such termination, provided that such notice is given within (90) calendar days after the date upon which the Service Availability report identifying the event giving rise to the termination right occurred.

Table 2A - Service Credits

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

- (c) Service Credits may not be redeemed for cash and shall be applied to Customer's next applicable fee payment. The issuance of Service Credits sets forth Supplier's sole obligation and liability and Supplier's sole remedy for any failure to meet the Service Availability.
- (d) Notwithstanding the foregoing, Supplier has no obligation to issue any Service Credit unless Customer requests such Service Credit in writing within ten (30) days of any failure to meet the Service Availability.

Schedule 2B: Maintenance and Support

Support.

Supplier shall provide limited Level II Support (in those instances where Customer reasonably determines that a problem is likely related to the Supplier's technology) and Level III support. Customer or its Affiliates will, as between Supplier and Customer or its Affiliates, be responsible for Level I and Level II support for any Customer Users.

For the purposes of this Agreement:

"Level I Support" means: The services provided in response to an Customer User's notification of a suspected problem in the Supplier's technology.

"Level II Support" means: The services provided to a Customer User to perform an in-depth analysis of the suspected problem, attempt to recreate the problem and to provide an acceptable resolution.

"Level III Support" means: The services provided to resolve problems in the Supplier technology that are determined to be, or are highly probable to be, the result of a design or manufacturing defect in the Supplier technology or the interface between the Supplier technology and Customer components that cannot be resolved by Customer or its Affiliates, and which requires product design engineering knowledge or expertise to isolate and effect a resolution.

1 Supplier Business Hours

- (i) Supplier hours of operations are working days during published hours designated by Supplier for each geographic region.
- (ii) Supplier will provide email support Monday through Friday between 8:30 am and 8:30 pm US Eastern time zone to Customer, which includes automated email response and critical case monitoring 24 x 7, 365 days/year.

2 Customer Provided Support

- (i) Customer is responsible for providing Level I and Level II Support to Customer Users. If Customer believes the BP User problem is due to Supplier, Customer shall open an incident with Supplier via the process described in Section 1 of this Schedule 2B.
- (ii) If a Customer User contacts Supplier directly, Supplier shall refer such entity to Customer's customer care organization. In particular, Customer is responsible for de-enrolling Customer Users from mobile payment programs as well as handling all refund, chargeback and other account related requests. If Customer believes a Customer User problem is due to Supplier, then Customer shall open an incident with Supplier via the process described in Section 4. below.

3 Incident Management and Operations

Supplier and Customer shall manage any incidents and/or defects related to the Services, in accordance with the following:

3.1 Incident Management:

- (i) Incidents Detected by Supplier. If Supplier detects a Level 1 or Level 2 incident as defined by Table 3 related to the Supplier technology or Services that impacts Customer, Supplier shall notify Customer of the incident via notification and subsequent updates posted to status.spreadly.com, with the ability for Customer to subscribe to e-mail notifications when such updates are provided on the status website:
 - Supplier's Incident Management Team Supplier will update the case documentation as the incident is worked toward resolution and continue to notify Customer in accordance with Table 3.

- Upon resolution the case owner will close the case and notify BP.

(ii) Incidents Detected by Customer. When Customer detects an incident related to the Supplier technology or Services that impacts Customer and such incident falls into one of the categories specified in Table 3 below that should be reported to Supplier, Customer shall follow the following process:

- Customer may enter a case incident directly into the Supplier support system using the interface and in accordance with the instructions delivered to Customer by Supplier.
- Alternatively, Customer may contact Supplier by sending an email to support@spreadly.com . The initial Supplier contact will enter the case into the Supplier support system.
- For Level 1 or Level 2 incidents, as defined by Table 3 below, Customer may contact Supplier by calling the RedAlert Critical Phone number staffed 24x7 at (984)-444-8633. The initial Supplier contact will enter the case into the Supplier Support System.
- Once notified, Supplier will act in accordance with the response rules defined in Table 3 below using the Customer requested contact channel of email, phone, or other channel.
- Supplier will assign an internal case owner who will update the case documentation as the incident is worked toward resolution and continue to notify Customer in accordance with Table 3.
- Upon resolution the case owner will close the case and notify Global Customer.
- Customer may log into the Supplier Extranet at any time to review the status of its case.

3.2 Incident Action Items:

3.2.1 Incident Action times measure Supplier's responsiveness to reported incidents, as such it is measured from the time Customer reports or Supplier knows of the incident. Response times are set forth in Table 3 below. When submitting an incident report, Customer shall indicate the severity for initial response in accordance with the severity guidelines set forth Table 3. In the event Supplier reasonably believes the severity level assigned by Customer is incorrect, Supplier may request the level be changed, and each Party shall promptly escalate such conflicts to its management team for resolution through consultation between the parties, during which time the parties shall continue to handle the support issue in accordance with Customer's initial severity level designation.

3.2.2 First response is achieved when Supplier acknowledges the receipt of the incident to Customer. First update occurs at the time Supplier provides Customer an initial explanation or understanding of the cause of the incident. Subsequent updates are regular progress reports by Supplier on the resolution of the incident; for Level 1 and Level 2 incidents, subsequent updates will be provided to Customer as frequently as reasonably possible via status.spreadly.com, with the ability for Customer to subscribe to e-mail notifications when such updates are provided on the status website.

3.2.3 Each update shall include, at a minimum, a detailed description of the services affected, start time of the incident, current status of Supplier's repair efforts, estimated time of repair and Supplier's plan for resolution of the problem.

3.2.4 All response and escalation times are actual time clock times unless otherwise qualified as 'business hours' or 'working day'.

3.2.5 Customer understands that the Customer escalation contact may need to be reached in the agreed upon time frame for Supplier to maintain the service level specified

in this Schedule 2B.

Table 3 – Response Times

INCIDENT LEVEL	IMPACT	First Response	First Update	Target Resolution Times
1	Transaction Processing Services (including, but not limited to, validation, tokenizing, vaulting, processing) are unavailable. Issue is critical such that the Transaction Processing Services are inaccessible or the majority of its functionality is unusable. Customer may escalate Severity Level 1 issues via Red Alert service (email, phone, text) which will immediately invoke Speedy incident response teams and procedures.	15 minutes	60 minutes	As soon as commercially practicable with the highest level of urgency, but in no event more than 24 hours
2	Transaction Processing Services experience a significant Error that results in significantly impaired and degraded performance and reliability of Customer's use of the Transaction Processing Services.	15 minutes	4 hour	3 days
3	Incident or defect only impacting a single/few End Users and not having an immediate impact on ongoing operation of Customer's business. This incident level is attained for any functional or operational issue that meets none of the higher Incident Level criteria.	15 minutes	48 Business Hours	Next update

4 Incident Resolution:

(i) Supplier will use commercially reasonable efforts to provide a suitable workaround for the issue within the Target Resolution Times and will work to provide a resolution until a fix is available. A valid resolution for an incident at a specified Incident Level is a workaround that lowers the incident Level of the Incident, although the incident remains open at the lower Incident Level.

(ii) In order to understand and resolve any incident, Supplier may need detailed information from Customer as well as Customer' assistance to diagnose the problem. Customer understands that Supplier support of the service levels described in this Schedule 2 is contingent upon Customer fulfilling its responsibilities as set forth in this Schedule 2. and responding promptly to all commercially reasonable requests from Supplier relating to resolution of the incident.

