DATA PROCESSING ADDENDUM

Traxo, Inc. ("**Traxo**" or "**Processor**") and _____ (the "**Client**" or "**Controller**") have entered into a written agreement or agreements (the "**Agreement**") pursuant to which Traxo provides data processing services to Client (the "**Services**") that may entail the Processing of Personal Information (as defined below).

The EU General Data Protection Regulation imposes specific obligations on Data Controllers with regard to their vendor relationships, including obligations to have agreements in place containing various provisions relating to data protection.

Traxo and Client desire to amend their Agreement dated _____ through this Data Protection Addendum to Agreement between Traxo, Inc. and Client (this "**Addendum**") to address the obligations of the parties regarding the Processing of Personal Information received by Traxo from Client on behalf of its personnel, customers, and users in the European Union that is subject to Traxo's obligations under the EU General Data Protection Regulation.

This Addendum is hereby incorporated by reference into the Agreement in order to demonstrate the parties' compliance with the EU General Data Protection Regulation.

1. Effectiveness

1.1 **Termination.** This Addendum will terminate upon the earliest of: (i) termination of the Agreement as permitted hereunder or by Traxo's Terms and Conditions (and without prejudice to the survival of accrued rights and liabilities of the parties and any obligations of the parties which either expressly or by implication survive termination); (ii) as earlier terminated pursuant to the terms of this Addendum or (iii) as agreed by the parties in writing.

2. Definitions

"**Customer Data**" means all electronic data submitted to, or made available to, Traxo by or on behalf of Client.

"**Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, and the GDPR, in each case which are applicable to the Processing of Personal Data under the Agreement and which are applicable to Client.

"**EU General Data Protection Regulation**" and "**GDPR"** means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

"**Personal Information**" or "**Personal Data**" shall mean any information relating to an identified or identifiable natural person ("**Data Subject**"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity, in each case which such data is Customer Data.

"**Process**" or "**Processing**" shall mean any operation or set of operations which is performed upon Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, transfer, and erasure or destruction.

"Sub-processor" means any Third Party (including any third party, but excluding an employee of Traxo)

appointed by or on behalf of Traxo to Process Personal Data on behalf of Client under the Agreement.

"**Third Party**" means a natural or legal person, public authority, agency or body other than the Data Subject, Traxo, Client and persons who, under the direct authority of Traxo or Client, are authorized to Process Personal Information.

The terms, **"Commission"**, **"Member State"**, **"Personal Data Breach"**, and **"Supervisory Authority"** shall have the same meaning as in the GDPR, and shall be construed accordingly.

3. Processing of Personal Data

3.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Client is the Controller, Traxo is a Processor and that Traxo may engage Sub-processors pursuant to the requirements set forth in Section 5 **"Sub-processors"** below.

3.2 **Client Authority.** Client represents and warrants that it is and will at all relevant times remain duly and effectively authorized to give the instruction set forth in Section 3.4 below on behalf of itself.

3.3 **Provision of the Service; Client Responsibility**. Traxo provides the Service to Client under the Agreement. In connection with the Service, the parties anticipate that Traxo may Process Customer Data that contains Personal Information relating to Data Subjects. Client shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws. Client's instructions for the Processing of Personal Data shall comply with Data Protection Laws. In addition, Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data.

3.4 Traxo's Processing of Personal Data.

a. Processing Purposes. Traxo shall keep Personal Information confidential and shall only Process Personal Data for the purpose of the provision of the Services under the Agreement and in accordance with Client's documented instructions which are consistent with the terms of the Agreement, unless Processing is required by Data Protection Laws to which Traxo (or the applicable Sub-processor) is subject, in which case Traxo shall to the extent permitted by the Data Protection Laws inform Client of that legal requirement before the relevant Processing of that Personal Data. Traxo shall not be required to comply with or observe Client's instructions if such instructions would violate applicable Data Protection Laws.

b. This Addendum, the Agreement and any Statement of Work thereunder, are Client's complete and final instructions to Traxo for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately.

c. The following are deemed instructions of the Client to Traxo: The Processing of Personal Data (i) in accordance with the Agreement, this Addendum and any Statement of Work under the Agreement, including without limitation with the transfer of Personal Data to any country or territory; and (ii) to comply with other documented instructions provided by Client where such instructions are consistent with the terms of the Agreement, this Addendum, and applicable Data Protection Laws.

