Enhanced Security Addendum for
AWS Marketplace Contract
(Financial Services and other Sensitive Information)

This Enhanced Security Addendum (this “Addendum”) is part of the Enterprise Contract for AWS Marketplace (the “Enterprise Contract”) or the Standard Contract for AWS Marketplace (the “Standard Contract”), as applicable, between a Buyer and a Seller (for Enterprise Contracts) or a Licensor (for Standard Contracts) and governs the treatment of Confidential Information in the case of a SaaS Subscription. Each of the Standard Contract and the Enterprise Contract is a Marketplace Contract. Each Seller and each Licensor is a Supplier. All capitalized terms used but not defined in this Addendum have the meanings given to them in the Enterprise Contract or the Standard Contract, as applicable.

Supplier’s obligations under this Addendum are in addition to those set forth in the Security Addendum. Any ambiguity in this Addendum will be resolved in favor of protecting the confidentiality and security of Personal Information and other Confidential Information. In the event of a conflict between the terms and conditions of this Addendum and the Security Addendum, this Addendum will govern.

1. Data Protection.

1.1 Compliance with Applicable Law. Any collection, use, storage, processing or transfer of Personal Information by Supplier shall be undertaken in compliance with all applicable local, state, federal, and international Laws governing Buyer’s collection, maintenance, transmission, dissemination, use and destruction of Personal Information.

1.2 PCI Compliance. To the extent Supplier has access to the payment card information of Buyer’s employees or clients, any collection, maintenance and/or use of Personal Information by Supplier shall be undertaken in compliance with the Payment Card Industry Association Security Standards.

1.3 Use of AWS Services. Buyer acknowledges that Supplier uses AWS Services for the processing and hosting of the SaaS Services provided pursuant to this Agreement. Buyer consents to Supplier’s storage of Confidential Information in the AWS region selected by Supplier and to Supplier’s use of AWS Services to process Confidential Information and provide the SaaS Services.

1.4 Disclosure of Data Due to Legal Obligation. If Supplier is required by law to disclose or produce any Confidential Information of Buyer, Supplier will cooperate with Buyer, as reasonably requested by Supplier, in seeking protective orders or confidential treatment for any Confidential Information of Buyer before any Confidential Information of Buyer is disclosed or produced.

2. Data Retention Period. Supplier agrees to retain all Confidential Information of Buyer for a period of time specified by Buyer in writing and to dispose securely of all Confidential Information at the end of the specified retention period, unless otherwise instructed in writing.
3. **Information Security.** Supplier will implement and maintain, as part of its Security Program, at a minimum, but without limitation to, the following additional requirements:

3.1 formalized information security and confidentiality training not less than annually;

3.2 a disciplinary process for employees who fail to adhere to applicable information security policies;

3.3 physical or logical separation of Confidential Information from Supplier’s data and third party data;

3.4 encryption of Confidential Information at rest and in transit to or from systems owned or operated by or for Supplier to support the Services using industry standard encryption methods;

3.5 specific controls to ensure that Supplier has and enforces two-factor authentication for any and all remote connection to Supplier systems that access Confidential Information;

3.6 all Confidential Information deleted by Supplier will be securely and permanently deleted in accordance with industry standards, such as NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitation December 18, 2014;

3.7 maintain records to ensure the ability to audit access to Confidential Information, including (i) logging successful and unsuccessful sign-on attempts and (ii) ensuring that audit trails capture detailed activity within a user’s session;

3.8 upon request by Buyer, completing and providing to Buyer security questionnaires and/or self-assessment security compliance reviews;

3.9 risk assessments at least annually of the safeguards for the protection of Personal Information and other Confidential Information; and

3.10 audits at least once per year that verify its information security practices as to the use, handling and storage of Confidential Information in accordance with the requirements of this Addendum.

4. **Data Breaches.** Supplier shall notify Buyer promptly (but in any event within three days) upon discovery of any actual or reasonably suspected Security Incident, and will cooperate with Buyer in every reasonable way to help Buyer regain possession of the Confidential Information and prevent any further compromise, unauthorized use or disclosure. Supplier must document responsive actions taken in connection with any actual or reasonably suspected Security Incident, and conduct a mandatory post-incident review of actions taken, if any, to make changes in business practices relating to the protection of Confidential Information.

5. **Audits and Investigations.**
5.1 At least once annually, Supplier shall commission an SSAE 18 SOC2 Type II audit (or an equivalent attestation by an independent third party) and will promptly provide to Buyer a copy of or online viewing access the audit reports issued (or a summary of the audit reports, in a level of detail reasonably acceptable to Buyer, if use or distribution of the reports is restricted by the third party auditor) as a result of such audits. Supplier will cooperate and provide the third party auditor with access to, and the right to inspect and audit, all records and systems relating to (i) the collection, processing, or transfers of data relating to Confidential Information and (ii) the information security measures used by Supplier and its contractors to secure Confidential Information.

5.2 Supplier further agrees to cooperate in any investigation by Buyer (and in responding to any inquiry relating to Personal Information). In the event of any such investigation or inquiry, upon notice to Supplier, Buyer may suspend any further transfers of Personal Information for so long as may be necessary to obtain assurances that any additional transfers will not provide the basis for further regulatory action or possible liabilities. Any such suspension will not relieve either Party for any liability arising from the Agreement or any other commercial agreements with Buyer.