5 Incident Escalation:

Escalation is the process used by Customer if any of the expectations of incident response time is not met including:

(a) First Response is not returned within specified time frame of the Incident Level and

(b) First and Subsequent update is not returned specified time frame of the Incident Level. Escalation times and contacts are set forth in Table 4 below. To request escalation of an Incident Level, Global Customer should call the RedAlert Critical Phone number at (984)-444-8633 or the named Supplier point of contact who will escalate to the relevant contact.

Table 4 – Escalation will take place as follows (applies 24 hours x 7 days per week)

Incident Level	Level	Expectation not met	ESCALATION CONTACTS	
			Supplier	Customer
1.	1st Escalation	Immediate	Customer Support	Retail Ops Support Lead
	2nd Escalation	2 hours	Manager of Support	Head of Service Delivery – Retail
	3rd Escalation	4 hours	Director of Services	Service Delivery Director
2.	1st Escalation	Immediate	Customer Support	Retail Ops Support Lead
	2nd Escalation	4 hours	Manager of Support	Head of Service Delivery – Retail
	3rd Escalation	8hours	Director of Services	Service Delivery Director
3.	1st Escalation	8 hours	Customer Support	Retail Ops Support Lead
	2nd Escalation	24 hours	Manager of Support	Head of Service Delivery – Retail
	3rd Escalation	2 days	Director of Services	Service Delivery Director

Schedule 3

Pricing and Financial Provisions

1 Charges for the Services

The charges for the services include an annual platform licensing fee and an API usage fee (together the “Base Annual Fees”) as defined in the applicable Release Order.

2 Invoices UK/US

- 2.1 The Supplier shall invoice the Charges to the Customer monthly in arrears at the start of each year of the Initial Term and each Renewal Term of the applicable Release Order in accordance with **Section 9 (Charges, Invoicing, and Payment)** of this Agreement. The Supplier shall, if so requested by the Customer, use the AP System designated by the Customer to submit any invoices.

[Either AP]

Invoices will be processed through the Customer’s AP System

If the Customer has not so designated, then invoices should be sent to the following address:

[(UK):]

BP International Limited

c/o PO Box 36. Mitcheldean. Gloucestershire. GL17 0WH

Customer contact name and email address:

Cost Centre:

GL Code:

BP Legal Entity (if different from above):

[Or (US):]

BP General Invoices

Unless otherwise advised by Customer, all invoices will be submitted directly to the email address, postal address or fax number noted in the ‘send original invoice to’ details on the PURCHASE ORDER, or if Supplier is e-enabled, electronically via P2P or Customer’s internet-based marketplace.

Customer contact name and email address:

Paykey number:

BP Legal Entity (if different from above):

- 2.2 Each invoice shall in addition contain, as a minimum:

- 2.2.1 a description of the Services to which the invoice relates and the Release Order BP reference number, if one is applicable;
- 2.2.2 the number of days or hours worked and a description of the work performed by day by each relevant Supplier Personnel to the extent that the Services are delivered on a time and materials basis and an itemisation of all other costs;
- 2.2.3 identification of any VAT or equivalent sales tax and explanation of the nature of such charges for Services provided outside the EU;
- 2.2.4 any import duty, if applicable;

- 2.2.5 a VAT (or if applicable sales tax) registration number;
- 2.2.6 any service level credits due to the Customer together with a report on service level failures to which such service level credits relate; and
- 2.2.7 any other information that is reasonably requested by the Customer.
- 2.2.8 The following requirements will be met for emailed invoices:
 - Invoices will be in portable document format (pdf) or tagged image format (tif), and not encrypted;
 - There will be only one (1) file attached per email and only one (1) invoice per file. Additional files, including logo or letterhead graphics will result in the invoice not being processed for payment;
 - The invoice will be the first page of the attachment with supporting documents following;
 - The total size of the email (attachment plus text) should not exceed twenty-five (25) megabytes;
 - The attachment name will be less than or equal to fifty (50) characters.

2.3 Payment of Charges

2.3.1 All payment of Charges shall be made in accordance with **Section 8 (Taxes)** and **Section 9 (Charges, Invoicing, and Payment)** of this Agreement.

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

ACH payment or wire transfer to the following account:

Receiver:	Silicon Valley Bank
ABA/Routing #:	121140399
SWIFT Code:	SVBKUS6S
Beneficiary:	3301451580
	Spreedly, Inc.
	300 Morris St, Suite 400
	Durham, NC 27701
	USA

Check delivered to the address specified in the relevant invoice.

2.3.3 All payments due under this Global Agreement shall be payable in United States dollars.

Schedule 4 Policies

Any reference in a Policy to “BP”, “BP group” or similar references shall be deemed to be a reference to the Applicable Customer and its Affiliates and any reference in a Policy to the “contractor”, a “business partner” or similar reference shall be deemed to be a reference to the Applicable Supplier and its Affiliates.

Mandatory Policies are as follows:

- A. Code of Conduct
- B. International Trade Regulation
- C. Anti-Corruption & Anti-Money Laundering Compliance
- D. Business and Human Rights
- E. Digital Security & ISRS
- F. Data protection and GDPR (including an indemnity for breach)
- G. Audit
- H. Minimum Requirements on Health, Safety, Security and Environment
- I. Business Continuity Planning (BCP)

A. CODE OF CONDUCT

1.1. Supplier confirms that it has carefully reviewed the Applicable Customer’s Code of Conduct which is available at the www.bp.com website. Without limiting any of Supplier’s other obligations Supplier shall, and shall procure that Supplier Personnel shall, at all times in performing their obligations under the Agreement and each Release Order:

- 1.1.1. act consistently with the applicable principles of the Applicable Customer’s Code of Conduct set out at www.bp.com as amended from time to time; and
- 1.1.2. comply with, have the rights and accept the obligations set out in all other policies of the Applicable Customer and its Affiliates referred to in the Agreement or relevant Release Order as such policies are amended from time to time.

Failure to comply with this provision will constitute a material default giving rise to a right of termination by Applicable Customer pursuant to clause 20.1.1 of the Agreement.

B. APPLICABLE LAWS INCLUDING TRADE LAWS

All capitalized terms used in this section which are not otherwise defined shall have the meaning set forth below, unless otherwise defined in the Agreement.

“Applicable Laws” means any applicable laws, codes, legislative acts, regulations, ordinances, rules, rules of court, and orders, as amended from time to time, including

- (a) statutes (including regulations enacted under those statutes);
- (b) international, national, regional, provincial, state, municipal, or local laws;
- (c) judgments and orders of courts of competent jurisdiction;
- (d) rules, regulations, and orders issued by an authority;
- (e) regulatory approvals, permits, licences, approvals, and authorisations by an authority; and
- (f) Trade Laws.

“Trade Laws” means any Applicable Laws of the European Union, United Kingdom, United Nations, United States and other applicable jurisdictions regarding export controls and economic sanctions or restrictions including those that:

- (a) prohibit or restrict the export or import of Goods, Services, software and technology to or from persons and countries specified therein, including the provision of Services by designated persons;

(b) would expose Supplier or Applicable Customer to punitive measures for violation.