3.5 **Details of the Processing.** The subject-matter of Processing of Personal Data by Traxo is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under the Agreement, as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws), are further specified in Exhibit A to this Addendum, as may be amended by the parties from time to time.

4. Traxo Personnel

Throughout the term of this Addendum, Traxo shall restrict its personnel from Processing Personal Data without authorization by Traxo and shall limit the Processing to that which is needed for the specific individual's job duties in connection with Traxo's provision of the Services under the Agreement. Traxo will impose appropriate contractual obligations on its personnel, including relevant obligations regarding confidentiality, data protection and data security. Traxo shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and have received appropriate training regarding their responsibilities.

5. Sub-processors

5.1 **Appointment of Sub-processors.** For the purpose of the appointment of Sub- processors, Client acknowledges and agrees that Traxo may engage third-party Sub-processors in connection with the provision of the Services, including without limitation the Processing of Personal Data.

5.2 **List of Current Sub-processors and Notification of New Sub- processors.** When requested by the Client, Traxo shall make available to Client an up-to-date list of all Sub-processors used for the processing of Personal Data.

5.3 **Objection Right for New Sub-processors.** Traxo shall give Client prior written notice of the appointment of any new Sub-processor, including full details of the Processing to be undertaken by the Sub-processor. If, within 14 days of receipt of that notice, Client notifies Traxo in writing of any objections (on reasonable grounds) to the proposed appointment, then (i) Traxo shall work with Client in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor; and (ii) where such a change cannot be made within 14 days from Traxo's receipt of Client's notice, notwithstanding anything in the Agreement, Client may by written notice to Traxo with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub-processor.

5.4 **Sub-processing Agreement; Liability.** Traxo has or shall enter into a written agreement with each Sub-processor (the **"Sub-processing Agreement"**) containing data protection obligations not less protective than those in the Agreement and/or this Addendum with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor. Traxo shall be liable for the acts and omissions of its Sub-processors to the same extent Traxo would be liable if performing the services of each Sub-processor directly under the terms of this Addendum.

5.5 **Copies of Sub-Processor Agreements.** Traxo shall provide to Client for review copies of the Sub-processor agreements as Client may reasonably request from time to time. The parties agree that all commercial information may be removed by the Traxo beforehand. The parties agree that copies of the Sub-processor agreements that must be provided by Traxo to Client may have all commercial information removed by Traxo beforehand.

6. Security

6.1 **Adequate Measures.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Traxo shall in relation to the Personal Data implement and maintain throughout the term of this Addendum, the technical and organizational measures set forth in Exhibit B (the **"Security Measures"**). Client acknowledges and agrees that it has reviewed and assessed the Security Measures

and deems them appropriate for the protection of Personal Data.

7. Data Subject Rights

7.1 **Correction, Blocking and Deletion.** Traxo shall comply with any commercially reasonable request by Client to correct, amend, block or delete Personal Data, as required by Data Protection Laws, to the extent Traxo is legally permitted to do so.

7.2 **Data Subject Requests**. To the extent legally permitted, Traxo shall promptly notify Client if Traxo receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**"). Factoring into account the nature of the Processing, Traxo shall assist Client by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Client, in its use of the Services, does not have the ability to address a Data Subject Request, Traxo shall, upon Client's request, provide commercially-reasonable efforts to assist Client in responding to such Data Subject Request, to the extent that Traxo is legally authorized to do so, and the response to such Data Subject Request is required under Data Protection Laws. To the extent legally permitted, Client shall be responsible for any costs arising from Traxo's provision of such assistance.

8. Personal Data Breach

8.1 **Notification of Data Breach.** Traxo shall, to the extent permitted by law, notify Client without undue delay upon Traxo becoming aware of a Personal Data Breach affecting Personal Data, providing Client with sufficient information to allow Client to meet any obligations to report such Personal Data Breach to a Supervisory Authority or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2 **Assistance to Client** Traxo shall co-operate with Client and take such reasonable commercial steps as are directed by Client to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Traxo shall provide reasonable assistance to Client with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which Client reasonably considers to be required of it by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law & Regulation, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, Traxo or the Sub-processors

10. Return or Destruction of Personal Data.

10.1 **Return or Deletion.** Subject to the provisions of Section 10.2 below, at Client's election, made by written notice to Traxo following 30 days of the date of cessation of any Services involving the Processing of Personal Data (the **"Cessation Date"**), Traxo shall: (a) return a complete copy of all Personal Data to Client in such format and manner requested by Client and reasonably acceptable to Traxo; and (b) to the extent permitted by applicable laws, delete and procure the deletion of all other copies of Personal Data Processed by Traxo or any Sub-processor. Traxo shall comply with any such written request within 30 days of the Cessation Date.

