DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") forms part of the On-Demand Subscription Agreement, executed as of _____, 201__, ("**Agreement**") by and between Amber Road, Inc. ("**Vendor**") and _____ ("**Client**"). Each of Vendor and Client may individually be referred to as a "Party" and together as the "Parties". This Addendum is effective as of May 25, 2018 ("**Addendum Effective Date**").

The terms used in this Addendum have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement remain in full force and effect.

The Parties agree as follows:

1. PROCESSING OF PERSONAL DATA.

1.1. **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Personal Data, Client is the Controller, Vendor is the Processor, and that Vendor may engage Sub-Processors pursuant to the requirements set forth herein.

1.2. **Client Processing.** Client will, in its use of the Services, only Process Personal Data in accordance with the requirements of Data Protection Laws and Vendor instructions. Vendor will notify Client if, in Vendor's reasonable opinion, a Client instruction would violate Applicable Law. Client is solely responsible for the accuracy, quality and legality of Personal Data, the means by which Client acquired Personal Data, and the lawfulness of the Processing instructions it issues to Vendor.

1.3. **Vendor Processing.** Personal Data shall be considered Confidential Information pursuant to the Agreement and Vendor will protect Personal Data as confidential and will only Process Personal Data on behalf of, and in accordance with, Client's documented instructions for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Client's Authorized Users or Authorized Affiliates in their use of the Services; (iii) Processing to comply with other documented instructions provided by Client where such instructions are consistent with the terms of the Agreement; and (iv) as required by Applicable Law; provided, that if Vendor is required to Process Personal Data by Applicable Law, Vendor will notify Client of any such requirement before Processing the Personal Data (unless such law, regulation, or court order prohibits such information on important grounds of public interest).

1.4. **Confidentiality; Disclosure.** Vendor will: (i) keep and maintain all Personal Data in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, or disclosure; (ii) not use, sell, rent, transfer, distribute, or otherwise disclose or make available Personal Data for Vendor's own purposes or for the benefit of anyone other than Client, in each case, without Client's prior written consent; and (iii) not, directly or indirectly, disclose Personal Data to any person other than Authorized Persons without Client's prior written consent, unless and to the extent required by government authorities or by Applicable Law, in which case, Vendor shall notify Client before such disclosure or as soon thereafter as reasonably possible.

1.5. **Details of the Processing.** The subject-matter of Processing of Personal Data by Vendor is the performance of the Services. The duration of the Processing, the types of Personal Data, and categories of Data Subjects Processed under this Addendum are further specified in Schedule 2, attached hereto.

2. VENDOR AUTHORIZED PERSONS.

2.1. **Authorized Persons Obligations.** Vendor shall at all times cause its Authorized Persons to abide strictly by Vendor's obligations under this Addendum.

2.2. **Confidentiality; Authorization; Training.** Vendor has implemented and maintains policies and procedures to ensure that any Authorized Person who accesses Client Data has been informed of the confidential nature of the Client Data, has executed a written confidentiality agreement, and has appropriate training, clearance, authorization,

and supervision commensurate with the level of access granted to such Authorized Person. Vendor will ensure that access to Client Data is limited to those Authorized Persons performing Services in accordance with the Agreement.

2.3. **Responsibility for Authorized Persons.** Vendor will be liable to Client for any acts or omissions of its Authorized Persons for any breach of this Addendum.

3. RISK MANAGEMENT.

3.1. **Security.** Vendor maintains an information and network security program that includes appropriate administrative, physical, organizational, and technical safeguards to prevent and guard against the unauthorized or accidental access, disclosure, destruction, loss, Processing, damage, or alteration of Client Data in Vendor's possession or control. Vendor's information and network security program includes vulnerability management policies that have been prepared to identify and minimize threats and risks to Vendor's data center used to store or transmit Client Data. This includes maintaining the following policies and procedures: an up-to-date anti-malware solution, quarterly vulnerability scanning, and annual penetration testing. Internal and external vulnerability assessments, including network/host applications, will be conducted quarterly by an independent certified security firm and after any major changes to the data center environment. Vendor will remediate any critical security issues actually discovered by such independent certified security firm within a reasonable timeframe. Upon request, Vendor shall provide Client with its most current "Client Data and Network Security Exhibit (SaaS)".