- 2.1 Supplier shall supply the Services under the Contract in accordance with all Applicable Laws.
- 2.2 Supplier shall not take any action or make omissions that would cause BP and/or any BP Affiliate to violate Trade Laws or be subject to sanctions, fines or penalties under Applicable Laws.
 - 2.2.1 If Supplier takes any action or performs any part of the supply in violation of Applicable Laws, or takes any action or makes omissions that would cause BP or any BP Affiliate to violate Trade Laws or be subject to sanctions, fines or penalties under Applicable Laws, Supplier shall bear any fines or penalties or additional costs resulting from such violation subject to the provisions of the Agreement.
 - 2.2.2 All costs for compliance with Applicable Laws connected with supply of the Services will be for the account of Applicable Customer, unless otherwise provided for in the Agreement.
- 2.3 Applicable Customer shall provide Supplier upon request with relevant end-use, end-user and country of end-use information with respect to the Services (including software or technology) to be supplied hereunder. Based on and in reliance on such information, Supplier will supply such items in compliance with Trade Laws. The Parties acknowledge that any change in end-use, end-user or country of end-use may be restricted or prohibited by Trade Laws.
- 2.4 At or before the Services commences, if required by applicable law, Supplier shall give notice to Applicable Customer any Services (including software or technology) that are controlled under applicable Trade Laws, including the jurisdiction of origin and any jurisdiction in which work is performed, and Supplier shall provide the applicable export control number, export control classification number or other similar export designation (if any).
- 2.5 Supplier shall promptly give notice to Applicable Customer of any breach or potential breach of Trade Laws.
- 2.6 Supplier shall indemnify Applicable Customer from and against all claims/losses for breach of the following, if connected with the performance or non-performance of the Agreement:
 - (a) Trade Laws, by Applicable Customer; and
 - (b) Supplier's obligations under clause 2.2 not to take any action or make omissions that would cause Applicable Customer to violate Trade Laws.
- 2.7 Notwithstanding the above and except as provided in clause 2.2 above, nothing in the Agreement is intended or should be construed to require Supplier or Applicable Customer to act or fail to act if such action or failure to act would be inconsistent with or penalised by the Applicable Laws of:
 - (a) Supplier's or Applicable Customer's country of incorporation; and/or
 - (b) the country of incorporation of any direct, indirect or ultimate parent company of Supplier or Applicable Customer.
- 2.8 Applicable Customer shall have the right to terminate this Agreement immediately if Supplier is found to have violated the applicable Trade Laws.
- 2.9 The 'United Nations Convention for the International Sale of Goods' is expressly excluded.

C. COMPLIANCE WITH LAWS AND ANTI-BRIBERY AND CORRUPTION

- 3.1** Supplier shall and procure that its Affiliates, subcontractors and Supplier Personnel shall throughout the term of the Contract and/or relevant Order, comply with:
- (a) all applicable export control, trade sanctions and other foreign trade control laws, rules and regulations including those of the territories where services are to be performed or goods to be supplied and the US Export Administration Regulations (the "Trade Restrictions");
 - (b) all applicable anti-bribery and corruption and anti-money laundering laws, rules, regulations or equivalent of the UK, the US and all locations where Services are provided including, the UK Bribery Act 2010 and the Foreign Corrupt Practices Act 1977 of the United States of America (regardless of whether Supplier is otherwise subject to those laws); and
 - (c) all other laws at all times relating to the performance of its obligations hereunder.
- 1.1.3. Supplier shall obtain and maintain throughout the Term, at its own cost, all the consents, licences and permissions it may require and which are necessary to enable the performance of its obligations under the Agreement and each Release Order.
- 1.1.4. Supplier shall ensure that Supplier attend such training, including on Applicable Customer's Code of Conduct, as directed by Applicable Customer from time to time.

3.2 Trade Restrictions

- 3.2.1** Supplier represents and warrants that to the best of its knowledge, it, its Affiliates, subcontractors and Supplier Personnel are not persons who are identified from time to time by any government or legal authority as a person with whom trade or financial dealings and transactions by either Supplier or Applicable Customer and/or their respective Affiliates are prohibited or restricted.
- 3.2.2** Failure to comply with the Trade Restrictions shall constitute a material breach of the Agreement and/or each relevant Release Order.
- 3.3 Anti-Bribery and Corruption**
- 3.3.1** Supplier acknowledges that Applicable Customer has a zero tolerance policy towards bribery and corruption including towards facilitation payments and grease payments.
- 3.3.2** Supplier agrees, undertakes and confirms that it, its Affiliates and Supplier Personnel have not and will not make, offer, promise to make or authorise the making to any person or solicit, accept or agree to accept from any person, either directly or indirectly, anything of value including without limitation gifts or entertainment, facilitation payments or grease payments, in order to obtain, influence, induce or reward any improper advantage in connection with the Agreement or any Release Order or where to do so would breach any applicable anti-corruption or anti-money laundering laws or regulations (the "Anti-Corruption Obligation").
- 3.3.3** Supplier shall on an on-going basis:
- a) notify Applicable Customer in writing promptly upon discovery of any actual or suspected breach of the Anti-Corruption Obligation; and
 - (b) inform all Supplier Personnel that they are required to act in accordance with the Anti-Corruption Obligation.
- 3.3.4** In accordance with Customer's audit rights in Section 7.3.4, Supplier shall, throughout the Term and for at least one (1) year following its expiration or termination:

- (a) permit Applicable Customer to inspect Supplier's records in the manner and frequency permitted under the Agreement to verify compliance with this Clause; and
 - (b) upon request cooperate and provide all reasonable assistance to enable Applicable Customer to ensure and monitor compliance with the Anti-Corruption Obligation.
- 3.3.5** Failure to comply with the Anti-Corruption Obligation shall constitute a material breach of the Agreement and/or each relevant Release Order.

D. BUSINESS AND HUMAN RIGHTS

- 4.1** Supplier confirms that it has carefully reviewed the BP Business and Human Rights Policy which is available at the www.bp.com website. In connection with Supplier's performance of the Agreement and consistent with the policy, Supplier shall conduct its business in a manner that respects the rights and dignity of all people and internationally recognised human rights, including without limitation:
- (a) not employing, engaging or otherwise using forced labour, trafficked labour or child labour; nor engaging in or condoning abusive or inhumane treatment of workers;
 - (b) providing equal opportunities, avoiding discrimination and respecting freedom of association of workers, in each case within the relevant national legal framework; and
 - (c) mitigating or avoiding adverse impacts to communities arising from Supplier's activities to the extent practicable.
- 4.2** Failure to comply with this provision may constitute a material breach of the Agreement and/or each relevant Release Order..

E. DIGITAL SECURITY

Contents

[Introduction](#)47

[1 Terms and Definitions](#)47

[2 Information Security Requirements](#)48

(a) Introduction

The Supplier shall comply with this Information Security Requirements for Suppliers schedule (“ISRS”) in relation to the Supplier’s performance of the Services, including the handling, storing, and processing of Customer Data and/or access to the Customer’s Systems.

This schedule is aligned to the NIST framework that supports the US Executive Order 13636 – Improving Critical Infrastructure Cybersecurity.

