Data Privacy and Security Rider.

a) To the extent applicable for the activities carried out under this Agreement, CSI will comply with all applicable privacy and security laws applicable to CSI at the time and in the locations where the Services are provided or offered to Company in connection with this Agreement, including without limitation and to the extent applicable: the California Consumer Privacy Act, the requirements for service providers set forth in Massachusetts 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth, and other similar laws and regulations that prescribe requirements applicable to service providers of personal information, as may be enacted from time to time, ("Data Protection Legislation"). If CSI accesses or uses any personally identifiable information as defined in applicable Data Protection Legislation ("Personal Data") in the course of providing the Program, CSI will limit its access, review, use, processing, disclosure, or other handling of such data/information to the minimum necessary to perform its obligations hereunder. To the extent CSI accesses or processes cardholder or other financial account data in connection with this Agreement, then it represents and warrants that its information security program, and any processing of such financial account data by CSI, complies with the Payment Card Industry Data Security Standard ("PCI DSS"), ISO 22307, and ISO 27000, as applicable.

b) When providing or offering the Services to Company, CSI shall: (i) comply with all applicable Data Protection Legislation and any applicable Payment Card Information Data Security Standards when processing, storing, transmitting, or accessing any payment information (including, without limitation, credit card, debit card or financial account information); (ii) process the Personal Data only to the extent and is such manner as is necessary to provide the Services; (iii) ensure appropriate operational and technical measures are in place to safeguard the Personal Data against any unauthorized access, loss, destruction, theft, use or disclosure; (iv) ensure all third-party vendor or service provider engaged by CSI to process the Personal Data on CSI's behalf has entered into a written contract with CSI that meets the requirements established by the Data Protection Legislation; (v) not cause or permit Personal Data to be transferred outside the country in which the services are provided, except where the transfer is necessary for the conclusion or performance of the services; (vi) ensure any transfer of Personal Data outside the country in which services are provided is adequately protected as required by applicable Data Protection Legislation; (vii) promptly notify Company if CSI becomes aware of any unauthorized or unlawful processing or breaches of security relating to the Personal Data ("Security Incident"); (viii) promptly take all reasonable actions to address and resolve any Security Incident, including by informing Company of the occurrence of a Security Incident and the remediation process; and, (ix) notify Company of any request by law enforcement for Personal Data in advance of providing such data unless prohibited by applicable law.

c) As between the parties, information including but not limited to customer or vender name, address, email, account information, payment amount ("Company Data") that Company provides to CSI pursuant to this Agreement or that CSI acquires in connection with this Agreement is deemed "Company Data". CSI shall at all times: (i) use Company Data only as necessary to perform its obligations under this Agreement; (ii) maintain and protect Company Data in confidence, with reasonable security precautions at least as great as the precautions it takes to protect its own confidential information of similar importance; and, (iii) not permit the Company Data to be used, sold, licensed, leased, transferred, or distributed, in any form or by any means, without the prior written consent of Company. The parties acknowledge and agree that as a result of this Agreement, CSI may have contacts with vendors.

Cybersecurity. CSI represents and warrants that it has implemented and will maintain a written information security program that incorporates administrative, technical, and physical safeguards designed to ensure the security, confidentiality, integrity, and reliability of the Personal Data, Company Data, and the Services. Such safeguards are commensurate with the type and amount of data access and utilized by CSI in providing the Services. CSI shall take commercially reasonable efforts to protect Personal Data and Company Data against reasonably anticipated threats or hazards, including from unauthorized access, loss, destruction, use, modification, or disclosure. Without limitation to the foregoing, CSI agrees that the information security program it has implemented and maintains will: (i) identify appropriately defined organizational roles related to security and incident response; (ii) ensure compliance with Data Protection Legislation and meet or exceed the requirements thereunder; (iii) appropriately protect against the destruction, loss, disclosure, alteration or other accidental or unauthorized access to Personal Data in the possession of CSI; (iv) include appropriate controls with respect to the employment of and access given to employees of CSI, including (as appropriate) background checks, security clearances that assign specific access privileges to individuals, and training regarding the handling of Personal Data; (v) include an appropriate network security program that includes, without limitation, utilization of industry standard encryption technologies when appropriate and, in any case, with respect to Personal Data or Company Data; and (vi) reasonably ensure the integrity and reliability of such facilities, systems, service, which shall include, to the extent appropriate: (A) critical asset identification, (B) configuration and change management for software systems, (C) physical and environmental protection, and (D) contingency planning/redundancy.

Disaster Recovery and Backup CSI maintains the capability to resume provision of the Services from an alternative location, and via an alternative data communications route if necessary ("DR Services"), in the event of a problem, crisis or other incident which results in the inability of CSI to provide the Services for as sustained period of time ("Disaster"). As part of the Services, CSI will (i) maintain and manage Disaster recovery plans for the infrastructure utilized in performing the Services; and (ii) periodically, but at least once every year during the term of the Agreement, update and test the operability of the Disaster recovery plans in effect and make adjustments as are deemed necessary or advisable.