10.2 **Retention of Copies.** Traxo and each Sub-processor may retain Personal Data to the extent required by applicable European Union law or the law of an EU Member State and only to the extent and for such period

as required by such laws and always provided that Traxo shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in such law requiring its storage and for no other purpose.

11. Audit.

11.1 **Report on Compliance.** Subject to the provisions of Section 11.3 below, at Client's written request, Traxo will provide Client all information necessary to demonstrate compliance with this Addendum. To the extent Traxo has acquired a confidential Service Organization Control (SOC) 2 Report (or a comparable report) on its systems examining logical security controls, physical security controls, and system availability, as produced by a Third Party auditor in relation to the Services (**"SOC 2 Report"**), Traxo will provide such report. The information provided will constitute Traxo Confidential Information under the confidentiality provisions of the Agreement or a non-disclosure agreement, as applicable.

11.2 **Audit.** Traxo shall allow for and contribute to audits, including inspections, by any Client or an auditor mandated by Client in relation to the Processing of the Personal Data by Traxo or Sub-processors in accordance with Sections 11.1 and 11.3 to this Addendum.

11.3 **Process.** The parties agree that the audits described in Section 11.2 above shall be carried out in accordance with the following specifications:

a. Client may contact Traxo in accordance with the **"Notices"** Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Client may also review the SOC 2 Report or another audit of Traxo's systems by and independent third party (**"Third Party Audit"**) if such a report is available.

b. Client shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Traxo or Sub-processor premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

c. Before the commencement of any such on-site audit, Client and Traxo shall mutually agree upon the scope, timing, and duration of the audit.

d. Traxo or Sub-processor need not give access to its premises for the purposes of such an audit or inspection:

   i. to any individual unless he or she produces reasonable evidence of identity and authority;

   ii. outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Client undertaking an audit has given notice to Traxo that this is the case before attendance outside those hours begins; or

   iii. for the purposes of more than one audit or inspection, in respect of Traxo or each Sub-processor, in any calendar year, except for any additional audits or inspections which: (A) Client reasonably considers necessary because of genuine concerns as to Traxo's or applicable Sub- processor's compliance with this Addendum; or (B) Client is required or requested to carry out by Data Protection Law and Regulation, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory; where Client has identified its concerns or the relevant requirement or request in its notice to Traxo.

11.4 Following the Audit:

a. If Client chooses to conduct an independent audit rather than rely on a current SOC 2 Report or current Third Party Audit, if applicable and available, or if Client makes such choice because a current SOC 2 Report or current Third Party Audit is not available, Client will be responsible for any fees charged by any auditor appointed by Client to execute any such audit. Traxo will provide Client with further details of any applicable fee, and the basis of its calculation, in advance of any such review or audit.

b. Client shall promptly notify Traxo with information regarding any non- compliance discovered during the course of an audit.

12. Transfer of Data.

Traxo complies with both the EU-US Privacy Shield and Swiss-US Privacy Shield frameworks. Traxo may transfer personal data from the EEA to the United States for purposes of this Addendum pursuant to the EU-US Privacy Shield and Swiss-US Privacy Shield provided that Traxo maintains its certification under the EU-US Privacy Shield and Swiss-US Privacy Shield. In compliance with the Privacy Shield Principles, Traxo commits to resolve complaints about our collection or use of personal information. EU and Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact Traxo at: Chris.Stevens@Traxo.com. Traxo has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved Privacy Shield complaints concerning human resources data transferred from the EU and Switzerland in the context of the employment relationship, and will cooperate with the United States Federal Trade Commission (FTC) on matters relevant to its jurisdiction. Traxo may also transfer personal data from the EEA to the United States pursuant to Standard Contractual Clauses as mutual agreed by the Parties.

13. Indemnification; Limitation of Liability

If one party is held liable for a violation of this Addendum committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred in accordance with the provisions of the "Indemnification" Section of the Agreement. Each party's liability, taken together in the aggregate, arising out of or related to this Addendum, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement. For the avoidance of doubt, Traxo's total liability for all claims from the Client or any third party arising out of or related to the Agreement and this Addendum shall apply in the aggregate for all claims under both the Agreement and this Addendum.

