Appendix D
Information Protection Contract Requirements

Participant shall comply, and cause Covered Parties to comply, with all of the provisions of the Information Protection Contract Requirements ("**IPCR**").

1) **Definitions**. For the purposes of this IPCR:

a) **"Agreement"** means [*insert master agreement name and contract number*] to which the IPCR is attached.

b) **"Amexco" or "AXP"** means the American Express entity or entities executing the Agreement and/or any Statement of Work thereunder.

c) "**Amexco Data**" means any Amexco confidential information as defined in the Agreement, including any adaptations, derivative works and translations, in any media or form, in whole or in part, and in addition, regardless of whether it constitutes confidential information as defined in the Agreement, any Personal Data, in each case, in any form, format or media whatsoever, including electronic and paper records, and including text, image, audio and video formats, that Participant receives access to in connection with the Agreement (other than Participant's Personal Data or any other data owned by the Participant as specifically set forth in the Agreement).

d) "**Applicable Law**", means all Applicable Laws, rules and regulations including all data protection, privacy, encryption and information security-related laws, rules and regulations and, where applicable, industry standards and other standards issued by self-regulatory organizations.

e) "**Including**", whether or not capitalized, means including without limitation.

f) **"Personal Data"** means any (i) individually identifiable information from or about an identified or identifiable individual in any form, format or media whatsoever, or any information that is combined with such individually identifiable information, including information that can be used to authenticate that individual or access an account, such as passwords or PINs, biometric data, recordings of individuals, unique identification numbers, answers to security questions, or (ii) information protected under Applicable Laws, such as, where applicable, "personal data" as defined by the European Data Protection Directive (95/46/EC).

g) "**Subcontractor**" means collectively and individually any third party authorized by Participant, including, any affiliate or subsidiary of the Participant, agent, representative, vendor, service provider, outsourcer, or the like, to which Participant discloses, or allows access to, Amexco Data in connection with this Agreement. Notwithstanding anything to the contrary herein, Subcontractors shall not disclose or allow access to any Amexco Data to any third party.

2) **Compliance**

Participant represents, warrants, and covenants that it (a) does and will comply with all Applicable Laws, and where applicable, industry standards (e.g. Payment Card Industry Data Security Standard (PCI DSS), ISO 22307 and ISO 27000)**;** and (b) has developed and implemented, and will maintain and monitor a written and comprehensive information security program in compliance with this IPCR and Applicable Laws**.** Upon request from time-to-time, Participant will certify its compliance with the foregoing.

3) **General**

a) All Amexco Data remains, at all times, the sole property of Amexco. Amexco reserves the right, where technically feasible and reasonable for the services provided as determined by Amexco, to require Participant to promptly change, update, delete, encrypt, truncate and/or mask any Amexco Data, in any manner, stored by Participant. Amexco Data or any portion thereof shall not be retained in any manner whatsoever, beyond the expiration or termination of the Agreement, except as required by Applicable Law and on prior notice to Amexco detailing the Applicable Law.

b) Prior to any storage media containing Amexco Data being assigned, allocated or reallocated to another user, or prior to such storage media being permanently removed from a facility, Participant will irreversibly delete such Amexco Data from both a physical and logical perspective, such that the media contains no residual data, or if necessary physically destroy such storage media such that it is impossible to recover any portion of data on the media that was destroyed. Participant shall maintain an auditable program implementing the disposal and destruction requirements set forth in this Section 3(b) for all storage media containing Amexco Data.

c) Unless otherwise instructed by Amexco, all Amexco Data must be (i) securely returned or (ii) properly and immediately disposed of in a secure manner that is reasonably designed to render the information permanently unreadable and not reconstructable into a usable format (i.e., in accordance with the then-current U.S. Department of Defense, or similar data destruction standard or CESG standards, as applicable). Any such return or disposal shall occur at such time that any such Amexco Data is no longer reasonably required to perform the services hereunder, but in any event, no later than upon completion of the relevant services. Upon request, Participant will certify that all such Amexco Data has been returned or disposed o in accordance with this IPCR.