3.2. **Contingency Plan.** Vendor has and will maintain a disaster recovery and business continuity plan. Such disaster recovery and business continuity plan will outline the procedures necessary to restore Vendor's systems and operations in a timely manner in the case of an emergency or disaster.

3.3. **Audit.**

3.3.1. Client may request once per calendar year (unless otherwise required by Applicable Law) a copy of Vendor's SSAE16 SOC 2 Type 2 report on Vendor's hosting environment and Services system within Vendor's organization. Such report will have been conducted by an independent auditing firm for the purposes of verifying the safety and soundness of Vendor's organization and the Services provided by Vendor.

3.3.2. Client may request once per calendar year (unless otherwise required by Applicable Law) with three (3) weeks' advance notice an on-site inspection of the systems and facilities relevant to the Services and protection of Client Data. Client and Vendor will mutually agree upon the scope, timing, and duration of the inspection prior to any such on-site inspection. If Client wishes to conduct an on-site audit using a third party auditor, Vendor may object to the Client's choice of third party auditor on reasonable grounds and in such event, Client shall select a different auditor. An inspection performed pursuant to this Section will not unreasonably interfere with the normal conduct of Vendor's business. Client will at all times comply with the use, security, safety, and access policies at and for such location for Vendor's employees and visitors as may be in effect from time to time. Client is responsible, and is fully liable, for the actions and omissions of its personnel while on Vendor's premises and/or using Vendor's systems, and Client will require its personnel to follow Vendor's safety, security, and other rules, guidelines, policies, and instructions.

4. SUBPROCESSING.

4.1. **Appointment.** Vendor may engage Sub-Processors in connection with the provision of the Services. Vendor has entered into a written agreement with each Sub-Processor containing data protection obligations no less protective than those in this Addendum with respect to protecting Client Data to the extent applicable to the nature of the services provided by such Sub-Processor. Vendor will provide to Client for review, copies of such Sub-Processor agreements (which may be redacted to remove confidential and/or proprietary information not relevant to the requirements of this Addendum) as Client may request from time to time.

4.2. **Current Sub-Processors.** A list of Vendor's current Sub-Processors is attached to this Addendum as Schedule 1.

4.3. **Objection to New Sub-Processors.** Vendor will provide written notification of new Sub-Processors to Client before authorizing any new Sub-Processor to Process Client Data in connection with the provision of the applicable

Services. If Client notifies Vendor within 10 days of such notification of any Client objections (on reasonable grounds) to the proposed appointment: (i) Vendor will work with Client in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-Processor; or (ii) where a change cannot be made within 30 days from Vendor's receipt of Client's objection, notwithstanding anything in the Agreement, Client may terminate the Agreement to the extent that it relates to the Services that require the use of the proposed Sub-Processor.

4.4. **Cross Border Transfers.** Vendor will not permit any Sub-Processor to transfer any Client Data across national borders without Client's prior written consent. Vendor will require its Sub-Processors to enter into data transfer agreements or contractual clauses in connection with any international transfers of Client Data that has been approved by Client.

4.5. **Liability.** Vendor will be liable to Client for any acts or omissions of its Sub-Processors to the same extent Vendor would be liable if performing the services of each Sub-Processor directly under the terms of this Addendum.

5. DATA SUBJECT RIGHTS.

5.1. **Notification.** Vendor will promptly notify Client if it receives a (i) request from a Data Subject to exercise the Data Subject's rights granted by Data Protection Laws ("**Data Subject Request**"); or (ii) complaints or other requests relating to a Party's obligations under Data Protection Laws, or relating to Personal Data or a Data Subject ("**Complaint**").

5.2. **Support; Response.** Vendor will, without undue delay, provide reasonable information to Client (and procure that any relevant Sub-Processor does the same) to assist Client in responding to a Data Subject Request or Complaint within the timeframe set out in the Data Protection Laws. Vendor will not respond to such Data Subject Request or Complaint without Client's prior written consent or as required by applicable Data Protection Law.

