LINK #1 TO P.O.

Confidentiality, Privacy and Data Security

Exhibit [X] to Purchase Order Terms and Conditions

I. ADDITIONAL TERMS FOR PROCESSING PERSONALLY IDENTIFIABLE INFORMATION.

In addition to the terms in Section 12. Confidential Information and Ownership of Deliverables in the Purchase Order, the terms in this **Section I. ADDITIONAL TERMS FOR PROCESSING PERSONALLY IDENTIFIABLE INFORMATION** apply to Seller's Processing of PII.

1. **Organizational Program to Protect Confidential Information**. Seller will develop, implement, and maintain a comprehensive information security program ("Program" that: (i) is written (in one or more readily accessible parts); (ii) designates one or more employees to maintain the Program; (iii) sets forth the Technical and Organizational Security Measures for identifying, assessing, and mitigating reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing USCC Confidential Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including: (A) ongoing employee (including temporary and contract employee) training; (B) employee compliance with policies and procedures; and (C) means for detecting and preventing security system failures; (iv) develops security policies for employees (including temporary and contract employees) relating to the storage, access, and transportation of records containing Buyer's Confidential Information outside of business premises; (v) sets forth reasonable restrictions upon physical access to records containing Buyer's Confidential Information, and storage of such records and data in locked facilities, storage areas, or containers; (vi) regularly monitors to ensure that the Program is operating in a manner reasonably calculated to prevent unauthorized Processing of Buyer's Confidential Information; and upgrading information safeguards as necessary to limit risks; and (vii) reviews the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing Buyer's Confidential Information. Supplier will educate and train appropriate employees (including temporary and contract employees) consistent with the Program.

2. **Technical and Organizational Measures**. Seller will protect Buyer's Confidential Information with at least the same Technical and Organizational Security Measures and level of care with which it protects its own Confidential Information, but in no event with less than reasonable care and fully consistent with (i) Industry Standards (i.e., consistent with standards published by the National Institute of Standards and Technology ("NIST"), the International Organization for Standardization ("ISO") or other standards that have been publicly acknowledged and actually adopted by a substantial number of companies working with comparable information and which are recognized by reasonable experts in the field as acceptable) ("Industry Standards"), and (ii) all applicable legal requirements (collectively, "Minimum Technical and Organizational Security Measures").

3. **Access to Buyer's and Third Party Networks and Systems**. Neither Seller nor its Personnel may access Buyer's networks and systems and Third Party networks and systems that Process Buyer's Personally Identifiable Information ("PII") without Buyer approval and subject to the terms of the Order. Seller will protect access Buyer's networks and systems and Third-Party networks and systems approved by Buyer that Process Buyer PII with at least the following Technical and Organizational Security Measures:

   (i) secure user authentication protocols, including (A) control of user IDs and other identifiers; (B) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (C) control of data security passwords to ensure that such passwords are kept in a location and format that does not compromise the security of the data they protect; (D) restricting access to active users and active user accounts only; and (E) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system. Only those passwords that meet prevailing legal and Industry Standards for strength and complexity may be used;

   (ii) secure access control measures that (A) restrict access to records and files containing Buyer Confidential Information using access controls to those who need to know such information to perform the Services; and (B) assign unique identifications plus passwords, which are not default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls. The number of super-users or users with administrator access to Buyer Confidential Information should be limited;

   (iii) transport layer encryption (with a minimum encryption of TLSv1.2) and security protocols (equivalent to TLS, IPSEC, or SSH) to safeguard USCC Confidential Information during: (A) transmission over open, public networks; or (B) wireless transmission;

   (iv) reasonable monitoring of all systems for unauthorized Processing of Buyer Confidential Information;

   (v) reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of Buyer Confidential Information, including intrusion detection and data exfiltration monitoring tools for any environment in which Buyer Confidential Information will be placed;

   (vi) reasonably up-to-date versions of system security agent software which must include protection from and against Malware, which will reduce or eliminate the effects of any Malware installed or injected by itself or any Third Party and discovered in Seller's network, system, devices, or other equipment, and appropriate patches and definitions;

   (vii) not storing Buyer's Confidential Information on any Seller's information system except where necessary to perform the Services and not storing USCC Confidential Information on portable devices or media including laptop computers, smartphones, tablets, PDAs, removable hard disks, flash drives, and tapes, to the greatest extent feasible;

   (viii) physical facility security appropriate in light of the risks presented;