d) Notwithstanding anything to the contrary herein, to the extent and for so long as Participant retains Amexco Data on any archival systems, back-up systems, data storage solutions, or any existing or future recordation medium whatsoever, Participant's obligations with respect to such Amexco Data shall survive in accordance with Section 11 below.

e) Participant shall establish and maintain administrative, technical, organizational and physical safeguards to protect the security, integrity, confidentiality and availability of Amexco Data, including to protect Amexco Data against any anticipated threats or hazards and to protect against any unauthorized or unlawful access to, use of, acquisition of or disclosure of Amexco Data, or any other compromise of Amexco Data.

f) Participant agrees to deploy applicable and necessary security patches to all systems that process, store or otherwise support the services described in the Agreement, including

operating system, open source, and application software, and the like, as quickly as reasonably possible.

g) Participant agrees to employ supported software (e.g., software under active maintenance, including operating system, open source, application software and/or the like) on any systems that process, store or otherwise support the services described in the Agreement.

h) Participant shall not access, acquire, use, process or disclose Amexco Data for any purpose other than the purpose stated in the Agreement.

i) Participant shall ensure each individual to whom Amexco Data is disclosed or made accessible will comply with and remain bound by Participant policies at least as protective of Amexco Data as those found in the Data Protection and Confidentiality Rules ("**DPCR**") attached hereto as **Exhibit A**. Each such individual shall be informed of and shall acknowledge their understanding of the security and data protection rules as stated in such Participant's policies by a tangible means and Participant, upon request, shall promptly provide to Amexco evidence of each individual's acknowledgement.

j) Amexco may provide Participant with test data that is approved for use in non-production environments. Participant agrees that no other Amexco Data will be used by or on behalf of Participant in non-production environments unless authorized by Amexco and then only if all data, as determined by Amexco, has been masked, aliased, truncated, scrambled, scrubbed, anonymized, obfuscated, deidentified or otherwise sanitized before replication to non-production systems, or the Amexco Data is in a secured and controlled environment with limited access and appropriate controls. Participant may not return this data to any production system.

k) Participant shall document the consequences for violations of Participant's data protection, information security, privacy and confidentiality-related policies.

4) **Indemnity**

a) Participant shall, at its own expense, defend, indemnify and hold harmless Amexco, its parent, and their respective employees, agents, subsidiaries, and affiliates, from and against any and all claims, suits, demands, actions, damages, losses, liabilities, proceedings, litigation, costs and expenses, including reasonable attorney's fees, relating to or arising out of this IPCR, including (i) the acts, omissions or obligations undertaken by Participant or Subcontractor pursuant to this IPCR, including any improper, unauthorized or unlawful access to, use or processing, acquisition of, or disclosure of Amexco Data, (ii) any misrepresentation or breach of warranty made by Participant herein, (iii) or any breach of this IPCR by Participant.

b) Amexco reserves the right to assume the exclusive defense and control of any matter otherwise subject to indemnification by Participant, and Participant shall fully cooperate with Amexco in asserting a defense. Participant shall pay Amexco's reasonable attorneys' fees and expenses incurred from any and all lawsuits or arbitrations brought against Participant by Amexco in connection with this IPCR.

5) **Security Records Retention**

Participant agrees to maintain and enforce retention policies for any and all reports, logs, audit trails and any other documentation that provides evidence of security, systems, and audit processes and procedures according to requirements mutually agreed upon by Amexco and Participant and in accordance with all Applicable Laws.