All other aspects, terms and conditions of the Agreement, and the exhibits and any prior addenda thereto, shall remain in full force and effect except as modified by this Addendum.

Traxo, Inc.	**[Client]**
By: Cara Whitehill	**By:** _____
Printed Name: Cara Whitehill	**Printed Name:** _____
Title: Chief Commercial Officer	**Title:** _____
Date: August 1, 2020	**Date**: _____

EXHIBIT A TO DATA PROCESSING ADDENDUM: DETAILS OF PROCESSING

1. Data subjects

1.1 The Data Processor may process Personal Data about the following categories of Data Subjects on behalf of the Data Controller:

- Client customers
- Client employees
- Client contractors
- Other representatives of the Client

2. Personal data

2.1 The Data Processor processes the following **special categories of personal data** about the categories of Data Subjects above on behalf of the Data Controller:

- n/a

2.2 The Data Processer may process the following **general categories of personal data** about the categories of Data Subjects below on behalf of the Data Controller:

- Name
- Email
- Employer affiliation
- Loyalty program or membership number
- Phone Number

2.3 The personal data under the categories above are collectively referred to as the "**Personal Data**".

3. Nature and Purpose of the processing

3.1 The Data Processor's processing of Personal Data on behalf of the Data Controller is carried out for the following nature and purpose:

- Traveler itinerary management
- Traveler expense information

4. Data processing activities/nature of processing operation

4.1 The Data Processor's processing of Personal Data for the Data Controller is carried out through any or all of the following activities:

- Ingestion of client account and user information via email, API, ETL and parsing, to create databases for client solutions.
- Parsing of client travel itineraries to extract itinerary and cost information.
- Integration of travel itinerary and cost information into client's desired endpoints
- Rendering of relevant itinerary data in a browser-based reporting tool for authorized users of data exporter to access.

5. Duration

5.1 The Parties expect that the Data Processor will be processing the Personal Data for the initial period set out in the Agreement and, then, for as long as the Agreement is automatically renewed.

EXHIBIT B TO DATA PROCESSING ADDENDUM: SECURITY MEASURES

1. Personnel. Data Importer's personnel will not process customer data without authorization. Personnel are obligated to maintain the confidentiality of any customer data and this obligation continues even after their engagement ends.

2. Data Privacy Contact

Traxo, Inc.
Attn: Chris Stevens, CTO
6125 Luther Lane, #224
Dallas, TX 75225

3. Technical and Organization Measures. The Data Importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

3.1 Organization of Information Security.

a. *Security Roles and Responsibilities.* The Data Importer has appointed Chris Stevens as the security officer responsible for coordinating and monitoring the security rules and procedures. A Data Protection Officer is not required.

b. *Duty of Confidentiality.* The Data Importer's personnel with access to customer data are subject to confidentiality obligations.

3.2 Risk Management.

The Data Importer conducts regular testing and monitoring of the effectiveness of its safeguards, controls, systems, including conducting penetration testing. The Data Importer implements measures, as needed, to address vulnerabilities discovered in a timely manner.

3.3 Storage.

The Data Importer's database servers are hosted in a data center operated by Amazon Web Services, that has been qualified per the Data Importer's vendor management procedure. The Data Importer maintains complete administrative control over the virtual servers, and no third-party vendors have logical access to customer data.

3.4 Asset Management.

a. *Asset Inventory.* The Data Importer maintains an inventory of all media on which customer data is stored. Access to the inventories of such media is restricted to authorized personnel.

b. *Asset Handling.*

   i. The Data Importer employees are required to utilize encryption to store data in a secure manner and are required to use two-factor authentication to access Traxo's networks.

ii. The Data Importer imposes restrictions on printing customer data and has procedures for disposing of printed materials that contain customer data.

iii. The Data Importer's personnel must obtain authorization prior to storing customer data on portable devices, remotely accessing customer data, or processing customer data outside the Data Importer's facilities.

3.5 Software Development and Acquisition: For the software developed by Data Importer, Data Importer follows secure coding standards and procedures set out in its standard operating procedures.

3.6 Change Management: Data Importer implements documented change management procedures that provide a consistent approach for controlling, implementing, and documenting changes (including emergency changes) for the Data Importer's software, information systems or network architecture. These change management procedures include appropriate segregation of duties.

