Information Security & Controls Addendum

This Information Security & Controls Addendum between TicketSocket, Inc.**,** a Delaware corporation ("**TicketSocket**") and the User identified in the User Agreement to which this is an addendum ("**User**"), sets forth the terms and conditions relating to the security controls that TicketSocket has adopted when Processing User Data in association with the Services to be rendered by TicketSocket to User pursuant to the User Agreement (the "**Agreement**"). Information regarding security controls used by TicketSocket's Subprocessors are referred to in section V below.

I. Definitions

"User Data" means, any and all data and information including, but not limited to, User confidential information, Personal Data, (as defined in the Agreement), financial data, and account data which is (i) disclosed at any time to TicketSocket or its personnel by User in anticipation of, in connection with or incidental to the performance of TicketSocket's services for or on behalf of User; (ii) Processed (as defined below) at any time by TicketSocket or its Personnel in connection with or incidental to the performance of TicketSocket's services for or on behalf of User; or (iii) derived by TicketSocket or its Personnel from the information described in (i) and (ii) above.

"User Systems" means any User's information systems, applications, databases, infrastructure (including without limitation, software and hardware), platforms, and networks.

"TicketSocket Systems" mean TicketSocket's information systems, applications, tools, software, hardware, databases, infrastructure, platforms, and networks used with respect to Processing User Data in any manner.

"Highly Privileged Account" or "HPA" means accounts with system level administrative or super-user access to information systems, applications or databases, administration of accounts and passwords on a system, or ability to override system or application controls.

"Personnel" means the individual employees, agents, consultants or contractors of TicketSocket or User (as applicable).

"Public Cloud" means multi-tenant environment, where a service provider makes resources, such as applications, storage and computing infrastructure, available to the general public over the Internet.

"Process" or "Processed" or "Processing" means any operation or set of operations performed upon User Data, whether or not by automatic means, such as creating, collecting, procuring, obtaining, accessing, analyzing, recording, organizing, processing, adapting, storing, maintaining, altering, retrieving, transmitting, consulting, using, disclosing or destroying such data.

"Subprocessor" means any third party service provider appointed by TicketSocket (in accordance with
the terms of the Agreement) to Process User Data.

II. Information Security Risk Management Requirements

A. TicketSocket shall maintain official written policies and procedures for the administration of information security throughout its organization to ensure the security, availability, integrity and confidentiality of TicketSocket Systems, User Systems and User Data.

B. TicketSocket shall have an IT security function with clearly defined information protection roles, responsibilities and accountability.

C. TicketSocket Personnel with access to User Data and/or User Systems shall participate in the information security awareness training provided by TicketSocket on a periodic basis (no less frequently than annually).

III. Core Information Security Requirements

A. Information Systems Audit

1. TicketSocket shall perform internal vulnerability assessments on TicketSocket Systems used to provide the services to User. Furthermore, TicketSocket shall perform an external vulnerability assessment on all external internet facing TicketSocket Systems that impact User Data. Such assessments will be conducted not less frequently than semi-annually.
2. TicketSocket shall use its best efforts to remediate any finding rated as high or critical (or similar rating representing similar risk) in any assessments or audits of TicketSocket Information Systems within 30 days. Additionally, TicketSocket shall use its best efforts to remediate any finding rated as medium within 90 days. If such findings are not able to be or are not remediated within the time period provided, TicketSocket must notify User immediately with a proposed action plan to remediate.
3. Upon reasonable request (not less than ten (10) business days), TicketSocket shall provide formal reports for any assessments or audits performed on User-related TicketSocket's Information Systems, which shall include at a minimum the scope of the assessment or audit and any finding rated as a medium and above.

