

## UK FINANCIAL SERVICES ADDENDUM

This Addendum ("**Addendum**") is effective as of the date the last party signs this Addendum (the "**Addendum Effective Date**") and is entered into by and among Spreedly ("**Customer**") and the AWS Contracting Party or AWS Contracting Parties (as applicable) ("**AWS**") under the Agreement. This Addendum supplements the AWS Customer Agreement available at <http://aws.amazon.com/agreement> (as updated from time to time) between Customer and AWS, or other agreement between Customer and AWS governing Customer's use of the Service Offerings (the "**Agreement**"). The parties agree as follows.

**1. Application of this Addendum.** This Addendum applies where Customer uses AWS Services to perform outsourcing that is subject to the regulatory oversight of the Regulator under Applicable Law as long as the Customer or the Customer's End User is a Regulated Entity and is subject to oversight by the Regulator in relation to any AWS Services being consumed under the Agreement.

**2. Information Security Program.** AWS will implement and maintain an information and security program which is designed to provide at least the same level of protection as evidenced by:

- the AWS security controls verified by AWS's appropriately skilled and knowledgeable external auditors in its then current System Organization Controls 1, Type 2 report ("**SOC 1 Report**") and its then current System Organization Controls 2, Type 2 report (for availability/security and confidentiality) ("**SOC 2 Report**", together with the SOC 1 Report, the "**Reports**");
- its then current certification under ISO 27001; and
- its then current status as a Level 1 service provider under PCI DSS (together with the ISO 27001, the "**Certifications**")

or, in each case, such alternative industry standard reports or certifications that are its successor or reasonable alternative (provided that they are at least as protective as the standards set out above) as determined by AWS (together, the "**AWS Information Security Program**").

Customer may, at no additional charge, directly access and download copies of AWS's SOC 1 Report, SOC 2 Report, ISO 27001 and PCI DSS certifications through the AWS Site (as at the Effective Date, located at <https://aws.amazon.com/artifact/>) ("**AWS Artifact**"). In the event that AWS no longer maintains such website, provided that Customer and AWS have a valid and applicable NDA in place, Customer may request copies of AWS's security and compliance reports directly from AWS.

For the avoidance of doubt, it will not constitute a breach of AWS's obligations pursuant to this Section if exceptions are identified in any SOC 1 Report or SOC 2 Report (or their successor or alternatives), provided that AWS has taken appropriate steps, in its sole discretion, to remediate those exceptions.

**3. Submission of requests for expansion of scope of the Certifications or Reports.** Customer may by Notice submit requests for the expansion of scope of Certifications and Reports where justified from a legal, regulatory, or risk management perspective. The number and frequency of such requests should be reasonable and legitimate from a risk management perspective. AWS will maintain an internal process aimed at enabling AWS to aggregate, review, and consider such Notices from all customers.

**4. Right of Access and Audit.**

**4.1** AWS agrees to provide the Regulated Entity, the Regulator, the Resolution Authority and the Auditor (each a "**Requester**") with full access and unrestricted rights of audit and information to, where relevant:

- a. data, devices, information, systems and networks used for providing the services outsourced, including where appropriate AWS's policies, processes and controls on data ethics, data governance and data security;



b. in respect of any Regulated Entity that is a PRA Institution, upon request by the Requester, summary reports evidencing AWS's penetration testing on the AWS Network ("**Penetration Testing Report**"). The Penetration Testing Report, together with the Reports and Certifications, provide the Requester with information to assess the effectiveness of AWS's implemented cyber and internal IT security measures and processes. The contents of the Penetration Testing Report and any information pertaining to methodology and scope will be provided subject to AWS's internal security policies and procedures. Requester may only request the Penetration Testing Report once annually.

c. AWS's company and financial information; and

d. AWS's external auditors, personnel and premises used for providing the services outsourced,

in each case to the extent required to enable the Regulated Entity to comply with their legal and regulatory obligations and monitor AWS's provision of the AWS Services (collectively the "**Right of Access and Audit**").

**4.2** AWS's contractual terms with Sub-outsourcing service providers include terms on access and audit, and enable Requester to exercise equivalent rights as under the Right of Access and Audit in order to audit such Sub-outsourcing service providers that the Regulated Entity (in its sole discretion) considers to be material under Applicable Law. The Requester shall exercise such activities in accordance with Section 4.3.

