SCHEDULE E

REQUIREMENTS FOR INFORMATION SECURITY PROGRAM

These requirements for information security program ("***Terms***") constitute an agreement between MoneyGram Payment Systems, Inc. ("***Customer***") and you ("***you***" or "***Supplier***") related to your provision of Goods and/or Services to Customer. All terms capitalized herein but undefined shall have the definitions assigned them in the master services agreement ("***MSA***") executed by and between Customer and the Supplier.

INFORMATION SECURITY

1. **Protection**. The following describes specific elements of the security program that Supplier must have in place for purposes of: (i) ensuring the security and confidentiality of Confidential Information, (ii) protecting against any anticipated threats or hazards to the security of such information, and (iii) protecting against the unauthorized access or use of such information in ways that could result in substantial harm or inconvenience to Customer, its customers, or its Representatives (the "***Program***"). At a minimum, the Program shall comply with the current security obligations imposed by the Gramm-Leach-Bliley Act (GLBA), the California Consumer Privacy Act (CCPA), and the General Data Protection Regulation (GDPR).

   1.1. **Designation of Representatives**. Supplier shall designate one or two Representatives that shall be responsible for coordinating and overseeing the Program from a security standpoint (the "***Program Officer(s)***"). The Program Officer(s) may designate other Representatives to oversee and coordinate particular elements of the Program.

   1.2. **Scope of Program**. The Program shall apply to Confidential Information, whether in paper, electronic or other form, that is handled or maintained by or on behalf of Customer or its Affiliates.

   1.3. **Elements of the Program**.

      1.3.1. **Risk Identification and Assessment**. Supplier shall identify and assess external and internal risks to the security, confidentiality, and integrity of Confidential Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the Program, the Program Officer will establish procedures for identifying and assessing such risks in each relevant area of Supplier's operations, including:

         1.3.1.1. **Information Systems and Information Processing, Administration, and Disposal**. The Program Officer shall inventory physical devices and software and shall evaluate potential risks to information associated with Supplier's Systems, including network and Software design, information processing and administration, and the storage, transmission and disposal of information. This evaluation will include an assessment of Supplier's current policies, procedures, and practices relating to the security of the information. The Program Officer will also develop and assess procedures for monitoring potential information security threats associated with Supplier's Systems and applications and for ensuring that such Supplier Systems and applications are updated by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

1.3.1.2. **Detecting, Preventing, and Responding to Attacks**. The Program Officer will: oversee Supplier's efforts to detect, prevent, and respond to attacks; develop procedures for coordinating responses to attacks; and develop incident response teams and related internal policies. The Program Officer may delegate to a qualified representative of the information security or information technology groups the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by Supplier.

1.3.1.3. **Access and Use.** The Program Officer will coordinate with appropriate Supplier staff to evaluate the effectiveness of Supplier's internal policies, procedures and practices relating to access to and use of Confidential Information.

1.3.1.4. **Employee Training.** Supplier shall use Customer's security training as a part of the new hire training to ensure that all affected employees are made aware of the security and fraud concerns which may place Customer's information at risk. Training shall include instruction on the policies and procedures designed to limit that risk.

1.3.1.5. **Monitoring and Controls.** Supplier shall implement detailed requirements to monitor compliance with the Program in order to timely identify potential weaknesses and improvements. In addition, the Program shall include appropriate controls to ensure that identified weaknesses are addressed and necessary adjustments are made to the Program. Controls include, for example: managing access credentials and identities; monitoring physical and remote access; creating awareness and training; backups; monitoring data at rest and in motion; and data destruction policies.

1.3.1.6. **Designing and Implementing Safeguards.** The risk assessment and analysis described above shall apply to all methods of handling or disposing of Confidential Information, whether in electronic, paper or other form. The Program Officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards.

1.3.1.7. **Overseeing Supplier.** The Program Officer shall examine and evaluate the information security internal policies, practices and capabilities of Supplier's existing and potential third-party vendors and service providers. This responsibility will include raising awareness of, and Supplier's methods for, selecting and retaining only those vendors that are capable of maintaining appropriate safeguards for nonpublic or Confidential Information to which they will have access. The Program Officer will develop and incorporate standard, contractual protections applicable to vendors, which will require such providers to implement and maintain appropriate safeguards. Such standards shall be provided to Customer during the implementation planning phase for review and approval. These standards shall apply to all existing and future contracts between the Supplier and its vendors.