B. Operations Security

1. TicketSocket shall implement and maintain security controls to detect and prevent unauthorized access, intrusions, computer viruses and malwares on its Information Systems to protect User Data including:
    a. Ensuring that security client software which includes anti-virus and malware protection is set to receive automatic virus definitions as well as managed patches and updates.
    b. Installing of critical security patches for operating systems and applications within 30 days of publication, and within 90 days for other types of patches and updates;
    c. Installed versions of operating systems, software and firmware for all systems are licensed and TicketSocket supported.
2. TicketSocket shall implement and maintain a security event logging system to log all authorized and unauthorized access attempts to associated systems, data or application services. Security event logs shall be maintained for at least one year.

C. Access Control

1. TicketSocket shall limit access to TicketSocket Systems, User Systems and/or User Data to a limited number of authorized Personnel and Subprocessors so that they may perform their respective duties in support of the obligations set forth in the applicable Agreement with TicketSocket.

2. TicketSocket shall assign a unique ID to all authorized Personnel prior to granting access to TicketSocket Systems and User Data.
3. TicketSocket shall implement processes to support the secure creation, modification and deletion of accounts and High Privilege Accounts.
4. TicketSocket shall terminate any separating TicketSocket Personnel's access no later than the date of separation, whether physical or logical, that may provide access to User Data and/or User Systems.
5. TicketSocket shall ensure a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies (such as token devices), including the following password requirements at minimum:
    a. Temporary passwords must be provided to TicketSocket Personnel in a secure method, with expiration on first use.
    b. User account credentials (e.g. password) must not be shared or stored in clear text.
    c. Complex password best practices must be enforced that include minimum password length, lockout, and set expiration period.
    d. Default or accounts with empty or null passwords are prohibited.
    e. Information systems (including User Systems and TicketSocket Systems) must not be left authenticated when unattended and must be password protected when not in use.

D. Network & Data Transmission Security

1. TicketSocket shall implement firewall protection, intrusion detection system (IDS) and standards designed in a risk based manner to maintain the integrity of User Data at all times, and that restrict connections between untrusted networks and any system components in the environment.
2. TicketSocket shall implement encryption with respect to all records and files containing User Data transmitted across public networks or wirelessly.

E. System & Storage Security

1. TicketSocket shall implement and maintain physical and technical controls designed to:
    a. Guard against unauthorized access to disruption, altering, or removal of TicketSocket Systems, User Systems, and User Data.
    b. Ensure that no User Data is physically or virtually co-mingled with any of TicketSocket's (or any third party's) other data, unless the data is logically separated.
2. TicketSocket shall ensure that all User Data will be Processed and maintained solely on designated target systems and that no User Data at any time will be Processed on or transferred to any portable computing device or any removable media (e.g. thumb drives or external hard drives) other than physically secured retention media solely used for the purpose of backup or data retention for business continuity planning/disaster recovery purposes, which shall be encrypted to industry standards.
3. TicketSocket shall ensure that TicketSocket Personnel must not store any User Data on personally-owned devices (e.g. tablets and mobile devices).
4. TicketSocket shall identify and implement risk based data loss prevention controls to protect User Data as required by regulatory compliance obligations.

F. Application Security

1. TicketSocket shall have a documented software development lifecycle process which includes requirements gathering, system design, integration testing, user acceptance testing, and system acceptance.
2. TicketSocket shall provide all developers secure software development training and information regarding vulnerabilities discovered along with prevention and remediation measures for those vulnerabilities.
3. TicketSocket shall design and develop all applications in accordance with the following core security principles:
    a. Least Privilege – Recommends that accounts have the least amount of privilege required to perform their business processes.
    b. Minimize Attack Surface – Recommends reducing entry points that can be exploited by malicious users.
    c. Separation of Duties – Recommends that different entities have different roles.
    d. Fail Secure – Recommends limiting amount of information exposed on errors encountered by a system or application.
    e. Defense in Depth –Recommends layered security mechanisms that will increase security of the system as a whole.
    f. Complete Mediation – Recommends access to all resources of a system is always validated.
    g. Single Point of Failure – Recommends adding redundancy to critical systems.
4. TicketSocket shall develop all web applications based on secure coding practices such as the Open Web Application Security Project (OWASP) or NIST SP 800-95 guidelines for web services.
5. TicketSocket shall use industry best practice quality control methods to ensure that software developed by TicketSocket or its contractors does not introduce security vulnerabilities to User's computing or application environment. This includes identifying risks through threat and vulnerability analyses, including scanning for the Open Web Application Security Project (OWASP) Top 10 most critical web application security risks and remediating risks prior to delivery of systems or applications.