   (ix) except as otherwise agreed by the parties and specified in a Statement of Work, no remote/home access to Buyer's Confidential Information will be permitted, except by Seller's employees using VPN (with encryption and two-factor authentication) who are located in (A) the United States, (B) a country that is

within the European Economic Area, or (C) a country that is a member of the Organization for Economic Co-operation and Development;

(x) maintenance of active logs and audit trails of access to Buyer's Confidential Information that can reasonably determine the files and databases accessed, the user ID of the individual accessing the files and databases, the date and time of access, whether access was authorized or denied, and otherwise allow transactional changes to be reversed, provided that such logs and audit trails will be retained for a period of at least one year or longer if required by applicable law; and

(xi) application and database vulnerability assessments (mitigating any material issues).

4. **Inspection, Audits and Data Security Assessments**. Upon reasonable prior written notice, Buyer may conduct supervised on-site inspections and/or audits of any facilities used by Seller to access Buyer networks and systems, and Supplier will cooperate with Buyer regarding such inspections or audits. If Buyer determines that, as a result of any inspection or audit, Seller has been deficient or negligent in complying with the requirements of Section I, Buyer may request that Seller take immediate corrective action. If such corrective action is not taken to the reasonable satisfaction of Buyer, Buyer may immediately terminate this Order and all SOWs upon written notice to Seller. Prior to the execution of this Order, and not more than once annually thereafter during the term, Buyer also may require that Seller complete a data security assessment in a form specified by Buyer.

5. **Preservation of Data Quality.** Seller will implement and maintain appropriate processes to enable the access to and/or modification and/or correction of Buyer PII. Seller will preserve the accuracy of Buyer Confidential Information and, where required by applicable law or as otherwise directed by Buyer, Seller will update, amend, correct, or delete Buyer PII that Buyer informs Seller, or Seller otherwise knows, is inaccurate or incomplete. Supplier will perform back-ups of Buyer PII on a regular basis.

6. **Assurance of Protection**. Seller will maintain and, upon request from Buyer, provide all necessary documentation to evidence its compliance with this Order, including any Third Party audits or reports described herein subject to reasonable restrictions on disclosure. If Buyer determines that, as a result of any review of such document, Seller has been deficient or negligent in complying with the requirements of this Section I of Exhibit [x], Buyer may request that Seller take immediate corrective action. If such corrective action is not taken to the reasonable satisfaction of Buyer, Buyer may immediately terminate this Order and all SOWs upon written notice to Seller.

7. **Notification of Access Requests**. Seller must notify Buyer in writing as soon as reasonably practicable and in any event within three business days after: (i) any complaint about Processing of Buyer Confidential Information by Seller or any Third Party acting on behalf of Seller; (ii) any request for access from any government official or judicial or administrative proceeding relating to any Buyer Confidential Information (where not legally prohibited from doing so); or (iii) any other request related to Buyer Confidential Information from a Third Party. Seller will cooperate fully with Buyer in any effort of Buyer to intervene and quash or limit such requests.

8. **Processing PII Outside the United States**. To the extent Seller or any Personnel or subcontractor will Process PII outside of the United States, Seller will comply with all of the security and confidentiality restrictions set forth in this Order with respect to such Processing,

Commented [DDA1]: I removed the following: (a) countries that are in the EEA or (b) countries that are members of the OECD and (c) XXX except that Supplier may not store PII in XXXX unless expressly allowed in this agreement, a SOW or written amendment to this Agreement.

and Seller will ensure that all such Processing in countries other than the United States complies with the privacy and data protection laws of such countries. Notwithstanding the foregoing, Buyer may revoke and/or terminate the aforementioned authorization if (i) so directed by a governmental entity, regulatory authority. or court of competent jurisdiction; or (ii) in Buyer's reasonable opinion, changes in applicable laws, regulations, orders, or pronouncements from any regulatory or legal authority materially impact the legal risks to, and/or obligations of, Buyer associated with Seller's access to and/or use of PII at or from locations outside the United States.