1 Terms and Definitions

- 1.1 In this Part, the following terms shall have the meanings set out below. All other capitalised terms shall have the meanings set out in the Global Agreement.
- 1.2 **Account Owner** – means the Supplier Person who uses an account or, in the case of System Accounts, who is responsible for its usage.
- 1.3 **Automation Systems** – means automation or other related systems required for safe compliant and reliable operations.
- 1.4 **Secret** – means Confidential Information of high value or sensitivity where unauthorised disclosure could cause serious damage to the Customer or the Customer Affiliates. Examples of Secret information would include, but not be limited to, takeover plans, unpublished company results for the Customer or the Customer Affiliates and assessments of exploration opportunities.
- 1.5 **Confidential** – means Confidential Information where unauthorised disclosure could be prejudicial to the interests of the Customer or the Customer Affiliates or cause significant difficulty or embarrassment to the Customer or its employees. Examples of Confidential information would include, but not be limited to, Personal Data, information supporting contract negotiations, trading strategies and technical data relating to the Customer or Customer Affiliate’s Upstream segment.
- 1.6 **Multi-Factor Authentication** – means authentication that requires both something that only the User knows, such as a password and also something the User has, such as a token or certificate.
- 1.7 **OWASP** – means Open Web Application Security Project.
- 1.8 **Privileged Account** – means any account that has elevated entitlements to systems, network devices or applications.
- 1.9 **System Account** – means any account used to run specific services on a system and allow system to system communication without User involvement.
- 1.10 **User** – means an individual that accesses a system using an account.
- 1.11 **UserID** – means a unique system identifier used to identify a User.

2 Information Security Requirements

2.1 Compliance Requirements

- 2.1.1 The Supplier shall conduct an annual compliance assessment against the requirements in this ISRS that shall be made available to the Customer upon request. The Supplier may rely on existing independent third-party audit reports or certifications (e.g. annual PCI-DSS Level 1 certification audit by an independent third-party Quality Assurance Inspector and SOC-2 Type 2 certification) where the security requirements are equivalent to those contained in the ISRS.
- 2.1.2 The Supplier shall support the Customer and/or the Customer's agent in assessing the Supplier's compliance with the ISRS by providing access to documentation and resources as required to support these requirements.

2.2 Asset Management

- 2.2.1 The Supplier shall maintain an inventory of all IT assets and automation system assets supporting the Services. This shall include, but is not limited to, internal and external systems, physical devices, software platforms, applications, databases and third-parties (e.g. suppliers, sub-contractors). The Supplier shall provide this inventory to Customer on request.
- 2.2.2 The Supplier shall, and shall procure that its Affiliates and subcontractors shall, establish and maintain clear security roles and responsibilities, including information security and physical security.

2.3 Governance

- 2.3.1 The Supplier shall appoint a named individual with overall responsibility for information security and provide the Customer with a contact to escalate operational security issues or incidents, via the email address DS_SupplierSecurityC@uk.bp.com.
- 2.3.2 The Supplier shall implement and maintain an information security policy that is substantially the same as current industry standards such as the NIST Framework, ISF Standard of Good Practice or ISO27001/2.
- 2.3.3 Where IT systems are in scope of PCI-DSS, the Supplier shall maintain compliance with the currently applicable version of the Payment Card Industry Data Security Standard as published by the PCI Security Standards Council. The Supplier shall co-operate with BP's requirements for PCI QSA audits and site visits.
- 2.3.4 The Supplier does not operate or maintain automation systems as part of the Services provided to the Customer..
- 2.3.5 If the Services contain cloud-hosted services, the cloud-hosted services shall be subject to the applicable security requirements defined herein. The Supplier shall obtain independent third-party assurance at least annually that cloud-hosted services are operated in accordance with the ISRS or to an equivalent level of security (E.g. CSACCM, ISO27017, ISO27001).
- 2.3.6 For the avoidance of doubt, the Supplier is responsible for the performance of all subcontractors, including cloud-service providers and shall procure that all subcontractors shall have contracts with substantially similar obligations as set out herein. In addition, the Supplier shall meet all of their responsibilities under any applicable shared responsibility models provided by their cloud service providers.

2.4 Risk Management

- 2.4.1 The Supplier shall conduct an information security risk assessment on at least an annual basis and manage risks to Confidential information and IT systems supporting the Services in accordance with documented risk management procedures.
- 2.4.2 The Supplier shall establish and maintain risk management processes to identify, assess and manage risks to Confidential Information and IT systems supporting the Services. The Supplier shall report material risks to the Customer promptly.
- 2.4.3 The Supplier shall conduct penetration testing of its internet-facing systems on at least an annual basis using independent testing professionals who are accredited to a recognised standard (e.g. CREST, Tigerscheme, CHECK). The Supplier shall ensure that identified vulnerabilities are remediated promptly.
- 2.4.4 If the Supplier is required to process Secret information as part of the Services, then it shall be required to conduct penetration testing of its systems and provide evidence of such testing to the Customer prior to the processing of Secret information.
- 2.4.5 If the Supplier is developing, managing or hosting Customer or Customer Affiliate systems, the Supplier shall allow the Customer to check that the Supplier has completed penetration testing and provide commercially reasonable and limited access to documentation, systems and resources as required.

2.5 Access Control

- 2.5.1 The Supplier shall restrict physical and logical access to Confidential information and IT systems supporting the Services to the minimum levels of access and privileges required to perform a function or role.
- 2.5.2 The Supplier shall assign every User account an Account Owner, who is accountable for its rights and responsibilities. Every action performed under a User account shall be traceable to an individual.
- 2.5.3 The Supplier shall immediately revoke all access for Supplier Personnel no longer working on the Services or those that no longer require access.
- 2.5.4 The Supplier shall maintain records of all Supplier Users with access to Customer information and systems.
- 2.5.5 The Supplier shall review User accounts and their privileges on a regular basis to verify that access permissions are appropriate and remove access that is no longer required. Privileged Accounts shall be reviewed on at least a six-monthly basis.
- 2.5.6 The Supplier shall enforce the use of strong passwords and protect passwords from unauthorised access and interception.
- 2.5.7 The Supplier shall restrict the use of Privileged Accounts to authorised individuals performing system administration activities.
- 2.5.8 The Supplier shall only use System Accounts for system-to-system communication and shall configure them to prevent interactive logins from Users.
- 2.5.9 The Supplier shall ensure that remote access to IT systems and networks supporting the Services shall be restricted to only authorised individuals using secure entry-points and approved devices.
- 2.5.10 The Supplier shall design all networks to protect network integrity and separate network zones with a firewall or equivalent that enforces a policy that restricts traffic to only authorised business traffic. The Supplier shall review firewall policies on at least an annual basis.

- 2.5.11 If the services provided under this agreement are in-scope of legal and regulatory requirements (e.g. NIS-D/NIS-R, SOX etc.) The Supplier shall use only corporately managed devices to access Customer networks and information systems.
- 2.5.12 If Supplier Users require BP credentials to provide the service, Supplier shall ensure all applicable Users are registered for and employ BP Multi-Factor Authentication and password reset mechanisms and comply with BP policies and guidelines, as updated from time to time.