G. Physical Security

1. TicketSocket facilities used to store or access User Data shall have physically secure perimeters, and all entry points shall be properly protected against unauthorized access.
2. Access to TicketSocket locations where User Data is stored shall be restricted to TicketSocket Personnel and authorized visitors.
3. TicketSocket Personnel and authorized visitors shall be issued identification cards. Identification cards shall be visibly displayed at all times while on TicketSocket premises.
4. Visitors shall be required to sign a visitors register (maintained for at least one year) and be escorted or observed at all times.

H. Public Cloud

Except for Amazon Web Services ("AWS"), TicketSocket shall not utilize "public cloud" computing services as part of any hosted solution or service or otherwise connect User Systems to, or allow User Data to be collected, transmitted , hosted, stored or otherwise Processed on a "public cloud" service without first obtaining written approval from the User. User acknowledges and agrees that AWS may be used by TicketSocket to provide the Services.

I. Right to Audit

Not more than once in each calendar year, User shall have the right to monitor TicketSocket's compliance with the terms of this Addendum. User or its authorized representatives shall have the right, by providing reasonable advance written notice, to inspect, review and audit TicketSocket's security controls, information and/or materials in TicketSocket's possession, custody or control, relating in any way to TicketSocket's obligations under this Addendum. An inspection performed pursuant to this Addendum shall not unreasonably interfere with the normal conduct of TicketSocket's business, but shall include within its scope an evaluation of TicketSocket's Personnel (including, without limitation TicketSocket's agents, consultants and contractors) providing services under the Agreement. User specifically acknowledges that in respect of Subprocessors, TicketSocket would not be able to provide any wider audit rights than those granted to it by such Subprocessors. TicketSocket shall cooperate fully with any such inspection initiated by or on behalf of User.

IV. Compliance Requirements

A. Payment Card Industry (PCI) Data Security Standard (DSS)

1. TicketSocket shall acknowledge responsibility to protect payment card holder data and shall ensure compliance to PCI DSS.
2. TicketSocket shall provide User with a valid PCI Report on Compliance (or an Attestation of Compliance along with the Executive Summary section of the Report on Compliance) annually.
3. If TicketSocket is unable to provide a PCI Report on Compliance or Attestation of Compliance, TicketSocket agrees to take part, as an auditable entity, in User's annual PCI DSS audit.
4. TicketSocket shall remediate deficiencies identified during the PCI DSS audit in a reasonable time acceptable to all parties (i.e. TicketSocket, User and User's banks.)

V. Subprocessor Compliance

TicketSocket's Subprocessors and security details are set out below.

A. Amazon Web Services

1. AWS uses EBS storage encryption on all applications and databases via AWS. Amazon EBS encryption uses AWS KMS keys when creating encrypted volumes and snapshots. Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data at- rest and data-in-transit between an instance and its attached EBS storage.
2. AWS WAF is enabled for application level firewall protection, and helps protect web applications or APIs against common web exploits and bots.
3. TicketSocket takes advantage of AWS' ability to, isolate specific IPs on specified ports to connect directly to the servers. This helps to control traffic to TicketSocket Systems, including the kind of traffic that can reach TicketSocket Systems.

B. Conformance Cybersecurity

1. Conformance Cybersecurity have been appointed to conduct penetration testing. It provides PCI Security Standards Council (PCI SSC) Qualified Security Assessor (QSA) services.