9. **Processing PII in non-EEA or non-OECD Countries**. The following additional Technical and Organizational Security Measures will apply when Seller or any Personnel or subcontractor of Supplier is Processing PII in countries that are not members of the Organization for Economic Co-operation and Development and are not in the European Economic Area:

    a. PII while at rest must be protected using encryption (with a minimum of AES 256/256 encryption); and
    b. Seller will not store PII on any electronic medium, other than in transient storage incident to its transmission, unless Seller complies with the following further requirements for all such Processing of PII:
        i. implementation of enhanced measures to limit physical access to all PII, including use of electronic access controls, closed circuit television and intrusion detection systems, and entry control procedures, including delivery areas;
        ii. physical and logical separation of PII from the data of Seller's other customers;
        iii. prohibition of functioning drives and ports by which PII could be copied or saved onto portable electronic media;
        iv. prohibition on any local subcontracting of the Processing of PII; and
        v. prohibition on access to personal email and personal Internet access at any workstation accessing PII.

10. **Data Security Incidents**. Seller will notify Buyer immediately in the event of any Data Security Incident or other material failure of Seller to comply with the requirements of this Section I. but in no event later than three (3) days after awareness of such incident. Such notifications will include informing Buyer by calling Buyer's Incident Management Hotline at (877) 877-9768.

    a. Seller will not disclose the existence of a Data Security Incident without the express written permission of Buyer, except as necessary to inform Buyer, insurers, outside legal counsel, and forensic investigators, or as required by applicable law (in which case, it will provide Buyer with reasonable prior notice where permitted by applicable law to do so).
    b. Seller, at Seller's cost and expense, will assist and cooperate with Buyer concerning the investigation of the causes and scope of a Data Security Incident and the taking of remedial measures including the following: (i) Seller will fully cooperate with the response to regulatory inquiries, litigation, and other similar actions relating to any Data Security Incident; (ii) Seller will take such actions as may be necessary or reasonably requested by Buyer to understand and minimize the effects of the Data Security Incident, including steps to secure the affected Buyer Confidential Information and determine the scope of the Data Security Incident in a forensically sound manner; and (ii) Seller will document its responsive actions in writing and, if Buyer requests, will include a post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of Buyer Confidential Information. With the exception of urgent

action to understand and minimize the harm of the Data Security Incident, Seller will take action in response to a Data Security Incident only at the direction of Seller's counsel in anticipation of litigation resulting from such Data Security Incident, and it will mark all such documentation appropriately as "Attorney Work Product." Actions taken in response to any such Data Security Incident will be documented in writing if Buyer requests, and, if Buyer requests, Seller will include a post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of Buyer Confidential Information.

11. **Data Subject Access Requests**.
    a. Seller must notify Buyer in writing as soon as reasonably practicable and in any event within three (3) business days after receiving any data subject rights request that relates to PII Seller collected or maintains on Buyer's behalf and will cooperate with Buyer in verifying the authenticity of such request.

    b. Buyer reserves the right to require Seller to provide a copy of, update, correct, or delete all PII associated with a particular individual or household at any time, in Buyer's sole and absolute discretion (a "Data Request"), in accordance with the following:
        i. Data Requests will be provided to the Seller in writing and will identify individual(s) or household(s) whose information must be deleted;
        ii. Seller shall have thirty (30) days to comply with a Data Request by (A) providing a copy of the data in a reasonably accessible format or effecting the update, correction or deletion of data identified therein, and (B) providing written confirmation thereof to Buyer, provided that if Seller is required by law to retain information subject to a Data Request it shall promptly so advise Buyer in writing and Buyer will provide further direction;
        iii. Seller shall maintain complete and accurate records relating to its compliance with each Data Request (which records shall not include data that was the subject of a request). Buyer and its auditors shall have the right to review Supplier's compliance with any Data Request;
        iv. In connection with a Data Request Audit, Seller shall provide Buyer access at all reasonable times to the records relating to Data Requests; systems used to effect updates, corrections or deletion of information identified in such requests; and employees and contractors who facilitated compliance, in whole or part, with Data Requests.

12. **Background Checks for Personnel on Buyer's Premises or Processing SPII**. If Seller will have its Personnel on Buyer's premises with Buyer's badge or Processing SPII; Seller will conduct background checks, in each case only to the extent permissible under applicable law (including any such law requiring such person's consent), on its Personnel to whom Seller proposes to grant access to Buyer's facilities or Buyer's SPII. Seller will not allow access to any Buyer's premises or SPII by any Seller Personnel until such Personnel passes the background check. For any Supplier Personnel who is proposed to Process SPII, background checks will include the following to the extent these items are reasonably available in a given jurisdiction:

    a. Criminal Background Check. For any Supplier Personnel in the United States, a criminal background check covering each country, state, provincial and federal court district, or equivalent, in which such person has lived, worked or attended college or university in the last five years, to verify the absence of a crime involving violence against another person, dishonesty, a sex crime or any other serious crime equivalent to a felony under United States law. For any Supplier Personnel outside of the United