2.6 Awareness and Training

- 2.6.1 The Supplier shall procure that all Supplier Personnel complete information security awareness training and be made aware of their responsibilities with regards to information security and the handling of Confidential information at least annually.
- 2.6.2 The Supplier shall provide Privileged Users with specific training for their role and make them aware of their specific information security responsibilities.
- 2.6.3 The Supplier shall provide Supplier Personnel with clear instructions and awareness for using Confidential information and IT systems, including but not limited to, the following requirements:
 - 2.6.3.1 Keep Confidential information and IT equipment secure at all times, including when travelling or working out of the office or from home;
 - 2.6.3.2 Keep UserIDs, passwords and PINs for IT systems and devices, confidential and protect them from unauthorised access;
 - 2.6.3.3 Do not connect untrusted removable media devices to IT systems or laptops;
 - 2.6.3.4 Keep devices used to access Confidential information and IT systems up-to-date with security updates;
 - 2.6.3.5 Handle Confidential information in accordance with its classification and documented handling procedures;
 - 2.6.3.6 Only share Confidential information with authorised individuals on a need-to-know basis. Secret information shall only be shared with individuals authorised by the Customer to handle Secret information;
 - 2.6.3.7 Do not email Secret information;
 - 2.6.3.8 Confidential information must be encrypted when emailing or sharing externally;
 - 2.6.3.9 Checking, before sending emails containing Confidential information, that all the recipients are authorised to receive the Confidential information;
 - 2.6.3.10 Be aware of phishing and ransomware attacks and do not click on links in emails or documents or provide any Confidential information over the phone without verifying the caller;
 - 2.6.3.11 Do not use personal instant messaging services, personal email accounts or personal applications to conduct Customer business or to share or receive Confidential information;
 - 2.6.3.12 Be discreet when discussing Confidential information so you cannot be overheard and do not share Confidential information online, including using the social media, external social networks instant messaging or blogging sites;
 - 2.6.3.13 Maintain a clear desk and a clear screen so that Confidential information cannot be viewed or accessed by unauthorised individuals;
 - 2.6.3.14 Do not leave sensitive Confidential information unattended or on voicemails;

2.6.3.15 Securely dispose of paper and other media using correct procedures. Secret information shall be disposed of using a cross-cut shredder; and

2.6.3.16 Report confirmed or suspected information security incidents and non-compliance with this Part of the Global Agreement promptly and without delay.

2.7 Data Security

2.7.1 The Supplier shall implement full-disk encryption on portable devices accessing or holding Confidential information.

2.7.2 The Supplier shall develop and configure applications and databases, and devices to protect the confidentiality, integrity and availability of Confidential information. This shall include:

2.7.2.1 Implementation of access control, Authentication and session-management;

2.7.2.2 Performance of input and output data validation checks;

2.7.2.3 Not revealing system information in end-user error messages;

2.7.2.4 Protecting Confidential information, including using cryptography where required;

2.7.2.5 Time-out for User connections after a period of inactivity; and

2.7.2.6 logging of User activity so that actions can be traced to an individual.

2.7.3 The Supplier shall encrypt Secret and Confidential information in storage and in transit.

2.7.4 The Supplier shall establish and maintain procedures and controls to protect the security of Confidential information at every stage of its lifecycle from creation through processing, storage and disposal. This shall include secure sanitisation and disposal of devices holding Customer information.

2.7.5 [Intentionally omitted].

2.7.6 The Supplier shall manage source-code in accordance with documented procedures that restrict access and verify the integrity of code prior to deployment.

2.7.7 If the Supplier is performing application development, it shall implement separate environments for production, development and testing and implement separation of duties.

2.7.8 The Supplier shall not use Confidential information for testing without the prior consent of the Customer.

2.8 Information Protection Processes and Procedures

2.8.1 The Supplier shall implement systems and end-user devices using standardised builds that include a hardened operating system, malware protection, host-based security software and systems that are patched against known vulnerabilities prior to deployment.

2.8.2 The Supplier shall develop IT systems and applications in accordance with a secure development methodology that includes a security risk assessment and requirements to protect the confidentiality, integrity and availability of Confidential information.

2.8.3 If the Supplier is developing web applications, it shall develop them in accordance with the OWASP top ten (10) pro-active controls, as published by OWASP from time to time and verify that web applications are configured to protect against the OWASP top ten (10) vulnerabilities.

2.8.4 Configuration changes shall be made by authorised individuals in accordance with documented change management procedures and using approved systems and tools.

- 2.8.5 The Supplier shall backup Confidential information and IT systems as required to meet Customer continuity requirements, including the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, in accordance with tested backup and restore procedures. The Supplier shall protect backups from loss, damage and unauthorised access.
- 2.8.6 The Supplier shall implement procedures to securely delete Customer information from IT systems and devices in accordance with current industry standards such as NIST 800-88 or an equivalent.
- 2.8.7 The Supplier shall monitor the effectiveness of information security controls and continuously improve controls and processes as required.
- 2.8.8 The Supplier shall monitor CERT notifications that may affect any element of the Supplier's IT systems and patch systems in accordance with a documented procedure that prioritises the remediation of vulnerabilities based on risk.

2.9 Maintenance

- 2.9.1 The Supplier shall maintain IT systems in a timely manner in accordance with change management procedures.
- 2.9.2 The Supplier shall restrict access for remote maintenance to authorised Users performing approved maintenance, using authorised devices and tools.

2.10 Protective Technology

- 2.10.1 The Supplier shall securely collect, monitor and retain event logs so that access to Confidential information and systems can be traced. The Supplier shall provide logs to the Customer upon request.
- 2.10.2 The Supplier shall only use removable media to handle Confidential information that is both hardware encrypted and protected by a password.
- 2.10.3 The Supplier shall implement identity and access management systems to control access and authenticate Users prior to granting access.
- 2.10.4 The Supplier shall use Multi-Factor Authentication for access to systems holding Secret information, for remote User virtual private network access and administration of core infrastructure.

2.11 Security Continuous Monitoring

- 2.11.1 The Supplier shall collect and correlate security events from systems and sensors to identify information security incidents and cyber-attacks.
- 2.11.2 The Supplier shall analyse security events to identify cyber-attacks and possible attack methods. The Supplier shall promptly investigate suspected and confirmed attacks and report them to soc@bp.com.
- 2.11.3 The Supplier shall implement security monitoring to protect against data leakage, malicious intrusions and prevent malicious software from being downloaded by Users.
- 2.11.4 The Supplier shall install and maintain malware protection software on end-user devices and servers to identify malware, malicious code and unauthorised mobile code.
- 2.11.5 The Supplier shall monitor for unauthorised personnel, connections, devices and software.
- 2.11.6 The Supplier shall conduct vulnerability scans against infrastructure and applications in accordance with their risk to the Customer, to identify and remediate any security vulnerabilities and misconfiguration.

2.12 Detection Processes

- 2.12.1 The Supplier shall establish security detection processes that are tested and continuously improved including clear roles and responsibilities for security monitoring and detection activities.
- 2.12.2 The Supplier shall assess security events and suspected incidents against defined criteria and respond to incidents in accordance with their potential impact to the Customer and the Customer Affiliates.