6) **Data Security Breach Notification**

In the event there is, or Participant reasonably believes that there is or was, any improper, unauthorized or unlawful access to, use of, acquisition of, or disclosure of Amexco Data or any other compromise of the security, confidentiality, privacy or integrity, of Amexco Data ("**Security Incident**"), Participant shall immediately notify Amexco by phone at for U.S.: 1-888-732-3750 or International: 1-602-537-3021 and in writing via email to: EIRP@aexp.com (send a secure email) of the Security Incident. Participant shall fully cooperate with Amexco to investigate and resolve any privacy, data protection, information security, integrity or confidentiality issues involving Amexco Data, including any Security Incident and/or notifications related thereto. Participant shall be responsible for all costs related to or arising from any Security Incident, including investigating the Security Incident and providing notification to all individuals affected by the Security Incident. Subject to Applicable Law, the Participant shall not make any public or other announcements or admissions of liability without the prior written consent of Amexco. Subject to Applicable Law, the provision of such notifications, if any, including the content, shall be solely at the discretion and direction of Amexco.

7) **Compliance Assessments and Inspections**

a) Participant shall document and, if requested by Amexco, promptly provide to Amexco, at a minimum, access to copies of all relevant Participant privacy, data protection, and information security and/or confidentiality-related policies, procedures and standards (including escalation procedures for non-compliance) for Amexco review.

b) Participant shall fully cooperate with Amexco in connection with any inspections, on-site or by phone, including inspections for privacy, data protection and information security compliance, and with self-assessment security compliance reviews. On-site inspections will be done by Amexco authorized representatives upon reasonable advance notice during regular business hours.

c) Upon Amexco's request, Participant shall promptly make available to Amexco copies of any third party data processing or information security, data protection and/or privacy-related assessment, test results, audit or review (e.g., SSAE 16, SOC I, II and III, SysTrust, WebTrust), or other equivalent evaluations in its possession or control.

d) If the services to be supplied by Participant will, at any time, include Participant hosting an Internet facing application and/or mobile application**,** Participant agrees to promptly perform and provide to Amexco a summary attestation from a vulnerability threat assessment ("**VTA**") test or such other testing, at minimum on an annual basis, demonstrating that the Internet facing application and/or mobile application has no material security vulnerabilities. The attestation report must include, at a minimum, a definition of how the vulnerabilities are rated (e.g., high / medium / low, serious / moderate / minimal) and evidence that the application has no open vulnerabilities at the highest rating and shows the number of vulnerabilities at any lower ratings. The VTA shall be performed by a vendor listed on the then current Amexco Chief Information Security Office (**"CISO"**) approved vendor list (which includes PCI Approved Scanning Vendors). Amexco reserves the right to review the detailed report from any such VTA at Amexco's sole discretion.

e) Participant agrees to allow Amexco to assess the manner in which Participant uses, stores, accesses, acquires or processes Amexco Data, subject to Participant's reasonable confidentiality and security precautions and procedures. Participant shall ensure that it has obtained sufficient permissions or consents that may be required under Applicable Law to ensure that Amexco is permitted to conduct such assessments. The purpose of such

assessments is to detect any improper, unlawful, or unauthorized access to, or use, acquisition, processing, or disclosure of Amexco Data. Amexco acknowledges and agrees that it will not be permitted to perform such an assessment if Participant can demonstrate that the assessment would: (i) cause Participant to be in breach of any Applicable Law, or Participant's internal data protection, information security, privacy and confidentiality-related policies or (ii) adversely impact or compromise any Amexco Data or third party customer data. In no event will the method of assessing such Participant's use, storage or processing of Amexco Data involve online access, or any other access, to Participant's systems, network, or infrastructure.

f) Participant shall remedy any issues identified under this Section 7 in a timely manner acceptable to Amexco.