States, Supplier must obtain verification for any criminal record with the police, under whose jurisdiction the permanent address or longest stay in the last five years of the subject falls. In such case, a certificate of police authorities, if available, must be provided.

b. ID Verification. Reasonable efforts to ensure that such person has not falsified his or her documents indicating such person's identity, including his or her passport, marriage certificate (if any) and other personal documents.
c. Employment Check. Verification of the employment claimed by such person and such person's qualifications, which may include the education levels and degrees such person claims to have completed and received.
d. Database Check. For any Supplier Personnel outside of the United States, Supplier must conduct a search for information pertaining to the employee or employee candidate in relevant databases pertaining to court decisions, brokers and brokerages, loan defaults, law enforcement activities, and relevant public information. In addition, search must be conducted on national news and media resources and the United States Office of the Foreign Asset Control database.
e. Drug Screen. Testing of such person for the unlawful use of illegal drugs to the extent allowed by applicable law.

13. **Mobile Applications, Websites, Online Services and Location Based Services**. Seller or any and all subcontractors and Personnel of Seller will Process personal information using mobile applications, websites, and online services in compliance with all applicable laws and regulations including, without limitation, the Children's Online Privacy Protection Act (COPPA), the California Consumer Privacy Act (CCPA), the California Online Privacy Protection Act (CaOPPA), and the California "Shine the Light" Law. Supplier will conspicuously post or provide a link to a copy of Supplier's privacy policy on such mobile applications, websites, and online services. If PII is Processed by Seller using mobile applications, websites and online services, Supplier will conspicuously post or provide a link to a copy of Buyer's privacy statement on such mobile applications, websites, and online services. Seller will Process such PII in compliance with Buyer's privacy statement. Seller will notify Buyer no fewer than sixty (60) days prior to engaging in the collection of PII from children under 13. Seller will notify Buyer no fewer than sixty (60) days prior to engaging in the collection of data from a particular computer or device regarding website viewing behaviors over time and across non-affiliate websites or mobile applications for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such website or mobile application viewing behaviors (collectively, "Online Behavioral Advertising"). If Seller engages in Online Behavioral Advertising, Seller will (i) disclose to USCC any use of cookies, beacons, and other tracking technologies, how "do not track" signals are responded to and any supported mechanisms that allow consumers to limit collection of such information or the use of cookies, and whether any PII will be disclosed to third parties; (ii) disclose prominently in its privacy policy any use of cookies, beacons, and other tracking technologies and will specify at least whether cookies are used, how "do not track" signals are responded to, and any supported mechanisms that allow consumers to limit collection of such information or the use of cookies, or otherwise opt-out of Online Behavioral Advertising, and if information is "sold" pursuant to the CCPA, offer an opt out of the sale of Personal Information; (iii) comply with the CCPA and similar state statutes; (iv) comply with Digital Advertising Alliance's (DAA's) Self-Regulatory Principles; and (v) if Supplier is a member of the Network Advertising Initiate (NAI), comply with the NAI Code of Conduct and NAI Mobile Application Code. Seller will notify Buyer no fewer than sixty (60) days prior to linking location information to a specific device (e.g. linked by phone number, userID) or a specific person (e.g. linked by name or other unique identifier) to provide or enhance a service. If Seller engages in

such location-based services, Seller will comply with the Cellular Telephone Industry Association's Best Practices and Guidelines for Location-Based Services.

II. ADDITIONAL TERMS FOR PROCESSING SENSISTIVE PERSONALLY INDENTIFIABLE INFORMATION.

In addition to the terms in **Section I. ADDITIONAL TERMS FOR PROCESSING PERSONALLY IDENTIFIABLE INFORMATION**, the terms in **Section II. ADDITIONAL TERMS FOR PROCESSING SENSISTIVE PERSONALLY INDENTIFIABLE** apply to Seller's Processing of SPII.