2.13 Response Planning

- 2.13.1 The Supplier shall report any confirmed security incidents or data breaches affecting Customer systems or Customer data to the Customer promptly and without delay to soc@bp.com.
- 2.13.2 The Supplier shall maintain security incident response plans to manage the response to incidents and shall test the security incident response plans on at least an annual basis.
- 2.13.3 The Supplier shall consult with the Customer prior to conducting forensic investigation following an incident and conduct any investigations in accordance with legal requirements for preserving evidence.
- 2.13.4 The Supplier shall contain and mitigate incidents in accordance with documented incident management procedures and response plans.
- 2.13.5 The Supplier shall mitigate newly identified vulnerabilities. Any vulnerabilities that cannot be fixed, that could have an impact on the security of Confidential information shall be reported to the Customer immediately.
- 2.13.6 If an actual incident as outlined above occurs, the Supplier shall conduct post incident reviews to identify root-causes and identify actions required to minimise the risk of similar incidents re-occurring. Response strategies and plans shall be updated in response to any lessons learned.

2.14 Recovery Planning

- 2.14.1 The Supplier shall develop and maintain security recovery plans that are executed during or after an event and restore systems affected by cyber security events.
- 2.14.2 The Supplier shall test security recovery plans on at least an annual basis and shall update recovery strategies and plans in response to testing and any lessons identified by post incident reviews.
- 2.14.3 The Supplier shall agree specific external communication requirements in response to a cyber-attack or data breach affecting Customer systems or data with Customer.

E. DATA PROTECTION

Where the Supplier is processing personal data as defined below, (Data Protection) in the course of providing the Services, the Supplier shall comply with all of its obligations set out below in Data Protection.

DATA PROTECTION

1. For the purposes of this Schedule:
 - 1.1 “**data controller**” means the person which, alone or jointly with others, determines the purposes and means of the processing of personal data;
 - 1.2 “**data processor**” means the person which processes personal data on behalf of the data controller;
 - 1.3 “**encryption**” means the process of converting information into an unintelligible form except to the holders of a specific encryption key;
 - 1.4 “**personal data**” means any information relating to an identified or identifiable natural person that is processed by the [Contractor/Supplier] as a result of, or in connection with, the provision of the supply of Goods and Services as applicable.; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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; and
 - 1.5 “**processing**” means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking erasure or destruction.
2. The Supplier acknowledges that the contracting Applicable Customer is the data controller in respect of any personal data that the Supplier processes on Applicable Customer’s behalf in the course of providing the Services and that the Supplier is a data processor of such data.
3. The Supplier agrees that it shall (and shall procure that each of its affiliates and Sub-contractors shall):
 - 3.1 only carry out processing of personal data in accordance with Applicable Customer’s instructions (which may be specific instructions or instructions of a general nature as set out

in this Agreement or as otherwise notified by Applicable Customer to the Supplier during the term of this Agreement) unless required to do so by European Union or Member State law (in which case, the Supplier shall inform Applicable Customer of that legal requirement before processing, unless that law prohibits the informing of Applicable Customer on important grounds of public interest);

- 3.2 implement appropriate technical and organisational measures against the accidental, unauthorised or unlawful access to, or processing, destruction, loss, alteration, damage or disclosure of personal data (these measures shall include, but are not limited to, the deployment of appropriate encryption solutions to protect personal data);
- 3.3 ensure that the technical and organisational measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing and accidental loss, destruction or damage to the personal data and having regard to the nature of the personal data which is to be protected;
- 3.4 ensure the reliability of any employees who have access to personal data and that all employees involved in the processing of personal data are bound under an appropriate obligation of confidentiality and have undergone adequate training in the care, protection and handling of personal data;
- 3.5 unless legally barred, promptly refer to Applicable Customer any queries in relation to the personal data from individuals, any data protection authority, any law enforcement authority or from any court, tribunal, regulator or government body for Applicable Customer to resolve;
- 3.6 at no additional cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to Applicable Customer as Applicable Customer may reasonably require, to allow Applicable Customer to comply with (i) the rights of individuals under applicable data protection laws, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and (ii) with information or assessment notices served by any data protection authority;
- 3.7 notify Applicable Customer, without undue delay, of any unauthorised or unlawful processing or any accidental loss, destruction, damage, alteration or disclosure of personal data (each a "security incident") and, in relation to each security incident and suspected security incident, it shall promptly investigate the security incident, provide Applicable Customer with detailed information about the security incident; and take reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the security incident;
- 3.8 not process or permit the processing of personal data outside the European Economic Area other than with the prior written consent of Applicable Customer and, where such consent is granted, the Supplier undertakes to enter into a suitable agreement with Applicable Customer and/or any relevant parties and/or adopt any necessary measures in order to ensure an adequate level of protection with respect to the privacy rights of individuals;
- 3.9 implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of personal data;
- 3.10 at no additional cost, assist Applicable Customer in complying with its obligation, where applicable, to undertake a data protection impact assessment;
- 3.11 maintain a record of all categories of processing activities carried out on behalf of Applicable Customer which shall be made available to Applicable Customer upon request; and
- 3.12 upon reasonable request of Applicable Customer, the Supplier agrees to (i) allow for and contribute to audits; and (ii) to submit for inspection, data files and documentation needed for

processing personal data and all other necessary information (and/or those of its agents, affiliates and Sub-contractors) to reviewing, auditing and/or certifying, by Applicable Customer (or any independent or impartial inspection agents or auditors, selected by Applicable Customer and not reasonably objected to by the Supplier) to demonstrate compliance with its obligations in this Schedule, with reasonable notice and during regular business hours.

- 4 If any part(s) of the personal data ceases to be required by the Supplier for the performance of its obligations under this Agreement, or on termination or expiry of the Agreement (whichever is earlier), the Supplier shall at the express choice of Applicable Customer (but not otherwise), either return to Applicable Customer all personal data that has been obtained or collected in providing the Services under this Agreement, or delete or destroy all copies of the personal data in the Supplier's possession or control and certify to Applicable Customer that it has done so, unless legislation or rule by the Card Associations imposed upon the Supplier prevents the return or destruction of all or part of the personal data. In that case, the Supplier shall continue to ensure the confidentiality of personal data in its possession and will not actively process such data any further.
- 5 The Supplier may only sub-contract or outsource the processing of personal data under this Agreement to any other person or entity ("**Sub-contractor**") if the Supplier:
 - 5.1 has provided reasonable prior notice to Applicable Customer of the identity and location of the Sub-contractor and a description of the intended processing to be sub-contracted or outsourced to the Sub-contractor to enable Applicable Customer to comply with the applicable data protection laws, and to evaluate any potential risks to the personal data;
 - 5.2 remains fully liable to Applicable Customer for the Sub-contractor's performance of this Agreement as well as for any acts or omissions of the Sub-contractor in regard of its processing of personal data;
 - 5.3 has received Applicable Customer's prior written consent to the sub-contracting or outsourcing; and
 - 5.4 has imposed legally binding contract terms and conditions substantially the same as those contained in this Schedule on the Sub-contractor ("**Sub-contractor Contract**").
- 6 Applicable Customer may require the Supplier by notice in writing to cease or suspend the sub-contracting or outsourcing of the processing of personal data to the Sub-contractor if, in Applicable Customer's reasonable opinion, the Sub-contractor is unable to comply with the terms of the Sub-contractor Contract.
- 7 The duration of processing of personal data shall be for the term of this Agreement, save to the extent where the processing of such personal data is otherwise required by European Union law or Member State law.
- 8 The nature and purpose of the processing of personal data by the Supplier where Supplier acts as a Data Processor including the categories of data subjects and the types of such personal data which will be processed are set out in this Agreement in particular in Annexure A.
- 9 The parties shall agree to amend this Schedule as required to enable them to comply with the provisions of the General EU Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016).