8) **Security Administration**

a) Participant shall provide information security, data protection and privacy awareness training, utilizing either Amexco's or Participant's training course at Amexco's discretion, to all individuals authorized by Participant to have access to Amexco Data. The training shall be consistent with best practices in the financial services industry and designed, at a minimum, to educate all such individuals on maintaining the security, confidentiality, integrity and availability of Amexco Data, and shall occur before such individuals are allowed access to Amexco Data and no less than annually thereafter. Amexco reserves the right to review Participant's training and to require Participant to modify that training if Amexco deems this necessary.

b) Participant's assigned administrator(s) must retain sole responsibility for granting access to Amexco Data for all Participant employees and other users, and for providing a process by which employee and other user accounts shall be created and deleted in a secure and timely fashion. This process must include appropriate leadership approval, auditable history of all changes, and an annual review of access authorization and excess access remediation.

c) Participant shall establish, maintain and enforce the security access principles of "segregation of duties" and "least privilege" with respect to the Amexco Data hereunder. "Least Privilege" for this purpose of this Section 8(c) shall mean the minimum access required to perform a job function.

9) **Material Changes Affecting the Delivery of Services**

a) In the event Participant desires to materially modify the process, method or means by which Amexco Data is used, disclosed, accessed, acquired, stored, processed or otherwise transmitted or handled hereunder, or change the geographic location(s) where the Amexco Data is accessed, processed or stored, Participant shall provide Amexco at least ninety (90) days prior written notice. Amexco shall have the right, in its sole discretion, to determine if the modifications represent unacceptable risks to Amexco or Amexco Data and to prohibit Participant from implementing any such material modification to the service(s) supplied under the Agreement until such time as the risks can be mitigated to Amexco's reasonable satisfaction or an alternate source for the service(s) can be found. Examples of such material modifications include: (i) disclosing Amexco Data to a new Subcontractor, or (ii) rerouting Amexco Data flows.

b) As part of the provisioning of the service(s) contemplated under the Agreement, any material changes to the service(s), and/or any new service(s), Participant agrees to provide any requested information in connection with, and/or actively participate in, Amexco's security governance processes. If significant additional capital investment is required for Participant to comply with Amexco's security requirements or policies and standards, Participant and Amexco shall mutually agree upon the allocation of such expenses.

10) **Use of Sub-Vendors**

a) Participant shall take all necessary steps to cause Amexco to be deemed a third party beneficiary to all agreements between Participant and Subcontractors under Applicable Law, and shall provide copies of such agreements to Amexco upon request (redacted with respect to provisions unrelated to the IPCR obligations).

b) Participant (i) shall ensure each Subcontractor adheres to all of the terms hereunder; (ii) shall be liable for each Subcontractor's compliance hereto as if such Subcontractor were a party to this Agreement and any such non-compliance, action or omission were undertaken by the Participant under this Agreement; and, (iii) shall be responsible for all fees and costs related to each Subcontractor meeting all of Amexco's requirements hereunder, including any financial and/or security audits, inspections, and/or related security assessments during the term of the Agreement.

c) In the event that Participant has knowledge of a breach of the terms of the IPCR by a Subcontractor, Participant shall notify Amexco immediately. In the event Amexco determines that Subcontractor has violated the IPCR, Amexco reserves the right to require Participant to promptly cease and desist using the Subcontractor for any of the services described in the Agreement immediately and to require the Subcontractor to securely return or securely delete all Amexco Data from all of Subcontractor's systems immediately in accordance with Section 3(a) hereof. If requested by Amexco, Participant will confirm in writing to Amexco that all Amexco Data has been securely destroyed or permanently erased by the Subcontractor.

d) Amexco reserves the right to review Participant's due diligence processes performed on any Subcontractor and perform additional due diligence of its own on Subcontractor and/or Participant, including to ascertain whether the proposed changes contemplated to the service(s) meet Amexco security requirements. Participant shall implement in a timely manner at its own cost any commercially reasonable remedies required by Amexco hereunder.

11) **Survival Rights**

This IPCR and all provisions herein shall survive so long as Participant retains any Amexco Data. Notwithstanding the return or destruction of the Amexco Data, Sections 1, 2, 3(a), 4, 5, 6, 7, 10, and 11 shall survive indefinitely solely with respect to Participant's activities under the Agreement and the IPCR.

