PRIVACY AND

(B) For so long as such system holds, contains, or processes Covered Data, cause the system to conform in all material respects with managementôs assertions with respect to the system upon which the then-most-recent SOC report or an industry standard independent audit report, and bridge or gap letter which covers the period between the expiry of the previous report and the release of the new report.

(C) Suppliers will, upon CHSôs request, make available to CHS for review, as applicable, Supplierôs latest Payment Card Industry (PCI) Compliance Report, SOC audit report, or any industry standard independent audit reports or certifications performed by or on behalf of Supplier assessing the effectiveness of Supplierôs information security program as relevant to the Covered Data.

(I) SOX: If Supplier is in scope for CHSôs compliance with the Sarbanesï Oxley Act (the "SOX Actò), as may be amended from time to time, Supplier will provide annually to CHS, for review. Supplierôs latest SOC report for as long as the system holds, contains or processes Covered Data, or

(II) PCI: Supplier will provide annually to CHS, for review. Supplierôs latest PCI Compliance Report(s) and/or SOC report for as long as the system holds, contains or processes Covered Data.

(g) Upon CHSôs request, to confirm Supplierôs compliance with this Addendum and any applicable laws, regulations, and industry standards, Supplier will permit CHS or CHSôs agents to perform an assessment, audit, examination, or review of all controls in Supplierôs physical and/or technical environment in relation to all Covered Data being handled, received or acquired and/or services being provided to CHS under the applicable agreement, and this Addendum. Supplier shall cooperate fully with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and applicable software that processes, stores, or transports the Covered Data for CHS pursuant to the applicable agreement and this Addendum. In addition, upon CHSôs request, Supplier shall provide CHS with the results of any audit by or on behalf of Supplier performed that assess the effectiveness of Supplierôs information security program as relevant to the security and confidentiality of the Covered Data shared during the course of the applicable agreement and this Addendum.

(h) PCI DSS. If, and to the extent that, any of the Covered Data is Cardholder Data that Supplier receives or Processes as a PCI Service Provider, Supplier will, unless expressly permitted otherwise in writing by the applicable CHS Party:

(i) Maintain current assessments and all other qualifications and certifications necessary to that designation under PCI DSS;

(ii) Deliver to CHS Supplierôs Attestation of Compliance (ñAOC)ò promptly upon completion thereof, in such form and containing such information as required under PCI-DSS, dated not more than one year after the previous AOC (if any) delivered by Supplier to CHS;

(iii) Provide to CHS, an agreed upon responsibility matrix identifying which PCI DSS requirements will be managed by the Supplier; and

(iv) Otherwise comply with all requirements of PCI DSS with respect to the Cardholder Data.

8. **Access to CHS Information Systems**.

(a) Use of Permitted Systems. Supplier will use any Permitted Systems solely to carry out Supplierôs obligations to the applicable CHS Party(ies). Supplier will use Permitted Systems for no other purpose.

(b) Conditions of Use. Supplier will use the Permitted Systems solely in accordance with the terms of such agreement(s) then in place between one or more CHS Parties and Supplier and such further conditions and policies as the applicable CHS Party makes available to Supplier from time to time. Such conditions and policies of use may include (and be described as) policies, procedures, technical requirements, and/or protocols. CHS may monitor Authorized Supplier Personsô access and activities within CHS Permitted Systems.

(c) Access by Authorized Supplier Persons. Supplier will limit access to the Permitted Systems to Authorized Supplier Persons. Supplier will provide to CHS the name of each Authorized Supplier Person. Each Authorized Supplier Person must establish and maintain a unique identifier for access and

of any Affiliate of CHS. Supplier will establish and document physical and electronic procedures to segregate and protect all information, data and communications (including, but not limited to, Covered Data).

9. **Security Breach Procedures**.

(a) Supplier will provide to the applicable CHS Party name and contact information for one or more representatives of Supplier (which may be a live-staffed help desk) who will serve as CHSôs primary security contact and be available to assist CHS twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with any actual or suspected Security Breach.

(b)

costs of any credit monitoring or other services required to mitigate such Security Breach for customers, end users, and other persons whose information was released as part of such Security Breach) arising from or otherwise related to any Security Breach.

10. **Coordination of this Addendum with Other Agreements**.

(a) The obligations in this Addendum are, wherever possible, to be regarded as additional to any other obligations in any agreement between Supplier and any CHS Party.

(b) Where possible, the provisions of this Addendum will be construed as consistent with those of other terms, conditions, and agreements between Supplier on the one hand and CHS on the other hand.

(c) Where the provisions of this Addendum cannot be construed consistently with the provisions of other terms, conditions, and agreements between Supplier on and CHS, the provision containing or imposing the greater restriction or protection benefitting the CHS Party will prevail.

Supplier:_____

Name:_____

Title:_____

Signature:_____

Date:_____

[i] The Center for Internet Security Critical Security Controls for Effective Cyber Defense work is licensed under a Creative Commons Attribution ï Non Commercial ï No Derivatives 4.0 International Public License. The link to the Critical Security Controls framework https://www.cisecurity.org/.