1. **Additional Technical and Organizational Security Measures for SPII.** To the extent that Seller Processes SPII, Seller will protect Buyer's SPII with at least the following Technical and Organization Security Measures:

    a. the terms of Section I. of this Order will apply to Seller's Processing of Buyer's SPII, notwithstanding Seller's access to Buyer's network and systems;
    b. encryption (with a minimum of AES 256/256 encryption) of SPII while at rest;
    c. Buyer SPII while stored on portable devices or media, including laptop computers, smartphones, tablets, PDAs, removable hard disks, flash drives, and tapes, must be protected using encryption (with a minimum of AES 256/256 encryption);
    d. hardcopy shipments of documents containing Buyer SPII must be undertaken using Seller employees and maintained in secure enclosures during shipment; and
    e. procedures for the secure disposal of printed materials containing Buyer SPII.

2. **Third Party Independent Reports.** On an annual basis, when Seller is Processing Buyer's SPII, Seller provide Buyer with either a SOC 2, Type II Report or an ISO Report as fully explained below.

    a. SOC 2, Type II Report. Seller will retain an independent, registered public accounting firm that is nationally recognized in the United States to perform an audit or series of audits of the control activities, systems, and processes established and maintained by Seller and its subcontractors to provide the Services and any other services then being provided to Buyer under this Order. Each such annual audit or series of audits will (i) include in its sample all locations from which Services are provided under this Order or SOWs and the computer, network, telephony, and other information technology systems used to support the Services provided from those locations; and (ii) conform to the requirements necessary to produce a SOC 2, Type II Report as set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (American Institute of Certified Public Accountants ("AICPA"), Technical Practice Aids) and AT section 101, Attest Engagements, or in any successor or substitute statement adopted by the AICPA (such report being referred to as a "SOC 2 Report"). Supplier will provide a SOC 2 Report (A) at the time of execution of this Agreement, but no later than 60 days after the Effective Date; and (B) annually during the term of this Agreement, but no later than 12 months after the date that the previous SOC 2 Report was provided. In addition, Seller will promptly notify Buyer of any areas of significant concern identified in any SOC 2 Report or, on an interim basis, of any areas of significant concern expected to be identified in any future SOC 2 Report, and will provide to Buyer periodic reports regarding Seller's efforts and progress towards resolving such areas of concern. If

Seller is not able to remedy such significant areas of concern to the satisfaction of Buyer, Buyer will have the immediate right, upon written notice to Seller, to terminate this Order and any applicable SOWs without penalty.

b. ISO Report. Seller will retain an accredited certification body that is nationally recognized in the United States to perform an audit or series of audits of the control activities, systems and processes established and maintained by Supplier as a requirement for Seller's ISO 27001:2013 certification (such report being referred to as an "ISO Report"). Seller will provide an ISO Report (i) on the Effective Date, but no later than 60 days after the Effective Date; and (ii) annually during the term of this Order, but no later than 12 months after the date the previous ISO Report was provided. In addition, Seller will promptly notify Buyer of any areas of significant concern identified in any ISO Report which impact Buyer or Buyer's services and will provide to Buyer periodic reports regarding Supplier's efforts and progress towards resolving such areas of concern. If Seller is not able to remedy such significant areas of concern to the satisfaction of Buyer, Buyer will have the immediate right, upon written notice to Seller, to terminate this Order and any applicable SOWs without penalty.

3. **Processing of Payment Card Information.** If Seller Processes Payment Card Information ("PCI") under this Order, Seller will comply with the following.

Commented [KBJ2]: Should this be part of the PO?

a. PCI-DSS Compliance. At all times during the term of this Order, if Seller transmits, stores or Processes PCI, Seller will comply with the applicable, current version of the Payment Card Industry Data Security Standard ("PCI DSS"), as adopted by the PCI Security Standards Council, LLC (or its successor or affiliated organization), with respect to any instance in which Seller Processes Payment Card Cardholder Data or Sensitive Authentication Data (as each of those terms is defined in the PCI DSS) in connection with the Services including the standards pertaining to storage of Sensitive Authentication Data. In no event will Seller retain any security code data, PIN verification code numbers, or the full contents of magnetic stripe data, subsequent to the authorization of a Payment Card transaction (as the term is defined in the PCI DSS) or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. Seller will provide to Buyer an Attestation of Compliance for Service Providers or Merchants, as appropriate ("Attestation of Compliance") as outlined in the PCI DSS with respect to Seller's processing, storing, or transmitting of Payment Card Cardholder Data or Sensitive Authentication Data: (i) on the Effective Date, which represents an Attestation of Compliance that was issued no longer than 12 months preceding the Effective Date; and (ii) annually during the term of this Agreement, but no later than 12 months after the date that the previous Attestation of Compliance was provided. Buyer may immediately terminate this Order and all SOWs upon written notice without penalty if Seller fails to comply with this paragraph. [**Note**: Need to determine Card Registration language].