6. SECURITY INCIDENT RESPONSE. Vendor has and will maintain security incident management and response policies and procedures and will notify Client without undue delay after becoming aware of the unauthorized or accidental access, disclosure, destruction, loss, Processing, damage, or alteration of Client Data in Vendor's or its Sub-Processor's possession or control ("**Security Incident**"). Vendor will make reasonable efforts to identify the cause of such Security Incident and take reasonable commercial steps Vendor deems necessary and reasonable to correct, remediate, and/or mitigate the cause of a Security Incident to the extent the correction, remediation, and/or mitigation is within Vendor's control. Vendor will cooperate, at its own expense, with Client and take reasonable commercial steps as Client directs to assist in any investigation, mitigation, remediation, and notification of a Security Incident for which Vendor was the cause. Vendor will not communicate a Security Incident to affected Data Subjects without Client's written authorization. Notifications provided to Client by Vendor pursuant to this Section will be made to the individual identified on Schedule 3, attached hereto.

7. RETURN & DESTRUCTION OF CLIENT DATA, RECORD KEEPING.

7.1. **Return & Destruction of Client Data.** Vendor will promptly, but without undue delay, return to Client, or destroy, Client Data upon Client's written request or the termination or expiration of the Agreement. Vendor may retain Client Data to the extent required by Applicable Law, contractual obligations, or if Client Data resides in backup archives and isolating individual Client Data is not practical. Vendor will continue to protect the security and confidentiality of such retained Client Data in accordance with the Agreement and this Addendum. Archived Client Data will not be restored back to production systems (except in certain rare instances, e.g., the need to recover from a natural disaster or serious security breach). Retention rules have been put in place so that Client Data in backup archives is retained for as short a time as necessary before being automatically deleted.

7.2. **Record Keeping.** Vendor will keep and maintain complete, accurate, and up to date written records of all categories of Processing activities carried out on behalf of Client as required by Data Protection Laws, including: (i) the name and contact details of the Sub-Processors carrying out specific Processing activities on behalf of Client; (ii) the categories of Processing carried out on behalf of Client; and (iii) where applicable, transfers of Personal Data to an international recipient.

8. DATA PROTECTION IMPACT ASSESSMENT & PRIOR CONSULTATION. Vendor will provide reasonable assistance to Client with any data protection impact assessments and prior consultations with supervising authorities or other competent data privacy authorities which Client reasonably considers to be required by applicable Data Protection Laws. In each case, such assistance will solely be in relation to Processing of Client Data by, and taking into account the nature of the Processing and information available to, Vendor.

9. CROSS BORDER TRANSFERS. Vendor self-certifies to, and complies with, the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework, as administered by the U.S. Department of Commerce. Vendor will maintain its self-certifications to, and compliance with, the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework with respect to the Processing of Personal Data that is transferred from the European Economic Area and/or Switzerland to the United States. Additionally, if requested by Client, Vendor shall promptly execute Standard Contractual Clauses as may be required to process Personal Data in accordance with Data Protection Laws.

10. CLIENT DATA DISCLOSURES. To the extent legally permissible, Vendor will promptly notify Client of any legally binding request for disclosure of Client Data by a law enforcement authority.

11. CHANGES IN APPLICABLE LAW. Client may propose variations to this Addendum which Client reasonably considers to be necessary to address the requirements of any Applicable Law. If Client gives notice under this Section 11, the Parties will promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those, or alternative, variations designed to address the requirements identified in Client's notice as soon as reasonably practicable.

12. INDEMNIFICATION. Vendor will indemnify Client for actual and reasonable costs incurred in providing Data Subjects affected by a Security Incident, caused by Vendor, with notice of the breach to Data Subjects and applicable supervisory authorities and complimentary access for one (1) year of credit monitoring services, which Client, in its sole discretion deems reasonably necessary to protect such affected individuals in light of the risks posed by the Security Incident.

13. GENERAL.

13.1. **Term.** The term of this Addendum commences on the Addendum Effective Date and will remain in effect until the later of (i) the expiration or termination of the Agreement or; (ii) Vendor's destruction of, or return to Client, all Client Data.

13.2. **Governing Law; Jurisdiction.** The validity, interpretation, and performance of this Addendum will be controlled and governed by the laws of the territory stipulated in the Agreement, without regard to conflicts of law provisions. The Parties hereby irrevocably consent to jurisdiction and venue for any dispute concerning this Addendum in the choice of jurisdiction stipulated in the Agreement.

