VIRTUAL INCENTIVES

Security Statement

Thousands of users have entrusted Virtual Incentives with their reward recipient data, delivering millions of rewards each year. We make it a priority to take our users' security and privacy concerns seriously. We strive to ensure that user data is kept securely, and that we collect only as much personal data as is required to provide our services to users in an efficient and effective manner.

Virtual Incentives uses some of the most advanced technology for Internet security that is commercially available today. This Security Statement is aimed at being transparent about our security infrastructure and practices, to help reassure you that your data is appropriately protected.

Application and User Security

- SSL/TLS Encryption: All communications, in transit, to and from the Virtual Incentives Reward Platform is sent over SSL/TLS connections. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) technology (the successor technology to SSL) protect communications by using both server authentication and data encryption. This ensures that user data in transit is safe, secure, and available only to intended recipients.
- Data Encryption: All data is stored in encrypted format at rest.
- User Passwords: User application passwords have minimum complexity requirements. Passwords are individually salted and hashed.
- User Authentication: User data on our database is logically segregated by account-based access rules. User accounts have unique usernames and passwords that must be entered each time a user logs on. Virtual Incentives issues a session cookie only to record encrypted authentication information for the duration of a specific session. The session cookie does not include the password of the user.
- Privacy: We have a comprehensive privacy policy that provides a very transparent view of how we handle your data, including how we use your data, who we share it with, and how long we retain it.

Continued

Security Statement (page two)

VIRTUAL INCENTIVES

Physical Security

- Data Centers: Our information systems infrastructure (servers, networking equipment, etc.) is located at a third party SSAE 16/SOC 2 audited data center.
- Data Center Security: Our data center is staffed and surveilled 24/7. Access is secured by security guards, visitor logs, and entry requirements such as passcards and biometric recognition. Our equipment is kept in locked cages.
- Environmental Controls: Our data center is maintained at controlled temperatures and humidity ranges which are continuously monitored for variations. Smoke and fire detection and response systems are in place.
- Location: All user data is stored on servers located in the United States.

Availability

- Power: Servers have redundant internal and external power supplies. Data center has backup power supplies, and is able to draw power from the multiple substations on the grid, several diesel generators, and backup batteries.
- Failover: Our database is log-shipped to standby servers and can failover in less than an hour.
- Connectivity: Fully redundant IP network connections with multiple independent connections to a range of Tier 1 Internet access providers.
- Uptime: Continuous uptime monitoring, with immediate escalation to Virtual Incentives staff for any downtime.

Network Security

- Third Party Scans: Security scans are performed weekly.
- Testing: System functionality and design changes are verified in an isolated test "sandbox" environment and subject to functional and security testing prior to deployment to active production systems.
- Firewall: Firewall restricts access to all ports except 80 (http) and 443 (https). Port 80 traffic is automatically redirected to port 443.
- Patching: Latest security patches are applied to all operating system and application files to mitigate newly discovered vulnerabilities.
- Access Control: Secure VPN, multifactor authentication, and role-based access is enforced for systems management by authorized engineering staff.
- Logging and Auditing: Central logging systems capture and archive all internal systems access including any failed authentication attempts.
- Monitoring: Intrusion Detections System (IDS) and Web Application Firewall (WAF) monitor and protect network traffic and systems against malicious activities.

Continued

Security Statement (page three)

VIRTUAL INCENTIVES

Storage Security

- Backup Frequency: Backups occur hourly internally, and daily to a centralized backup system.
- Production Redundancy: Data stored on a RAID 10 array.

Organizational & Administrative Security

- Employee Screening: We perform background screening on all employees.
- Training: We provide security and technology use training for employees.
- Service Providers: We screen our service providers and bind them under contract to appropriate confidentiality obligations if they have access to any user data.
- Access: Access controls to sensitive data in our databases, systems and environments are set on a need-to-know / least privilege necessary basis.
- Audit Logging: We maintain and monitor audit logs on our services and systems.
- Information Security Policies: We maintain internal information security policies, including incident response plans, and regularly review and update them.

Software Development Practices

- Stack: We code in C# and run on SQL Server 2012 and Windows 2008 R2 Server.
- Coding Practices: Our engineers use best practices and industry-standard secure coding guidelines to ensure secure coding.
- Validation: Application security testing is performed quarterly or in advance of major releases, via third party application service testing.

Handling of Security Breaches

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if Virtual Incentives learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under various state and federal laws and regulation, as well as any industry rules or standards that we adhere to. Notification procedures include providing email notices or posting a notice on our website if a breach occurs.