ANNEXURE A TO THE BASIC CLAUSES

A) General - subject matter of the processing:

The context of the processing of BP personal data is the performance of the following tasks on behalf of BP:

See Section 9 of Schedule 2 of this Agreement.

B) Nature and purpose of processing:

See Section 9 of Schedule 2 of this Agreement.

C) Personal data in scope:

The following types/categories of personal data may be used:

See Section 9 of Schedule 2 of this Agreement.

D) Persons affected (i.e. the data subjects):

The group of data subjects affected by the processing of their personal data is:

See Section 9 of Schedule 2 of this Agreement.

F. AUDIT

- 1.1 Applicable Customer shall have the right to audit the relevant Supplier records to verify compliance with this Schedule 4 in a manner and frequency as provided in Clause 7.3.4 of the Agreement.
- 1.2 Supplier shall co-operate fully in the conduct of such inspections and audits.

G. MINIMUM REQUIREMENTS ON HEALTH, SAFETY, SECURITY AND ENVIRONMENT

1 Introduction

Supplier is a financial technology company providing services over the internet. As a result of Supplier's service model, Supplier is rarely, if ever, required to perform work on-site at a customer facility. If such work becomes necessary, the Parties agree to outline the precise nature and scope of such work to be performed in a Release Order.

The following minimum health, safety, security and environmental ("**HSSE**") requirements and such further requirements as are described in a valid Release Order shall apply to the Supplier and its subcontractors when performing work on the Customer's sites or facilities and exclusively for the Customer at Supplier work sites. The Supplier shall ensure that any subcontractor whom it engages meets the HSSE requirements set out in this document (the "**Minimum HSSE Requirements**"). The Supplier shall ensure that its subcontractor keeps the Supplier fully informed and makes the required notifications to the Supplier in relation to these Minimum HSSE Requirements.

The Supplier shall take any additional precautions necessary to prevent harm to personnel or damage to property and/or the environment in the performance of Services for the Customer.

2 Definitions

The following terms in the Minimum HSSE Requirements have the meanings set out below. All other capitalised terms not otherwise defined herein shall have the meanings set out in this Agreement.

- 1.3 "Incident" shall refer to any injury or illness that is work related under the Occupational Safety and Health Act of the United States, or similar law or statute applicable in other countries where the Customer engages the Supplier under this Agreement;
- 1.4 "Days Away from Work Case" shall mean a work related injury or illness which has either of the following consequences:
 - 1.4.1 The member of the workforce could not have worked on any day after the injury or illness, irrespective of whether there was scheduled work; or
 - 1.4.2 The member of the workforce comes to work even when a physician or other licensed healthcare professional recommends that the individual stays at home.

2 Minimum HSSE Requirements

- 2.1** The Supplier shall comply with applicable HSSE laws and standards of governmental or regulatory agencies having jurisdiction at locations where work is performed for the Applicable Customer and demonstrate that there is an appropriate process in place to identify and ensure such compliance.
- 2.2** [Intentionally Omitted]
- 2.3** In respect of HSSE, the Supplier shall ensure that key advisory and management roles are performed by personnel having an appropriate level of skills, qualifications and experience.
- 2.4** [Intentionally Omitted]
- 2.5** [Intentionally Omitted]
- 2.6** [Intentionally Omitted].
- 2.7** [Intentionally Omitted]

- 2.8** The Supplier shall report and document all identified potential hazards, unsafe conditions, and unsafe acts through a near-miss program in relation to work carried out on the Applicable Customer's sites. All near-miss reports will be provided to the Applicable Customer's authorised representative.
- 2.9** The Supplier shall provide appropriate personal protective equipment ("PPE") to all personnel. The Supplier shall ensure appropriate PPE is used by all personnel provided by or on behalf of the Supplier (the "Supplier's Personnel") as required by the Applicable Customer's safety policies in relation to work carried out on the Customer's sites. Steel-toed safety shoes, hard hats, safety glasses, and additional PPE (e.g., flame resistant clothing ("FRC"), hearing protection, respiratory protection, face shields, fall protection, hand protection, etc.) may be required by the nature of the work and/or as specified by applicable law and Applicable Customer policy for identified tasks.
- 2.10** The Suppliers shall report headcount hours and kilometres driven on a **monthly** basis to the Applicable Customer's Authorised Representative. Headcount hours will include only those of the Supplier's and its subcontractor's employees working at the Applicable Customer's sites. Kilometres driven will include only work related driving.
- 2.11** The Supplier shall immediately notify the Customer's authorised representative of all business travel incidents where such travel has been conducted by the Supplier's Personnel in connection with the Services or this Agreement and involves personal injury, damage to property, or incidents with possible infractions of applicable law in relation to environmental protection.
- 2.12** If a fatality, Days Away from Work ("DAFW") case, or environmental incident requiring a report to a regulatory agency occurs in relation to work carried out on the Applicable Customer's sites, the Supplier's senior management will meet with the Applicable Customer business unit leadership team as a matter of priority to review the incident and discuss plans to prevent recurrence.
- 2.13** For all DAFW cases, the Supplier shall investigate and report its findings in a timely manner to the Customer's authorised representative. An investigation will also be conducted for all recordable, first aid, and significant near-miss cases, and the findings shall be reported to the Applicable Customer's authorised representative. The investigation should identify contributing/root causes associated with the incident as well as proposals for corrective action.
- 2.14** Unless otherwise agreed by the Applicable Customer, the Supplier shall ensure that the Supplier's Personnel performing work on a Customer's facilities or work sites have the appropriate experience, capability, skills and qualifications.
- 2.15** The Supplier's Personnel shall be trained by the Supplier as it relates to the Services in compliance with appropriate health, safety, and environmental codes, standards, laws, and regulations as required by all governmental or regulatory agencies having jurisdiction at the site where work is carried out.
- 2.16** With the exception of VISA, IPA/AA, SOC and Traction (training to be provided by Customer), the Supplier's Personnel working on the Customer's sites shall attend generic Applicable Customer account HSSE induction training the requirements of which shall be tailored to the specific services to be provided and detailed in the applicable Release Order.
- 2.17** The applicable Release Order will have a preventative maintenance program, agreed to by the parties, which will identify and prioritise maintenance for equipment and safety critical items in relation to the Services undertaken at the Applicable Customer's sites.
- 2.18** The Applicable Customer authorised representative shall have the right, at any time, to require Supplier to remove and bar from the Applicable Customer's sites any of the Supplier's Personnel whose conduct could jeopardize the safety of any person.

2.19 Other appropriate policies may be required for compliance or awareness when work is being carried out at the Applicable Customer's sites, and if so, these will be communicated to Supplier through the contract managers. These policies include the BP Code of Conduct and the LOMS for operational sites and local HSSE and OSF policies and protocols for all other sites.

