SECURITY OVERVIEW

1. Introduction. This Security Overview establishes the basic security requirements used by ParTech in securing the PAR POS Services, the PAR OPS Services, the PAR Ordering Services, the PAR Pay Services and the PAR Punchh Services for information security, as needed to ensure the confidentiality, availability, and integrity of Customer Data and Customer Personal Information.

2. Terminology. Capitalized terms used herein but not defined herein shall have the meaning ascribed to them in the Subscription Services Terms ("Terms") or the Data Processing Addendum (as applicable).

3. Specific Security Requirements.

   3.1 Security Policy. ParTech maintains a comprehensive set of written security policies and procedures which cover, at a minimum:
   - (i) ParTech's commitment to information security;
   - (ii) information classification, labeling, and handling, and such policies and procedures related to information handling must describe the permissible methods for information transmission, storage, and destruction and such methods must be no less protective than what is commercially reasonable and comport with applicable industry standards;
   - (iii) acceptable use of ParTech's assets, including computing systems, networks, and messaging;
   - (iv) information security incident management, including data breach notification and collection of evidence procedures;
   - (v) access controls, including periodic reviews of access rights;
   - (vi) logging and monitoring of ParTech's production environment, including logging and monitoring of physical and logical access to ParTech's networks and systems that transmit, access, Process and store Customer Data and Customer Personal Information;
   - (vii) disciplinary measures for personnel who fail to comply with such policies and procedures; and
   - (viii) the topics described in the remainder of this Section 3 in a manner consistent with the applicable requirements for such topics as set forth in this Section 3.

   3.2 Responsibility for ParTech's Information Security Program. ParTech has individuals within its Information Technology Department and individuals within its Development & Operations Security Department, with experience and training in cyber security and risk management. These departments are responsible for ParTech's information security program.

   3.3 Audits of ParTech's Information Security Program. ParTech shall cause an independent third party to conduct at least once each year a SOC 1 Type II audit and a SOC 2 Type II Audit of the ParTech Services for ParTech's Services. ParTech will provide a copy of these reports to Customer upon Customer's request, and such reports shall be considered Confidential Information of ParTech subject to Customer's confidentiality obligations under the Agreement.

   3.4 Monitoring. In addition, and without limiting any of its obligations hereunder, ParTech shall regularly monitor and review ParTech's information security program to ensure safeguards are appropriate to limit risks to Customer Data and Customer Personal Information.

   3.5 Asset and Information Management. ParTech shall:
   - (i) maintain an inventory of all Customer Data, including Customer Personal Information (if any) that ParTech Processes; and
   - (ii) maintain an inventory of physical computing and software assets ParTech uses in the performance of its activities under the Terms.

3.6 Employee-Related Matters. ParTech shall:

(i) train its new personnel (including contingent workers provided by staffing agencies) on the acceptable use and handling of ParTech's confidential information and confidential information of other companies that has been entrusted to ParTech (such as Customer Data and Customer Personal Information);

(ii) provide annual security education refreshers for its personnel (including contingent workers provided by staffing agencies) and maintain a record of personnel that completed such education; and

(iii) implement a formal user registration and de-registration procedure for granting and revoking access to ParTech's information systems and services; and upon termination of any personnel (including contingent workers provided by staffing agencies), ParTech shall revoke such individual's access to Customer Data, including Customer Personal Information, as soon as possible but in no event later than three (3) business days following termination of such individual.

3.7 Communications and Operations. ParTech shall:

(i) perform regular backups sufficient to restore services to Customer within a commercially reasonable period of time;

(ii) encrypt all backup media containing Customer Data;

(iii) on all servers and networks maintain up to date malware detection and prevention on ParTech's servers and/or end user platforms, including virtual machine implementations, that transmit, access, Process and store Customer Data;

(iv) maintain a hardened Internet perimeter and secure infrastructure using firewalls, antivirus, anti-malware, intrusion prevention/detection systems, and other protection technologies as is commercially reasonable;

(v) implement regular patch management and system maintenance for all ParTech's systems including virtual machine implementations, that Process Customer Data; and

(vi) upon Customer's written request, provide details on how Customer's Data is segregated and protected from ParTech's other client data, if deployed in a multi-tenant or multi- customer environment.

