ADDITIONAL TERMS AND CONDITIONS SPECIFIC TO INFORMATION SECURITY AND DATA MANAGEMENT:

Data Compromise Response

a. Immediately upon becoming aware of a Data Compromise, or of circumstances that could have resulted in unauthorized access to or disclosure or use of Customer or End User Data, Vendor will notify Customer, fully investigate the incident, and cooperate fully with Customer's investigation of and response to the incident. Except as otherwise required by law, Vendor will not provide notice of the incident directly to the persons whose data were involved, regulatory agencies, or other entities, without prior written permission from Customer.

b. Notwithstanding any other provision of this agreement, and in addition to any other remedies available to Customer under law or equity, Vendor will reimburse Customer in full for all costs incurred by Customer in investigation and remediation of such Data Compromise, including but not limited to providing notification to third parties whose data were compromised and to regulatory agencies or other entities as required by law or contract; the offering of 12 months' credit monitoring to each person whose data were compromised; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Data Compromise.

Data Integrity

Vendor will take commercially reasonable measures, including regular data integrity audits, to protect Customer and End User Data against deterioration or degradation of data quality and authenticity.

Data Privacy

a. Vendor will use Customer Data and End User Data only for the purpose of fulfilling its duties under this Agreement and for Customer's and its End User's sole benefit, and will not share such data with or disclose it to any third party without the prior written consent of Customer or a as otherwise required by law. By way of illustration and not of limitation, Vendor will not use such data for Vendor's own benefit and, in particular, will not engage in "data mining" of Customer or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by Customer.

b. All Customer and End User Data will be stored on servers, located solely within the Continental United States.

c. Vendor will provide access to Customer and End User Data only those Vendor employees and subcontractors who need to access the data to fulfill Vendor's obligations under this Agreement. Vendor will ensure that employees who perform work under this Agreement have read, understood, and received appropriate instruction as to how to comply with, the data protection provisions of this Agreement, and have undergone all background screening and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the data they will be handling prior to being granted access to the Data.

Data Retention and Disposal

a. Vendor will use commercially reasonable efforts to retain data in an End User's account, including attachments, until the End User deletes them or for an alternative time period mutually agreed by the parties.

b. Using appropriate and reliable storage media, Vendor will regularly back up Customer and End User Data and retain such backup copies for a minimum of 12 months. At the end of that time period and at Customer's election, Vendor will either securely destroy or transmit to Customer repository the backup copies. Upon Customer's request, Vendor will supply Customer a certificate indicating the records destroyed, the date destroyed, and the method of destruction used.

c. Vendor will retain logs associated with End User activity for a minimum of 12 Months, unless the parties mutually agree to a different period.

d. Vendor will immediately place a "hold" on the destruction under its usual records retention policies of records that include Customer and End User Data, in response to an oral or written request from Customer indicating that those records may be relevant to litigation that Customer reasonably anticipates. Oral requests by Customer for a hold on record destruction will be reduced to writing and supplied to Vendor for its records as soon as reasonably practicable under the circumstances. Customer will promptly coordinate with Vendor regarding the preservation and disposition of these records. Vendor shall continue to preserve the records until further notice by Customer.

Data Security and Integrity

a. All facilities used to store and process Customer and End User data will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Vendor's own data of a s similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Vendor warrants that all Customer Data and End User Data will be encrypted in transmission (including via web interface) and storage at no less than 128 bit level encryption. Vendor agrees and certifies that it, the system or any third parties working on the vendor's behalf have complied with all applicable requirements to be considered PCI- level 1 compliant and has taken all necessary steps to validate its compliance with the PCI DSS and PA DSS. Vendor is required to demonstrated compliance with this requirement by maintaining the application listing on The PCI Security Standards Council (see https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php?agree=true).

b. Vendor will use industry standard and up to date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Agreement.

c. [for outsourced email services] Vendor will configure the Services to filter spam while permitting communications from third party Internet Protocol addresses identified by Customer as legitimate

d. Vendor will at its expense conduct or have conducted at least annually:

- A SAS 70 audit of Vendor's security policies, procedures and controls resulting in the issuance of a Service Auditor's Report Type II;
- A vulnerability scan, performed by a scanner approved by Customer, of Vendor's systems and facilities that are used in any way to deliver services under this Agreement; and
- A formal penetration test, performed by a process and qualified personnel approved by Customer, of Vendor's systems and facilities that are used in any way to deliver services under this Agreement.

e. Vendor will provide Customer upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this Agreement. Customer may require, at its expense, Vendor to perform additional audits and tests, the results of which will be provided promptly to Customer.

Data Transfer upon Termination or Expiration

a. Upon termination or expiration of this Agreement, Vendor will ensure that all Customer and End User Data are transferred to Customer or a third party designated by Customer securely, within a reasonable period of time, and without significant interruption in service. Vendor will ensure that such migration uses facilities and methods are compatible with the relevant systems of the transferee, and to the extent technologically feasible, that Customer will have reasonable access to Customer and End User Data during the transition.

b. Vendor will notify Customer of impending cessation of its business or that of a tiered provider and any contingency plans in the event of notice of such a failure. This includes immediate transfer of any previously escrowed assets and data and providing Customer access to Vendor's facilities to remove and destroy Customer owned assets and data. Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to Customer. Vendor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to Customer. Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on Customer, all such work to be coordinated and performed in advance of the formal, final transition date.

Response to Legal Orders, Demands or Requests for Data

a. Except as otherwise expressly prohibited by law, Vendor will:

- Immediately notify Customer of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking Customer and/or End User Data;
- Consult with Customer regarding its response;
- Cooperate with Customer's reasonable requests in connection with efforts by Customer to intervene and quash or modify the legal order, demand or request; and
- Upon Customer's request, provide Customer with a copy of its response.

b. If Customer receives a subpoena, warrant, or other legal order, demand or request seeking Customer or End User Data maintained by Vendor, Customer will promptly provide a copy to Vendor.

Vendor will promptly supply Customer with copies of data required for Customer to respond, and will cooperate with Customer's reasonable requests in connection with its response.