3.7 Third Party Processor Management: In selecting third party Processors who may gain access to, store, transmit or use customer data, Data Importer conducts a quality and security assessment pursuant to the provisions of its standard operating procedures.

3.8 Human Resources Security. The Data Importer informs its personnel about relevant security procedures and their respective roles, as well as of possible consequences of breaching the security rules and procedures. Such consequences include disciplinary and/or legal action.

3.9 Physical and Environmental Security.

a. *Physical Access to Facilities.* The Data Importer limits access to facilities where information systems that process customer data are located to identified authorized individuals who require such access for the performance of their job function. Data Importer terminates the physical access of individuals promptly following the date of the termination of their employment or services or their transfer to a role no longer requiring access to customer data.

b. *Physical Access to Components.* The Data Importer maintains records of the incoming and outgoing media containing customer data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of customer data they contain.

c. *Protection from Disruptions.* The Data Importer uses commercially reasonable systems and measures to protect against loss of data due to power supply failure or line interference.

d. *Component Disposal.* The Data Importer uses commercially reasonable processes to delete customer data when it is no longer needed.

3.10 Communications and Operations Management.

a. *Security Documents.* The Data Importer maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel.

b. *Data Recovery Procedures.*

i. On an ongoing basis, the Data Importer maintains multiple copies of customer data from which

it can be recovered.

ii. The Data Importer stores copies of customer data and a data recovery procedures in a different place from where the primary computer equipment processing the customer data is located.

iii. The Data Importer has procedures in place governing access to copies of customer data.

iv. The Data Importer has anti-malware controls to help avoid malicious software gaining unauthorized access to customer data.

c. *Encryption; Mobile Media.* The Data Importer uses HTTPS encryption on all data connections. The Data Importer restricts access to customer data in media leaving its facilities. The Data Importer further has a destruction policy for hardware in the data center that stores customer data.

d. *Event Logging.* The Data Importer logs the use of our data-processing systems. We maintain logs for at least 10 days.

3.11 Access Control.

a. *Records of Access Rights.* The Data Importer maintains a record of security privileges of individuals having access to customer data.

b. *Access Authorization.*

i. The Data Importer maintains and updates a record of personnel authorized to access systems that contain customer data.

ii. The Data Importer deactivates authentication credentials of employees or contract workers immediately upon the termination of their employment or services as well as such authentication credentials that have not been used for a period of time not to exceed six months.

iii. The Data Importer identifies those personnel who may grant, alter or cancel authorized access to data and resources.

c. *Least Privilege.*

i. Technical support personnel are only permitted to have access to customer data when needed for the performance of their job function.

ii. The Data Importer restricts access to customer data to only those individuals who require such access to perform their job function.

d. *Integrity and Confidentiality.*

i. The Data Importer instructs its personnel to disable administrative sessions when leaving the Data Importer's premises or when computers are unattended.

ii. The Data Importer stores passwords in a way that makes them unintelligible while they are in force.

e. *Authentication.*

i. The Data Importer uses commercially reasonable practices to identify and authenticate users who attempt to access information systems.

ii. Where authentication mechanisms are based on passwords, the Data Importer requires that the passwords are renewed regularly.

iii. Where authentication mechanisms are based on passwords, the Data Importer requires the password to be at least eight characters long.

iv. The Data Importer ensures that de-activated or expired identifiers are not granted to other individuals.

v. The Data Importer maintains commercially reasonable procedures to deactivate passwords that have been corrupted or inadvertently disclosed or pursuant to a number of failed login attempts.

vi. The Data Importer uses commercially reasonable password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

f. *Network Design.* The Data Importer has controls to avoid individuals assuming access rights they have not been assigned to gain access to customer data they are not authorized to access.

3.12 Network Security.

a. *Network Security Controls.* Data Importer's information systems have security controls designed to detect and mitigate attacks by using logs and alerting.

b. *Antivirus.* Data Importer implements endpoint protection on its hosting environments, including antivirus; which are continuously updated with critical patches or security releases in accordance with Data Importer's server change control procedures.

3.13 Information Security Incident Management.

a. *Record of Breaches.* The Data Importer maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

b. *Record of Disclosure.* The Data Importer tracks disclosures of customer data, including what data has been disclosed, to whom, and at what time.

3.14 Business Continuity Management. The Data Importer employs redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original state from before the time it was lost or destroyed.