1.3.1.8. **Adjustments to Program.** The Program Officer is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the vendor's operations, applicable laws and regulations, and any other circumstances that may have a material impact on the Program. Any changes shall be provided to Customer for review and approval prior to implementing such changes.

1.3.1.9. **Specific Internal Policies.** Supplier shall develop specific internal policies that address Supplier's Systems and applications that support Customer. Such policies shall be provided to Customer for review and approval during the implementation planning phase.

1.3.1.10. Providing a Software system that controls and reports on all access attempts and attempted violations of the security policies and pre-approval of non-essential Representatives' access to sensitive areas (including data centers, telephone switch rooms, communications rooms, tape libraries and calling floors).

1.3.2. Supplier shall install and use a reasonable change control process to ensure that access to the Supplier Systems associated with the Customer Program and access to Program Information associated with the Customer Program is controlled and recorded. Supplier shall notify Customer of any planned system configuration changes or other changes affecting the security plan applicable to Program Information, setting forth how such change will impact the security and protection of Program Information. No such change affecting the security plan applicable to Program Information may be implemented without the prior written consent of a Customer security representative.

1.3.3. The Program shall prevent the unintended or malicious loss, destruction or alteration of Customer's files, Program Information, software and other property received and held by Supplier. Supplier shall maintain back-up files (including off-site back-up copies) thereof and of resultant output to facilitate their reconstruction in the case of such loss, destruction or alteration, in order to insure uninterrupted Services in accordance with the terms of this MSA, its Schedules, Customer's written policies and Supplier's disaster recovery plans.

2. **Detection**.

2.1. Supplier shall monitor the Supplier System and its procedures for security breaches, violations and suspicious or questionable activity. This includes suspicious external activity (including, without limitation, unauthorized probes, scans or break-in attempts) and suspicious internal activity (including, without limitation, unauthorized system administrator access, unauthorized changes to the Supplier System or network, Supplier System or network misuse or Program Information theft or mishandling). Supplier shall notify Customer promptly (but no later than 24 hours thereafter) of any security breaches or suspicious activities, including without limitation unauthorized access attempts and service attacks, such as denial of service attacks.

2.2. Supplier shall maintain for a mutually agreed-upon length of time and afford Customer all system records and logs solely related to the Customer Program. Customer may review and inspect any record of system activity or Program Information handling related to Customer without prior notice. Supplier acknowledges and agrees that records of system activity and of Program Information handling may be evidence (subject to appropriate chain of custody procedures) in the event of a security breach or other inappropriate activity. Upon Customer's request, Supplier shall deliver the original copies of such records to Customer for use in any legal, investigatory or regulatory proceeding.

3. **Response**.

3.1. Supplier shall monitor industry-standard information channels, including bugtraq, CERT, and OEMs, for newly identified system vulnerabilities regarding the technologies and services provided to Customer and fix or patch any identified security problem in an adequate and timely

manner. Unless otherwise expressly agreed in writing, "***timely***" shall mean that Supplier shall introduce such fix or patch as soon as commercially reasonable after Supplier becomes aware of the security problem. This obligation extends to all devices that comprise Supplier's system, including application software, databases, servers, firewalls, routers and switches, and hubs, and to all of Supplier's other Program Information handling practices.

3.2. **Information Supplier Shall Provide.** Upon Customer's request, Supplier shall meet with the Customer Information Security team to discuss information security issues in much greater detail at times reasonably requested by Customer and at mutually agreeable locations. Supplier shall discuss in detail and provide detailed information regarding the topics listed below, which shall be addressed in Supplier's information security plan for Customer. Customer acknowledges and agrees that the information Supplier so provides is Supplier's Confidential Information.

3.3. **Other Security Plan Features.** Supplier shall also implement and maintain in conformance with its security plan, the following requirements set forth by Customer below, and as amended from time to time:

3.3.1. Supplier shall use surveillance cameras to monitor the entry points to the data center and Contact Center floor(s). Security cameras shall be monitored and recorded 24 hours per day, seven days per week. Supplier shall obtain applicable consents to record and all cameras shall record and such records shall be stored for a minimum of 3 months.