2.20 The applicable Release Order shall contain an appropriate security management plan, which has been reviewed by the each party's respective management team, in order to ensure continual delivery of the Services where carrying out work on the Applicable Customer's behalf at the Supplier's sites. Within the security management plan, the Supplier shall ensure that the operational and any legal responsibilities related to security are clearly identified and allocated. It is recommended that such plan should contain details of how the Supplier:

2.20.1 maintains contacts within internal and external network groups;

2.20.2 ensures security representation at relevant leadership meetings;

2.20.3 conducts periodic risk assessments (including a site security survey and criminal risk assessment) to identify security risks;

2.20.4 ensures compliance of security services with relevant laws;

2.20.5 maintains a response plan to address government and community security concerns; and

2.20.6 implements a security threat alert system and associated response plan.

2.21 Consideration should be given to environmental aspects and impacts of this Agreement. Manufacturing and disposal of products, materials, packaging and waste should be carried out in accordance with applicable local/international environmental and ethical legislation.

H. Business Continuity Planning (BCP)

1 Business Continuity Policy

- 1.1 1.1 Business Continuity Program. Supplier shall maintain during the Term: (i) a program for ongoing management and governance of the Services under this Agreement supported by its executive management and appropriately resourced to enable Supplier to respond in the event of a disruption or disaster, including both technology recovery capability and business unit recovery capability, in such manner to allow critical business functions to continue within planned levels of disruption and to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of the Services through training, testing, maintenance and review and recovery objectives with respect to the Services under this Agreement (the "Business Continuity Program"); and (ii) a procedure for periodically testing the readiness and effectiveness of the Business Continuity Program. Supplier shall provide Applicable Customer with the opportunity to review and evaluate its Business Continuity Program and shall remedy any findings that Supplier determines are reasonably likely to materially and adversely affect Applicable Customer (if not addressed). Supplier shall provide to Applicable Customer annual reports of testing of its Business Continuity Program at Applicable Customer's request.

Schedule 5

Special Conditions

[Drafting Note: This document should set out any modifications and/or supplements to the Global Agreement which have not been reflected in the main body of that Global Agreement, such as those to deal with specific category requirements. To create this Schedule 5 to the Global Agreement itself list any additional terms or amendments that apply to the terms of the Global Agreement – e.g. insert additional provisions from the clause bank]

The Parties have agreed to the following Special Conditions, which are permitted modifications and/or supplements to the Global Agreement:

1. There are no Special Conditions.

Certificate Of Completion

Envelope Id: 0A861EAA400949668F94B62C5C736681

Status: Completed

Subject: [579 SF00526573] CW192660-PROVISION OF SECURE PAYMENT METHOD STORAGE & TRANSACTION PROXYING-SERVICES

Document Description:

BP Agreement Repository (Oyster) Number::

Team::

Accountable Team::

Source Envelope:

Document Pages: 63

Signatures: 2

Envelope Originator:

Certificate Pages: 5

Initials: 0

Norashikin Dzulkeffle

AutoNav: Enabled

Chertsey Road

Envelopeld Stamping: Enabled

Sunbury-on-Thames, Middlesex TW16 7LN

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

norashikin.dzulkeffle@bp.com

IP Address: 194.39.128.20

Record Tracking

Status: Original

Holder: Norashikin Dzulkeffle

Location: DocuSign

5/27/2021 9:45:33 AM

norashikin.dzulkeffle@bp.com

Signer Events


Andrew Jackson

andrew.jackson@bp.com

Market sector procurement downstream

BP- R&M Procurement

Security Level: Email, Account Authentication
(None)**Signature**

DocuSigned by:

 F7E82C13719043A...

Signature Adoption: Pre-selected Style

Using IP Address: 147.161.167.104

Timestamp

Sent: 5/27/2021 10:12:00 AM

Resent: 5/28/2021 12:29:12 AM

Viewed: 5/28/2021 1:10:30 AM

Signed: 5/28/2021 1:10:58 AM

Electronic Record and Signature Disclosure:

Accepted: 5/28/2021 1:10:30 AM

ID: 11ada76b-2cbe-4ea0-ae6d-e79037a24b5d

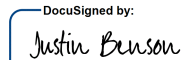
Justin Benson

justin@spreadly.com

CEO

Spreadly

Security Level: Email, Account Authentication
(None)

DocuSigned by:

 9624ED07D136401...

Signature Adoption: Pre-selected Style

Using IP Address: 70.250.119.131

Sent: 5/27/2021 9:56:07 AM

Resent: 5/28/2021 1:11:01 AM

Viewed: 5/28/2021 6:16:42 AM

Signed: 5/28/2021 6:16:56 AM

Electronic Record and Signature Disclosure:

Accepted: 5/28/2021 6:16:42 AM

ID: 99898390-ccbe-4732-a1d7-07ffa2679c1c

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp
Edward Gardner edward.gardner@bp.com BP GBS Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign	COPIED	Sent: 5/27/2021 9:56:07 AM Viewed: 5/27/2021 10:19:02 AM
Edward Gardner edward.gardner@bp.com BP GBS Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign	COPIED	Sent: 5/28/2021 6:17:00 AM
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	5/27/2021 9:56:07 AM
Certified Delivered	Security Checked	5/28/2021 6:16:42 AM
Signing Complete	Security Checked	5/28/2021 6:16:56 AM
Completed	Security Checked	5/28/2021 6:17:00 AM
Payment Events	Status	Timestamps
Electronic Record and Signature Disclosure		

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, BP (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through your DocuSign, Inc. (DocuSign) Express user account. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the 'I agree' button at the bottom of this document.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. For such copies, as long as you are an authorized user of the DocuSign system you will have the ability to download and print any documents we send to you through your DocuSign user account for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$1.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign 'Withdraw Consent' form on the signing page of your DocuSign account. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use your DocuSign Express user account to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through your DocuSign user account all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact BP:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: DocuSign@bp.com

To advise BP of your new e-mail address

To let us know of a change in your e-mail address where we should send notices and disclosures electronically to you, you must send an email message to us at DocuSign@bp.com and in the body of such request you must state: your previous e-mail address, your new e-mail address. We do not require any other information from you to change your email address..

In addition, you must notify DocuSign, Inc to arrange for your new email address to be reflected in your DocuSign account by following the process for changing e-mail in DocuSign.

To request paper copies from BP

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an e-mail to DocuSign@bp.com and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with BP

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your DocuSign account, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an e-mail to DocuSign@bp.com and in the body of such request you must state your e-mail, full name, IS Postal Address, telephone number, and account number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online agreement signing - agreement may not be signed by BP..

Required hardware and software

Operating Systems:	Windows2000? or WindowsXP?
Browsers (for SENDERS):	Internet Explorer 6.0? or above
Browsers (for SIGNERS):	Internet Explorer 6.0?, Mozilla FireFox 1.0, NetScape 7.2 (or above)
Email:	Access to a valid email account
Screen Resolution:	800 x 600 minimum
Enabled Security Settings:	<ul style="list-style-type: none">•Allow per session cookies•Users accessing the internet behind a Proxy Server must enable HTTP 1.1 settings via proxy connection

** These minimum requirements are subject to change. If these requirements change, we will provide you with an email message at the email address we have on file for you at that time providing you with the revised hardware and software requirements, at which time you will have the right to withdraw your consent.

Acknowledging your access and consent to receive materials electronically

To confirm to us that you can access this information electronically, which will be similar to

other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that you were able to e-mail this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the 'I agree' button below.

By checking the 'I Agree' box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC RECORD AND SIGNATURE DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify BP as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by BP during the course of my relationship with you.