Security, Privacy and Architecture of Virtual Incentives Reward Platform

Published: 6.14.2019

Virtual Incentives Corporate Trust Commitment

Virtual Incentives is committed to achieving and maintaining the trust of our clients. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including data submitted by clients and card recipients (collectively "Customer Data").

Services Covered

Vi Now is our state-of-the-art reward platform through which our clients submit information required for reward fulfillment ("Reward Platform") This document describes the architecture of, the security, privacy-related audits and certifications received for, and the administrative, technical and physical controls applicable to the Reward Platform.

Some of the elements described in this documentation, such as log retention, back-ups, disaster recovery and return and deletion of data, do not apply to the temporary developer testing environments branded as "Sandbox".

Architecture and Data Segregation

The Reward Platform is operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific identifiers and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

Control of Processing

Virtual Incentives has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer throughout the entire chain of processing activities by Virtual Incentives and its sub- processors. In particular, Virtual Incentives has entered into written agreements with its sub- processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organizational data security measures implemented by Virtual Incentives and its sub-processors are subject to regular audits.

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to the Reward Platform.

- **EU-U.S. Privacy Shield Certification**: Customer Data submitted to the Reward Platform is within the scope of an annual certification to the EU-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce, as further described in our Privacy Shield Notice. The current certification is available at https://www.privacyshield.gov/list by searching under "Virtual Incentives."

- **Payment Card Industry (PCI)**: For the Reward Platform, Virtual Incentives has obtained a signed Attestation of Compliance ("AoC") demonstrating Level 1 compliance with the applicable Payment Card Industry Data Security Standard ("PCI DSS"), as formulated by The PCI DSS Council as a data storage entity or third party agent from a Qualified Security Assessor that is certified as such by PCI DSS. A copy of Virtual Incentives AoC is available upon request from your organization's Virtual Incentives Client Success Manager.

Additionally, the Reward Platform undergos security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.

Security Controls

The Reward Platform includes a variety of configurable security controls that allow customers to tailor the security of the Reward Platform for their own use.

Security Policies and Procedures

The Reward Platform is operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored using a one-way salted hash.
- User access log entries will be maintained, containing date, time, user ID, entity ID operated on, operation performed (created, updated, deleted).
- If there is suspicion of inappropriate access, Virtual Incentives can provide customers log entry records and/or analysis of such records to assist in forensic analysis when available. This service will be provided to customers on a time and materials basis.
- Data center physical access logs, system infrastructure logs, and application logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- Passwords are not logged.
- Certain administrative changes to the Reward Platform (such as password changes and adding
- Virtual Incentives personnel will not set a defined password for a user. Passwords links are randomly generated and delivered automatically via email to the requesting user (which must be changed on first use).

Intrusion Detection

Virtual Incentives, or an authorized third party, will monitor the Reward Platform for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Virtual Incentives may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentication, and to ensure that the Reward Platform functions properly.

Security Logs

All systems used in the provision of the Reward Platform, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management

Virtual Incentives maintains security incident management policies and procedures. Virtual Incentives notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Virtual Incentives or its agents of which Virtual Incentives becomes aware to the extent permitted by law.

Virtual Incentives publishes system status information on the Virtual Incentives Trust website. Virtual Incentives typically notifies customers of significant system incidents by email, and for incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and Virtual Incentives' response.

User Authentication

Access to the Reward Platform requires authentication via one of the supported mechanisms as described in the Virtual Incentives Security Guide, including user ID/password or SAML based Federation as determined and controlled by the customer. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Physical Security
Production data centers used to provide the Reward Platform have access control systems that permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilize redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems. Facilities are secured by around-the-clock guards, interior and exterior surveillance cameras, two-factor access screening and escort-controlled access. In the event of a power failure, uninterruptible power supply and continuous power supply solutions are used to provide power while transferring systems to on-site back-up generators.

Reliability and Backup
All Web servers and Database servers are configured in a redundant configuration. All Customer Data submitted to the Reward Platform is stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to the Reward Platform is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance. Backups are encrypted and verified for integrity and stored both locally in the same data centers as their instance; as well as an offsite location.

Disaster Recovery
Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. The Reward Platform utilizes secondary facilities that are geographically diverse from their primary data centers, along with the required hardware, software, and Internet connectivity, in the event Virtual Incentives production facilities at the primary data centers were to be rendered unavailable.

Virtual Incentives has disaster recovery plans in place and tests them at least once per year. The scope of the disaster recovery exercise is to validate the ability to failover a production instance from the primary data center to the secondary data center utilizing developed operational and disaster recovery procedures and documentation. The Reward Platform' disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Covered Service (recovery time objective) within 12 hours after Virtual Incentives declaration of a disaster; and (b) maximum Customer Data loss (recovery point objective) of 4 hours. However, these targets exclude a disaster or multiple disasters causing the compromise of both data centers at the same time, and exclude development and test bed environments, such as the Sandbox service.

Data Encryption
The Reward Platform use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Reward Platform, including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128 bit symmetric encryption keys at a minimum. All data, including Customer Data, is transmitted between data centers for replication purposes across a dedicated, encrypted link utilizing AES-256 encryption. Additionally, all data in the Reward Platform is encrypted at rest utilizing Transparent Data Encryption (TDE).

Deletion of Customer Data
Customer Data submitted to the Reward Platform is retained in inactive status within the Reward Platform for 360 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days. Physical media on which Customer Data is stored during the contract term is not removed from the data centers that Virtual Incentives uses to host Customer Data unless the media is at the end of its useful life or being deprovisioned, in which case the media is first sanitized before removal. This process is subject to applicable legal requirements.

Analytics

Virtual Incentives may track and analyze the usage of the Reward Platform for purposes of security and helping Virtual Incentives improve both the Reward Platform and the user experience in using the Reward Platform. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.

Virtual Incentives may share anonymous usage data with Virtual Incentives service providers for the purpose of helping Virtual Incentives in such tracking, analysis and improvements. Additionally, Virtual Incentives may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our services.

Interoperation with Other Services
The Reward Platform may interoperate or integrate with other services provided by Virtual Incentives or third parties.