**4.3** The Requester will exercise the Right of Access and Audit and AWS will co-operate with the Requester in accordance with the following stipulations in the PRA's Outsourcing SS and/or EBA Guidelines, as applicable:

a. The Requester will exercise the Right of Access and Audit in a proportional and appropriate manner, taking into account: the size, structure and operational environment of the Regulated Entity and the nature, scale and complexity of their activities; the risks arising from the AWS Services used by the Regulated Entity; the materiality, criticality or importance of the AWS Services used by the Regulated Entity; and the potential impact of the AWS Services on the continuity of Customer's activities (and any impact tolerances, if applicable).

b. The Requester will exercise the Right of Access and Audit and determine the audit frequency and areas to be audited using a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards.

c. The Requester can appoint a third party to exercise the Right of Access and Audit, subject to the confidentiality provisions in Section 13(a). It is the Requester's responsibility to verify that its and any third party's personnel performing the audit have the appropriate expertise, qualifications and skills to perform relevant audits and assessments of the Services effectively.

d. The Requester will, before a planned onsite visit, provide Notice in a reasonable (in light of the nature and scope of the requested audit) time period of the onsite visit to a relevant business premise, unless an early prior notification has not been possible due to an emergency or crisis situation, or in the case of PRA Institutions and Payment Institutions, where such Notice would defeat the purpose of the audit.

e. If the Requester's exercise of the Right of Access and Audit could, in AWS's reasonable opinion, create a risk for another AWS customer's environment (including due to its impact on service levels, availability of data, and/or confidentiality), the Requester and AWS will agree on a way to address the request that provides the Requester an equivalent level of assurance which ensures that risks to another AWS customer's environment are avoided or mitigated.

f. The Requester will exercise the Right of Access and Audit in an outcomes-focused way, considering which audit techniques are appropriate to achieve the level of assurance required. Where the Requester determines that it is sufficient to comply with its regulatory obligations, the Requester should exercise its Right of Access and Audit by conducting offsite audits such as requesting AWS to



provide it with confidential copies of Certifications and Reports, or, if AWS has implemented a process for pooled audits, through a pooled audit conducted in co-operation with other AWS customers in accordance with such process.

**4.4** AWS acknowledges that nothing in this Addendum will limit or restrict relevant Regulators' or Resolution Authorities' information gathering and investigatory powers, including under Sections 165, 165A and 166 of the FSMA and Sections 3A, 83ZA - 83ZB of the Banking Act 2009.

**4.5** The exercise of the Right of Access and Audit to conduct onsite audits at AWS premises will be subject to AWS's reasonable policies and procedures designed to ensure the security and resiliency of the AWS multi-tenant environment, and other matters such as health and safety, including AWS physical security, premises and facility access and badge policies, information security policies, and audit policies ("**Audit Policies and Procedures**"). In the event that any provision in the Audit Policies and Procedures is inconsistent with this Section 4, the PRA Outsourcing SS or the EBA Guidelines (as applicable to the Regulated Entity), that portion of the Audit Policies and Procedures shall not apply and the terms of Section 4.3 will control.

**4.6** If there is a conflict between this Section 4 and another Section of the Agreement, the terms of this Section 4 will control.

**5. Notice.** Notices under Sections 3, 4 and 13(b) of this Addendum can be provided to AWS via the AWS webpage located at <https://pages.awscloud.com/AuditRequest.html> (and any successor or related locations designated by AWS), as may be updated by AWS from time to time. Notices under any other applicable Section of this Addendum will be provided in accordance with the Agreement.

**6. Performance Reporting.** AWS will provide ongoing reporting to Customer of developments that may have a material impact on AWS's ability to provide the AWS Services by making available performance information regarding service availability through the Service Health Dashboard, located at <http://status.aws.amazon.com>, or any successor or related locations designated by AWS. In addition, Customer may use Amazon CloudWatch (or any successor Service) to monitor and gather information on its AWS cloud resources and the applications it runs on AWS.

**7. Disclosure of Events with a Material Adverse Impact.** In order to assist Customer with providing notice to a Regulator of developments which may have a material adverse impact on its ability to use the AWS Services ("**Adverse Events**"), AWS will make available the information as set out in this Addendum and the Agreement, including by providing information and support by a technical account manager in case of unplanned Adverse Events as set out in the AWS Support Guidelines, provided Customer is enrolled in AWS Enterprise Support. For the purpose of this Section, "**AWS Enterprise Support**" means the AWS Support at the Enterprise-level tier (or any successor service providing such communications alerts), and "**AWS Support Guidelines**" means the guidelines currently available at <https://aws.amazon.com/premiumsupport/enterprise-support/> (or any successor or related locations designated by AWS), as such guidelines may be updated by AWS from time to time.