b. PA-DSS Compliance. At all times during the term of this Order, if Seller uses or develops a payment application that stores, transmits or Processes PCI, Seller will comply with the applicable, current version of the Payment Card Industry Application Data Security Standard ("PA-DSS"), as adopted by the PCI Security Standards Council, LLC (or its successor or affiliated organization). Seller will provide to Buyer an Attestation of Validation to ensure that Seller's payment application complies with the PA-DSS. Seller must provide the Attestation of Validation: (i) on the Effective Date that was issued no longer than 12 months preceding the Effective Date; and (ii)

annually during the term of this Agreement but no later than 12 months after the date that the previous Attestation of Validation was provided. Buyer may immediately terminate this Order and all SOWs upon written notice without penalty if Seller fails to comply with this paragraph.

c. Card Organization Registration. [**Need to work with Treasury**]. In addition to the requirements set out in Sections 12(m) and (n), at all times during the term of this Order, Seller will fully cooperate with Buyer and its merchant acquirer(s), as directed by Buyer, to ensure that Seller is properly and currently registered with the entities formed to administer and promote credit and/or debit cards (each a "Card Organization") as required by Buyer in connection with the Services. Seller will be responsible for (i) the payment of any fees (initial and renewal) for such registration required by the applicable Card Organizations; (ii) complying with the registration process of the applicable Card Organizations and/or USCC's merchant acquirer(s), including any site inspections, background investigations, and provision of financial statements and other requested information; (iii) complying with any periodic and other reporting required by an applicable Card Organization, including compliance reviews and attestations and network scans; (iv) maintaining such registration on an annual basis; and (v) complying with the Card Organization Rules of the applicable Card Organizations, including without limitation, those requiring security of Payment Card Cardholder Data. Seller will promptly notify Buyer and its merchant acquirer(s) upon the occurrence of any change to the information provided by it to the Card Organizations, such as any change to any of the following: (A) Seller's legal name or business aliases; (B) Seller's business address; (C) Seller's point of contact for the Card Organizations; (D) Seller's compliance status with PCI DSS; (E) Seller's legal entity status (such as a result of a merger); or (F) Supplier's financial solvency status. "Card Organization Rules" means the rules, regulations, releases, interpretations, and other requirements (whether contractual or otherwise) imposed or adopted by any applicable Card Organization and related authorities, including those of the PCI Security Standards Council, LLC (or its successor or affiliated organization), and the National Automated Clearing House Association. "PCI-DSS" means the applicable, current version of the Payment Card Industry Data Security Standard, as adopted by the PCI Security Standards Council, LLC (or its successor or affiliated organization). Buyer may immediately terminate this Order and all SOWs without penalty upon written notice if Seller fails to comply with this paragraph.

III. DEFINTIONS.

1. "Confidential Information" means, with respect to a party (including, with respect to Buyer, its Affiliates, as applicable), this Order, together with all confidential business or technical information or materials of such party; provided, however, that Confidential Information will not include information or materials that the Receiving Party (as defined in Section 12) can demonstrate: (i) was known to the Receiving Party prior to the date of receipt free of any obligation of nondisclosure; (ii) was generally known or available to the public prior to the date of disclosure to the Receiving Party or subsequently became generally known or available to the public, except through a Data Security Incident or by fault of the Receiving Party; (iii) was lawfully received by the Receiving Party from a Third Party free of any obligation of nondisclosure; or (iv) is or was independently developed by the Receiving Party without reference to any Confidential Information of the Disclosing Party (as defined in Section 12). Buyer Confidential Information means any

Confidential Information of Buyer provided by or on behalf of Buyer to Seller or that is otherwise obtained by Seller in connection with this Order including Deliverables and PII.

2. "Data Security Incident" means the actual or reasonably suspected (i) unauthorized access, acquisition, exfiltration, disclosure, theft, loss or misuse of Buyer Confidential Information, or (ii) any other inadvertent, unauthorized, or unlawful Processing of Buyer Confidential Information that compromises its security, confidentiality, or integrity, or otherwise creates a substantial risk of identity fraud or theft, regardless of the form of the Confidential Information.