Exhibit A

Data Protection and Confidentiality Rules

The protection of confidential information and personal data is of utmost importance to American Express. Whenever you perform services or your other job duties that involve receipt of or access to confidential information, you must - at a minimum - comply with these Data Protection and Confidentiality Rules ("**DPCR"**).

In these rules, several words are capitalized; these words have particular meanings.

- Wherever we use the term "**Amexco**" or "**AXP**" we mean the entire American Express corporate family and third parties that have relationships with American Express; namely, American Express Travel Related Services Company, Inc., and its parent, subsidiaries, affiliates, as well as its and their consultants, contractors, joint ventures, licensees, franchisees, and Participants authorized to represent American Express' interests or to use or provide services related to your Job Duties.

- Wherever we use the capitalized term "**Job Duties**," we mean the services performed by and other job duties of the individuals covered by this DPCR.

- Wherever we use the capitalized term "**Personal Data**," we mean (i) individually identifiable information from or about an identified or identifiable individual in any form, format or media whatsoever, or any information that is combined with such individually identifiable information, including information that can be used to authenticate that individual or access an account, such as passwords or PINs, biometric data, recordings of individuals, unique identification numbers, answers to security questions, or (ii) information protected under Applicable Laws, such as, where applicable, "personal data" as defined by the European Data Protection Directive (95/46/EC).

- Finally, wherever we use the term "**Amexco Confidential Information**," we mean Amexco's and its customers' and clients' trade secrets, documents, data, information, systems, files, records, forms and any information used in the provision of Job Duties, including without limitation, Personal Data.

You SHALL:

1. Safeguard all Amexco Confidential Information;
2. Agree that any work product produced or developed in the performance of Job Duties for Amexco constitutes Amexco Confidential Information subject to this DPCR and the agreement between your employer and Amexco around ownership of intellectual property;
3. Always sign off of or lock with a password protected screensaver your workstation whenever you are not working on it, including, time away for breaks, lunch, meetings, etc.;
4. not disclose, share or allow the use by another person of your password, and if, nevertheless that happens resulting in errors or fraud, you shall be held accountable for such errors or fraud;
5. Understand that, except where prohibited by law, computer terminals are subject to monitoring and terminal monitoring may occur simultaneously with telephone monitoring;

6. Understand that all transactions in the system are recorded by the computer and that these recordings of any transactions by a personal identification number and password may be monitored at any time;
7. Help safeguard Customers' (and/or employees', as applicable) expectations of privacy by exercising diligence and care in the handling of Amexco Confidential Information relating to them; and
8. Understand that this DPCR and the rules contained herein are extremely important and any individual who willfully disregards these rules is subject to discipline.
9. Help to ensure that your colleagues and other individuals under your supervision comply with this DPCR.
10. Ensure systems are periodically evaluated to identify and address vulnerabilities.
11. Ensure necessary security patches are deployed to systems that process, store or otherwise support Amexco Confidential Information.
12. Ensure account passwords are strong and periodically changed for those accounts used to process, store or otherwise support Amexco Confidential information.

You <u>SHALL NOT</u>:

1. Use Amexco Confidential Information for your own benefit or the benefit of any third party, except to the extent necessary for the performance of your Job Duties;
2. Access Amexco Confidential Information unless required to as part of the performance of your Job Duties;
3. Access Amexco Confidential Information that does, or could contain any of the following types of information:
    - Your own account or related Amexco Confidential Information for any reason; or
    - An account or related Amexco Confidential Information if you personally know the account holder or customer in any way, whether from inside or outside of work.

    (Note: If you are ever required to access any of the above information as part of your Job Duties, you must promptly notify management <u>prior</u> to such access and provide any information necessary for management to determine if this is permissible);
4. Discuss Amexco Confidential Information in public places;
5. Reveal Amexco Confidential Information to any third party and/or to any individual except to the extent strictly necessary to perform your Job Duties;
6. Give your password to any person; or
7. Use another person's password or identification number.