## **8. Sub-outsourcing.**

a. At least 180 days before any planned Sub-outsourcing or material changes thereto, in particular where this might affect the ability of AWS to meet its responsibilities under the Agreement, AWS will update the Sub-outsourcing list on the AWS Site, including the name of the service provider, a description of the services provided, and the location where the service provider is authorized by AWS (the "**Sub-outsourcing List**"). Notwithstanding the foregoing, with respect to any Sub-outsourcing for any AWS Services or AWS regions that are not generally available as of the Addendum Effective Date,



AWS will not be required to update the Sub-outsourcing List until the date that the applicable AWS Services or AWS regions are made generally available.

b. If Customer objects to any new or materially changed Sub-outsourcing during the 180-day period described above, then without prejudice to any termination rights under the Agreement, including termination rights under Section 7 of the Agreement, Customer may discontinue using the AWS Services relating to the Sub-outsourcing or move its Customer Content to another AWS region where the Sub-outsourcing is not authorized by AWS.

c. For any Sub-outsourcing, AWS will (a) perform due diligence on the service provider, (b) enter into a written agreement with the service provider which requires the service provider to comply with all applicable laws, applicable regulatory requirements, and relevant contractual obligations of the Agreement (including appropriate obligations with respect to confidentiality, data protection, data security, business contingency, operational disruption and audit), and (c) oversee the service provider in line with the terms of the Agreement and remain fully responsible under the Agreement for the provision of the AWS Services to Customer.

d. The AWS Information Security Program includes verification of the policies and controls that AWS implements to oversee and monitor AWS's Sub-outsourcing arrangements.

## 9. Post-Termination Support and Retrieval of Customer Content.

a. AWS will comply with the obligations set out in this Section 9 in order to support Customer in the orderly transfer of the Customer's activities. AWS will provide Customer with at least two years' Notice before terminating the Agreement for convenience pursuant to Section 7.2(a) (Termination for Convenience) of the Agreement. Following the Termination Date, AWS will provide Customer with at least a 90 day period during which it will not take any action to remove Customer Content pursuant to Section 7.3(b) (Post Termination) of the Agreement.

b. The AWS Services provide Customer with controls that Customer may use to delete Customer Content as described in the Documentation. Up to the Termination Date, Customer will continue to have the ability to delete Customer Content in accordance with this Section. For 90 days following the Termination Date, Customer may delete any remaining Customer Content from the Services, subject to the terms and conditions set out in the Agreement, unless prohibited by law or the order of a governmental or regulatory body or it could subject AWS or its Affiliates to liability. No later than the end of this 90 day period, Customer will close all AWS accounts.

**10. Compliance with Laws and Protection of Data.** Each party will comply with (i) all applicable laws, rules, regulations and ordinances in the performance of this Agreement applicable to it and binding on it, and (ii) all legal requirements regarding the protection of data that are applicable to it and binding on it in the performance of this Addendum, including, where applicable, requirements relating to protection of personal data, banking secrecy or similar confidentiality duties.

## 11. Business Continuity Planning

a. As of the Addendum Effective Date, AWS's information security program includes processes and procedures supporting business continuity and availability, and the SOC 2 Report includes confirmation that AWS maintains a business continuity system plan together with a description of the controls AWS operates for its business continuity system plan. AWS makes the SOC 2 Report available in accordance with the Addendum to enable Regulated Entities to assess AWS's business continuity system plan and associated controls.

b. AWS maintains a formal risk management program which includes regular reporting to AWS's senior leadership to continually identify, assess, mitigate, report and monitor risk, including business continuity planning for critical business functions ("**Business Continuity Plan**"). This program incorporates availability, redundancy, and infrastructure capacity planning within its standards, and is integrated into AWS's risk management program. AWS tests and updates its Business Continuity Plan



at least annually and will continue to conduct regular reviews of its security and Business Continuity Plan on an ongoing basis.

c. Without limiting any rights under the Agreement, in the event that AWS: (i) is declared bankrupt or in liquidation (or equivalent), (ii) is dissolved or wound up, or (iii) discontinues its entire business operations of providing the AWS Services (except as the result of any assignment permitted under the Agreement), Customer will have the immediate right to retrieve all Customer Content unless prohibited by law or the order of a governmental or regulatory body or insolvency practitioner (or equivalent).