3. "Malware" means any virus, timer, clock, counter, time lock, time bomb, Trojan horse, worm, file infector, boot sector infector, or other limiting design, instruction, or routine that could, if triggered, erase data or programming or cause the resources to become inoperable or otherwise incapable of being used in the full manner for which such resources were intended to be used.

4. "Personally Identifiable Information" or "PII" is a subset of Confidential Information and means information that identifies, relates to, describes, or could be reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household that is provided to Seller by Buyer or otherwise obtained by Seller in connection with this Order. Individuals whose data is encompassed by this definition may include, but are not limited to, customers, potential customers, and employees. Without limiting the foregoing, PII includes any of the following information, to the extent such information can be associated with, or could be reasonably linked with an individual or household: (i) an individual's first and last name, government issued number or identifier, date of birth, home or other physical address, e-mail address or other online contact information, telephone number, financial account number, credit or debit card number, biometric data, or mother's maiden name; (ii) personally identifiable "Customer Proprietary Network Information" ("CPNI"), as defined in the Communications Act of 1934 (at 47 U.S.C. § 222(h)) and its implementing regulations; (iii) a unique persistent identifier associated with an individual or a networked device including static or dynamic (with date and time) IP address, customer number held in a cookie, user ID, browser fingerprint, processor serial number, device serial number, or any other number that uniquely identifies a particular telecommunications device, processor, or computer, combined with any other information relating to an individual; (iv) a password, personal identification number, access code, answer to a security question, and any other security credential that provides access to PII; (v) records of personal property, products or services purchased, obtained or considered; purchasing or consuming histories or tendencies; and any inferences drawn from any of the information in this Section 4 to create a profile of an individual's preference or characteristics; (vi) information about an individual's internet or other electronic network activity information such as browsing and search histories; (vii) geolocation data; (viii) professional, educational, or employment-related information.

Commented [DDA3]: We view this as SPII. Should this be shifted into the definition of SPII?

5. "Personnel" means the employees, contractors, agents, and representatives of a party, including the employees, employee candidates, contractors, and agents of such party's subcontractors or other Third Parties.

6. "Process" or "Processing" means any operation or set of operations that is performed upon Confidential Information, whether or not by automatic means, including collecting, recording, organizing, storing, accessing, adapting, altering, retrieving, consulting, using, corrupting, transferring, transmitting, selling, renting, disclosing, disseminating, making available, aligning, combining, deleting, erasing, or destroying.

7. "Sensitive Personally Identifiable Information" or "SPII" means a subset of Personally Identifiable Information and means all: (i) government-issued identification numbers including

Social Security Numbers, driver's license numbers, identification numbers, and passport numbers; (ii) financial institution account numbers; (iii) credit or debit card "Primary Account Numbers" (PANs), Service Codes, and Sensitive Authentication Data, as those terms are defined in the current version of the "Payment Card Industry Data Security Standard" (PCI DSS), as adopted by the PCI Security Standards Council, LLC (or its successor or affiliated organization); (iv) "Protected Health Information" (PHI), as defined in regulations relating to the Health Insurance Portability and Accountability Act, as amended, and implementing regulations, 45 CFR §160.103; information related to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; the past, present, or future payment for the provision of health care to an individual; or any other individual medical, medical history, health, biometric, disability, or genetic information; (v) passwords, personal identification numbers, access codes, answers to security questions, and other security credentials that provide access to SPII as defined elsewhere in this definition; (vi) videos or photographs of identifiable individuals in private areas, including home security monitoring footage; (vii) real-time geolocation information associated with information that identifies, relates to, describes, or could be reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual; and (viii) any other Personally Identifiable Information that Buyer reasonably designates for Seller in writing as Sensitive Personally Identifiable Information. SPII only includes such information as is provided by or on behalf of Buyer to Seller or any Personnel or subcontractor of Seller or is otherwise obtained by Seller or any Personnel or subcontractor of Seller in connection with this Order.

Commented [KBJ4]: New definition.

8. "Technical and Organizational Security Measures" means appropriate administrative, technical, and physical safeguards sufficient to protect against reasonably anticipated threats or hazards to the security, integrity, and confidentiality of Confidential Information (including any unauthorized Processing of Confidential Information) commensurate with the type of Confidential Information in Seller's possession, custody, or control, including all such measures required by applicable laws.

9. "Third Party" means any person or entity that is not a party to this Agreement, including either Party's subcontractors, agents, service or content providers, subsidiaries and affiliates or any other Third Party acting on behalf of or for such party.