13.3. **Compliance.** Each of Client and Vendor will comply with all Applicable Laws.

13.4. **Severability.** If any term or provision of this Agreement or the application of any such provision is held by a court of competent jurisdiction to be contrary to law, invalid, illegal or unenforceable, then such term or provision will be deemed replaced by a term or provision that is valid and enforceable and that comes closest to expressing the intention of the original term or provision, and the remaining terms and provisions of this Addendum will continue in full force and effect.

13.5. **Continued Obligations; Rights.** Nothing in this Addendum reduces Vendor's obligations under the Agreement in relation to the protection of Client Data or permits Vendor to Process, or permit the Processing of, Personal Data in a manner which is prohibited by the Agreement.

14. DEFINITIONS.

14.1. "**Applicable Laws**" means Data Protection Laws and any laws, codes, legislative acts, regulations, ordinances, rules, rules of court, or orders to which a Party is subject.

14.2. "**Authorized Person(s)**" means any Vendor subcontractor, officer, director, employee, or consultant who have a need to know or otherwise access Client Data to enable Vendor to perform its obligations under the Agreement.

14.3. "**Complaint**" has the meaning set forth in Section 5.1 of this Addendum.

14.4. "**Controller'** means the entity which determines the purposes and means of the Processing of Personal Data.

14.5. "**Client Data**" has the meaning set forth in the Agreement and, for the purposes of this Addendum, includes Personal Data.

14.6. "**Data Protection Laws**" means (i) the laws or regulations implementing Directive 95/46/EC; (ii) GDPR and any laws implementing or supplementing GDPR; and (iii) the data protection or privacy laws of any other country.

14.7. "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

14.8. "**Data Subject Request**" has the meaning set forth in Section 5.1 of this Addendum.

14.9. "**GDPR**" means General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Union of 27 April 2016, enforceable from 25 May 2018.

14.10. "**Personal Data**" means any information relating to a Data Subject, including by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a Data Subject.

14.11. "**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

14.12. "**Processor**" means the entity which processes Personal Data on behalf of the Controller.

14.13. "**Security Incident**" has the meaning set forth in Section 6.

14.14. "**Services**" means the services provided by Vendor to Client pursuant to the Agreement.

14.15. "**Sub-Processor**" means an entity, but excluding Vendor's officers, directors, and employees, appointed by or on behalf of Vendor to Process Personal Data on behalf of Client in connection with the Agreement.

By signing below, each Party agrees that it has read and fully understands all of the terms and conditions in the Addendum, including all attachments attached hereto, and agrees and accepts all of the foregoing.

Vendor	**Client**
By: _____	By: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Schedule 1

Sub-Processors

Sub-Processor (Colocation Data Centers)	Country of Location
CSX Technologies Inc. (Primary Data Center)	Jacksonville, Florida USA
SunGard Availability Services (Secondary Data Center)	Carlstadt, New Jersey USA
Amazon AWS (Primary EU Data Center)	Frankfurt, Germany
Amazon AWS (Secondary EU Data Center)	Dublin, Ireland
Citic Telecom Tower (Primary Data Center – certain SCC clients only)	Kwai Chung, Hong Kong
Ap Lei Chau Service Centre (Secondary Data Center – certain SCC clients only)	Ap Lei Chau, Hong Kong

Schedule 2

Details of the Processing

This Schedule 2 includes certain details of the Processing of Personal Data as required by Article 28(3) of the GDPR.

Duration of Processing

- Vendor will Process Personal Data only during the term of the Agreement.
- Vendor may retain Client Data after the expiration or termination of the Agreement only in accordance with Section 7.1 of the Addendum.

Categories of Data Subjects

Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

Employees, business partners, business vendors, business suppliers, business customers

Type of Personal Data

Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- first, middle and last name
- title
- position and department
- employer
- contact information (company, email (home or business), phone (home or business), physical address (home or business))
- past or prior information relative to the above

Schedule 3

Client Notifications

In the event of a Security Incident, Vendor will notify the following individual(s):

Name: _____

Title: _____

Phone Number: _____

Email Address: _____

Fax: _____

Name: _____

Title: _____

Phone Number: _____

Email Address: _____

Fax: _____