## 12. Resolution and the UK Special Resolution Regime

a. This Section 12 applies to Regulated Entities that are subject to the UK's special resolution regime under the Banking Act 2009 and Applicable Law (each a **"SRR Institution"**).

b. AWS acknowledges that when a SRR Institution is taken into resolution, the SRR Institution will be subject to a range of powers exercisable by the Resolution Authority including pursuant to Sections 48Z and 70C-D of the Banking Act 2009. In the event that a SRR Institution is taken into resolution in accordance with the Banking Act 2009, AWS will comply with all laws applicable to it in relation to that resolution and, if so requested in writing, will cooperate in good faith with the Resolution Authority (but without prejudice to any rights or remedies AWS has under the Agreement) regarding any concerns in respect of the ongoing provision of the AWS Services to Customer.

c. AWS acknowledges that the occurrence of a Special Resolution Event does not, in and of itself, constitute a material breach giving rise to AWS's termination for cause rights with respect to the Agreement, provided that the Customer continues to fulfil its substantive obligations under the Agreement (as such term is understood for the purposes of Section 48Z of the Banking Act 2009), including payment obligations.

## 13. Confidentiality and Costs.

a. Any information, responses and documentation provided by AWS or by Customer in connection with this Addendum, including confidential information provided by AWS following an Adverse Event, (**"Confidential Compliance Information"**) will be treated as confidential information of the party owning it and will be provided to the recipient pursuant to confidentiality obligations reasonably acceptable to the party owning the Confidential Compliance Information (which, in case of the Regulator, means confidentiality obligations set out under applicable law) and will not be disclosed by the recipient, except that Confidential Compliance Information may be disclosed to: (a) the Regulator, provided that the Customer obtains confidential treatment or similar protections; and (b) the Customer, provided that all Confidential Compliance Information of AWS will be treated as confidential information of AWS under the Agreement, the NDA (if any) and this Addendum. Customer acknowledges that: (X) prior to exercising any rights under Section 4.2, the applicable Sub-outsourcing service provider(s) may require the Requester to first enter into a binding non-disclosure agreement; and (Y) any third party Auditor appointed by a Requester under Section 4 must first enter into a binding and enforceable non-disclosure agreement with AWS (and if applicable, any Sub-outsourcing service provider under Section 4.2). In addition: (i) End Users which are Regulated Entities may directly access and download Reports and Certifications via AWS Artifact (or an alternative method accessible via the AWS Site); and (ii) other Confidential Compliance Information of AWS (excluding Reports, Certifications and any other information from, referring to or otherwise included in the AWS Information Security Program) may be disclosed by Customer to End Users which are Regulated Entities provided that such End User has agreed to hold such information in confidence pursuant to a binding non-disclosure agreement with AWS. Notwithstanding the foregoing, audit findings under Section 4 which are made available to AWS under this Addendum may be disclosed by AWS, provided that: (A) AWS does not include any reference to the Customer, the Regulator and/or their agents in such disclosure; and (B)





such disclosure is not prohibited by Applicable Law. Customer will promptly provide AWS with written Notice of any disclosures made by Customer under this Section 13.

b. Customer will bear, and indemnify AWS against, all reasonable fees (including AWS's then-current rate(s) for its personnel), costs and expenses arising from the exercise of the rights described in Section 4 regardless of whether it was exercised by Customer or another Requester, except where a Regulator exercises such rights directly with AWS. Customer may request an estimate of the fees, costs and expenses associated with a proposed exercise of the Right of Access and Audit by providing AWS with Notice, including detailed information regarding the proposed scope of the Right of Access and Audit on which the estimate will be based. AWS will prepare a written statement of work including the applicable fees and Customer's requested scope of the Right of Access and Audit.

**14. Insurance.** As of the Effective Date, Amazon.com, Inc.'s memorandum of insurance is located at <https://ir.aboutamazon.com/Amazons-Insurance/>. Additionally, upon Customer's written request, AWS will provide to Customer a copy of this memorandum of insurance, or a similar successor document, evidencing its group insurance coverage. AWS will provide this documentation no more than once annually.

**15. Testing.**

a. Customer has the right to conduct penetration testing in accordance with AWS's Penetration Testing Policy (available at <http://aws.amazon.com/security/penetration-testing/> or any successor or related locations designated by AWS). Requests will be made in the manner described by the Penetration Testing Policy, or in such other manner as AWS directs.

b. AWS provides information to support Customer with designing, deploying and testing their use of the AWS Services in line with the Regulated Entity's operational resilience objectives. As at the date of this Addendum, this information is available at [https://d1.awsstatic.com/whitepapers/compliance/AWS\\_Operational\\_Resilience.pdf](https://d1.awsstatic.com/whitepapers/compliance/AWS_Operational_Resilience.pdf) (or any successor or related locations designated by AWS).