3.8 Access Control. ParTech shall:

(i) enforce commercially reasonable practices for user authentication; if passwords are used to authenticate individuals or automated processes accessing Customer Data, such passwords will comply with the current commercially reasonable practices for password usage, creation, storage, and protection;

(ii) ensure that user IDs are unique to individuals and are not shared;

(iii) assign access rights based upon the sensitivity of Customer Data, the individual's job requirements, and the individual's "need to know" for the specific Customer Data;

(iv) review the access rights of ParTech's personnel (including Subprocessors) to ensure need-to-know restrictions are kept current; and

(v) restrict access to Customer Data by segregating administrator-level access from user-level access.

3.9 Application Development; Vulnerability Scans and Penetration Tests. ParTech shall:

(i) implement a secure development methodology that incorporates security throughout the development lifecycle;

(ii) develop and enforce secure coding standards;

(iii) perform secure code reviews using automated scanning tools for all externally facing applications and for any software developed by ParTech and a ParTech Affiliate and delivered to Customer of the PAR POS Services and the PAR Pay Services;

(iv) perform vulnerability scans at least once each year, either by ParTech or through a 3rd party, for

all internal and externally facing applications that receive, access, process, or Store Customer Data; and

(v) perform penetration tests at least once each year for all externally facing applications that receive, access, process, or Store Customer Data and Customer Personal Information ("Penetration Test") of the PAR POS Services and the PAR Pay Services.

3.10 Subprocessors. ParTech shall:

(i) take reasonable steps to select and maintain Subprocessors that can maintain security measures to protect Customer Data in accordance with applicable laws and regulations and in a manner no less protective than the requirements set forth in the Agreement, including this Schedule, and maintain with each such Subprocessor a written contract requiring such Subprocessor, by contract, to implement and maintain such security measures;

(ii) other than as permitted in the Agreement, not provide to any Subprocessor, or allow any Subprocessor to Process, view or otherwise interact with, any Customer Data without obtaining the prior consent of Customer in accordance with the Data Processing Addendum;

(iii) not use, in connection with the Agreement, any software or service provided by a third party where such software or service (a) is deployed by such third party acting as an application service provider (or similar), (b) is a "software as a service" offering (or similar), or (c) involves the use of "cloud computing" or "cloud services" (or similar) without obtaining the prior consent of Customer in accordance with the Data Processing Addendum; and

(iv) upon written request by Customer, use commercially reasonable efforts to obtain from each Subprocessor (or if Customer's consent is limited to specific Subprocessors, each of those specific Subprocessors) the right for Customer to receive a copy of, or otherwise have the ability to review, the report(s) resulting from each audit or review of such Subprocessors' information security policies, practices and controls that was conducted by an independent third party (e.g., SSAE 16 SOC 1 Type II audit, ISO 27001 certification or similar) within the then most recent three (3) years and that is relevant to the security policies, practices and controls employed by such Subprocessor to protect Customer Data.

4. Information Security Incident Management. ParTech shall establish, test, and maintain an information security incident response process that includes, among other things, processes for evidence preservation, informing and working with law enforcement agencies, government agencies and similar parties as appropriate, and performing forensic analyses.

5. Business Continuity Management. ParTech shall:

5.1 establish and maintain a comprehensive business continuity plan ("BCP") that covers the restoration of both technology and business operations in the event of an unplanned event; the planning process for the BCP will include risk analysis, business impact analysis, recovery strategies for different scenarios to include geographic/regional events, pandemics, and natural disasters (e.g., tornado, hurricane, flooding, fire, power outage), and the BCP shall cover, among other things, ParTech's operations associated with its activities under the Agreement; and

5.2 test its BCP at least annually and provide Customer, at Customer's written request, with an annual attestation that ParTech successfully conducted a test of its BCP (such attestation shall include the scope, location(s), and date(s) of the test(s)).

6. Compliance. ParTech shall:

6.1 maintain a code of ethics and require employees to review and acknowledge it annually (except if and to the extent prohibited by law); and

6.2 if interacting directly with individuals, develop, implement and operate in accordance with a privacy policy (which among other things, describes the types of information collected, how the information is used, stored and shared, any options for an individual to "opt out" of any usage or sharing, and how an individual may access his or her information) and disseminate or otherwise make such privacy policy available to such individuals.