3.3.2. Supplier shall use card readers at each entry door. Card reader access records shall be kept for the Term and for 12 months thereafter.

3.3.3. Supplier security controls and procedures shall govern all Supplier Representatives. Upon termination, Representatives must return all Supplier property, including keys, badges and key cards. Supplier must inform all operations security personnel concerning termination of employment. Operations security personnel must then remove or rescind security rights for the individual.

3.3.4. Supplier shall (i) monitor all mainframe and LAN systems for unusual occurrences; (ii) aggressively investigate any suspected intrusion; and (iii) terminate any individual suspected of a security violation.

3.3.5. Supplier shall cooperate with Customer to assign Representative identification numbers ("***Representative ID***") and passwords to all Representatives during the hiring process for timecard processing. Supplier shall cooperate with Customer to ensure that each Representative is set up to only have access to the information or data that has been authorized for the specific use. The Representative identification number and password are used to control general Supplier security functions. Individual security logons and multi-factor authentication are required for specific project programs. Any changes in security levels must be submitted in writing and approved by the data owner before changes can be made.

3.3.6. Customer's Confidential Information shall be either (i) stored in an encrypted format in all locations where such Confidential Information may reside; or (ii) stored in a secured location such that access to both the location and to the Confidential Information is restricted to only those individuals that have a business need. For purposes of transmitting Confidential Information, such transmission shall either be (A) sent over a secure network; or (B) encrypted using a product that has been pre-approved by Customer in writing.

3.3.7. Supplier shall retain computer audit trails for six months for the following occurrences as it relates to Customer Data:

3.3.7.1. Authentication failures, including date and time of access, and user identification information;

3.3.7.2. Security administration activities;

3.3.7.3. Administrator and/or privileged users;

3.3.7.4. Representative user last logon date;

3.3.7.5. Access that occurs as a result of a powerful and/or elevated privilege (e.g., Administrator), whenever possible, rather than specific authorization shall be logged;

3.3.7.6. Changes to user accounts, profiles, and system configuration; and

3.3.7.7. Security violations.

3.3.8. If applicable, Supplier shall obtain PCI certification within 90 days of the Effective Date and shall at all times during the Term and any Termination Assistance Period comply with PCI requirements.

3.3.9. To maintain confidentiality:

3.3.9.1. The appropriate data security procedures shall be in place to maintain the integrity of both hard copy as well as electronic data.

3.3.9.2. Each Representative shall be required to sign and comply with a confidentiality agreement with terms at least as restrictive as the terms of Section 10 of the MSA.

PREVENTION STRATEGIES AND PHYSICAL SECURITY.

4. Ongoing security controls and procedures shall govern all Supplier Representatives working on the Customer Program. Each Representative shall be required to sign and comply with a confidentiality agreement. Supplier shall provide security on a continuous basis for all facilities that house the Customer Program by employing personnel to monitor the surveillance cameras and monitor building access. All Representatives shall be required to wear identification badges. Card-reader control units and/or security guards strictly control access from outside entrances into high security areas.

5. A software system shall control and report on all access attempts and all attempted violations of the security policy. Authorization to enter secure and sensitive areas must be pre-approved and entered into the security system. The secure areas that have limited access shall include:

5.1. Computer Rooms / Data Centers

5.2. Telephone Switch Rooms

5.3. Communications Rooms

5.4. Tape Libraries

DATA BACK-UP AND OFF-SITE STORAGE OF VOICE RECORDINGS AND ACD DATA.

6. Supplier shall implement a procedure of data file backup and off-site storage for its processing systems. Electronic communications, files, voice recordings and ACD data shall be backed-up at regular intervals appropriate for recovery capabilities. Critical files on each system shall be backed-up and rotated off-site. In the event of the destruction of a facility or processing system, those files can restore the data as it existed on the original system.

7. Three generations of files shall be retained as a standard practice and additional generations or files for archive or history purposes shall be retained as required for the application. Supplier shall use professional storage services providing industry standard secure off-site data storage.