**16. Definitions**

**"Applicable Law"** means the applicable laws and regulations administered by the Regulator in connection with the Regulated Entity's use of the AWS Services.

**"Auditor"** means a suitably qualified auditor who is engaged by the Regulated Entity or by the Regulator to audit Customer's or the Regulated Entity's use of the AWS Services under this Addendum.

**"AWS Network"** means AWS's data center facilities, servers, networking equipment, storage media, and host software systems (e.g., virtual firewalls) that are within AWS's control and are used to provide the Services.

**"AWS Services"** means all the generally available services made available by AWS or its Affiliates through the AWS Management Console (or through other means by which AWS makes such services available).

**"EBA Guidelines"** means EBA/GL/2019/02, "Guidelines on outsourcing", published by the European Banking Authority on 25 February 2019, or any successor or update thereto (subject to such successor or update being in force).

**"FSMA"** means the Financial Services and Markets Act 2000 as amended from time to time and any relevant secondary legislation that is applicable to the Regulated Entity.



**“Notice”** means any notice provided in accordance with Section 5.

**“PRA's Outsourcing SS”** means SS2/21, “Supervisory Statement: Outsourcing and third party risk management”, published by the Prudential Regulation Authority on 29 March 2021, or any successor or update thereto (subject to such successor or update being in force).

**“Payment Institution”** means either (i) a legal person that has been granted authorisation by the Financial Conduct Authority to provide payment services under the Payment Services Regulations 2017; or (ii) “electronic money institution” as defined in Article 2(1) of Directive 2009/110/EC, in each case provided such entity is subject to the EBA Guidelines.

**“PRA Institution”** means any of (i) a bank, building society or PRA-designated investment firm “banks”, (ii) insurance and reinsurance firms in scope of Directive 2009/138/EC as implemented in the United Kingdom, including the Society of Lloyds and managing agents (“insurers”), and (iii) UK branches of banks and insurers, in each case as such terms are understood in the PRA's Outsourcing SS and provided such entity is subject to the PRA Outsourcing SS.

**“Regulated Entity”** means the Customer or the Customer's End User (as the case may be) if and so long as such entity is regulated by or subject to oversight by the Regulator.

**“Regulator”** means the Financial Conduct Authority (the “FCA”) and/or the Bank of England (including the Prudential Regulation Authority, the “PRA”), or any successor UK financial services regulator.

**“Resolution Authority”** means the Bank of England.

**“Special Resolution Event”** means, with respect to a SRR Institution, the occurrence of a crisis prevention measure, crisis management measure or recognised third-country resolution action (in each case as defined under Section 48Z of the Banking Act 2009) in relation to the SRR Institution, or occurrence of any event linked directly to the application of such a measure or action, or other similar proceeding or event pursuant to Applicable Law.

**“Sub-outsourcing”** means a situation where AWS further transfers its obligations to provide the AWS Services under the Agreement to another service provider.

## 17. Miscellaneous

a. The parties agree that the existence and terms of this Addendum are not publicly known, will be treated as confidential information and will not be disclosed by either party, except that the existence and terms of this Addendum may be disclosed to (i) the Regulator, provided that the Customer obtains (or ensures that the Customer's End Users that are Regulated Entities obtain) confidential treatment or similar protections and (ii) Customer's End Users that are Regulated Entities, provided that the Customer makes the End User aware of the confidential nature of the Addendum and procures confidentiality protections from the End User that are at least as protective as the obligations of confidentiality that Customer owes to AWS under the Agreement, the NDA (if any) and this Addendum.

b. Customer's sole and exclusive remedy for any breach by AWS in relation to this Addendum is to terminate this Addendum. For purposes of this Addendum, the rights and obligations of the parties in this Addendum are in addition to, and not in replacement of, the rights and obligations of the parties in the Agreement, except that this Section will prevail over any conflicting term in the Agreement. Except as amended by this Addendum, the Agreement will remain in full force and effect.



c. This Addendum may be executed in two or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same document. The parties may sign and deliver this Addendum by facsimile or email transmission.


*[Remainder of Page Intentionally Left Blank]*





**IN WITNESS WHEREOF**, Customer and AWS have executed this Addendum as of the Addendum Effective Date.

**AMAZON WEB SERVICES, INC.**

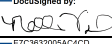
By: DocuSigned by:  
  
BD8775E476F8409...

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**SPREEDLY, INC**

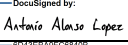
By: DocuSigned by:  
  
ETC3632005AC4CD...

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**AMAZON WEB SERVICES EMEA SARL**

By: DocuSigned by:  
  
BD13EB3A9FC8840B...

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

