Reward Gateway Client Due Diligence – USA

Classification – Confidential

March 2019 – Version 8.2

RewardGateway
the employee engagement people

745 Atlantic Avenue
Boston MA 02111
USA

Document Information

This document is provided for the exclusive purpose of evaluating Reward Gateway's services and contract provision capability. It must not be passed to any 3rd party without the express written permission of Reward Gateway (USA) Inc. The information in this document is confidential.

Information Security is our most important task

Overview of Security Standards

The security of employee data is our single highest priority. We invest heavily in people, processes and robust resources for Information Security. Reward Gateway's data security provisions are second to none and have been through some of the toughest tests and accreditations by government and US corporate clients.

Key points at a glance

1	Reward Gateway was the first benefits provider to achieve certification to ISO 27001 (Information Security Management System) standard for its technology platform.
2	We use Amazon Web Services (AWS), an ultra-secure cloud provider, to house our data. AWS holds its own ISO 27001 certificate amongst many other compliance programs, and is a PCI DSS Level 1 compliant Service Provider. For more information please visit https://aws.amazon.com/compliance.
3	Our systems are tested monthly by automated scans using Tenable.io which monitors our PCI DSS compliance and general vulnerability management.
4	We arrange annual penetration tests on our applications and infrastructure, and share those results in this document.

ISO 27001 certificate for Information Security Management System

In June 2009, Reward Gateway became certified by BSi to the stringent ISO 27001 international security standard. The scope of our assessment covered all of our operations around the world. BSi's strict three stage auditing process takes over a year and comprises multiple visits by their assessor. Systems, processes, procedures, staff training, and governance are all strictly vetted.

We have reassessment audits every six months which are conducted to assure our compliance with the latest standard version released in 2013. Our ISO 27001 certificate and the associated scope are provided in Appendix 1.

Ultra-secure cloud hosting – AWS

All of the employee data that we hold is stored in highly secure AWS data centers in Dublin, IE and Frankfurt, DE. The AWS infrastructure puts strong safeguards in place to help protect your privacy. We utilise both locations which provides our clients with a resilient and highly available service.

No client's personal data is ever stored on a workstation or removable media in any of our offices. AWS's ISO 27001 certificate and the associated scope is provided in Appendix 2.

Credit card security – PCI DSS Compliance

As a business that takes credit and debit card payments online we are subject to the Payment Card Industry Data Security Standard (PCI DSS). This standard, developed in collaboration with card providers such as Visa, MasterCard, and American Express, specifies what should and should not be done during a transaction. The compliance has the specific aim of reducing fraud.

All online transactions passing through Reward Gateway are securely processed by our payment gateway Checkout. Checkout (www.checkout.com) is a Level 1 PCI DSS Service Provider and a principal member and a direct acquirer of all major card brands (VISA/ Mastercard/ AMEX). More details are available on request.

Multi-tiered security architecture

We operate a multi-tiered approach to the safeguarding of data against unauthorised access:

Tier 1 – Physical data security

All employee data is housed in our secure cloud which is located at AWS ultra-secure data centers. AWS data center physical security begins at the Perimeter Layer. This Layer includes a number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures. We can supply more details on the levels of security afforded by AWS on client request.

Within our offices, employee data is only accessed routinely by our Support Team. They all use custom built terminals which restrict the use of external websites and items such as USB memory sticks. It is not possible to download data from these terminals and they can only be accessed from a secure area by employees with the relevant access privileges.

Tier 2 – System and application security

We use a wide range of techniques to maintain the logical data security of our systems. For security reasons, we do not reveal full details of these, however, they do include but are not limited to:

- TLS encryption for communication to our web platform.
- Forced complex password system and two-factor authentication for admin and management logins.
- Time and day based login restrictions for admin and management consoles.
- IP address login restrictions for admin and management consoles.
- Multi-tier admin and management user logins which maintain lowest 'need to know' security authentication for Reward Gateway's own staff.
- Full admin and management system login audit trail.
- Auto-lockout of systems after multiple incorrect password attempts preventing brute force attacks.

HR policies, employment contracts, and robust training schedules are all in place to enforce data security and privacy. They also ensure that all staff are aware of the critical role they play in maintaining the security of our data.

Although we have strict policies to prevent staff from downloading any employee data onto laptops and computers, we also have additional preventative measures in place. It is impossible through the admin control panel of our systems to actually perform an

extract or dump of the database. In addition, we use encrypted hard disks on all PC's and laptops in the office as an additional level of protection.

External penetration testing

Annually, we commission an independent, qualified assessor to conduct a remote security review of our web-based applications. The assessors use vulnerability testing software and manual techniques, both unauthenticated and authenticated with appropriate user credentials.

The testing methodology is based on best practice as described by the Open Web Application Security Project (OWASP). The OWASP organisation provides awareness about web application security and is widely recognised within commercial and government sectors. The following key areas are tested:

- Authorisation.
- Business logic.
- Authentication.
- Data validation.
- Server configuration.
- Information gathering.
- Session management.
- Configuration management.

Further tests undertaken by clients

In addition to our own tests, several of our clients conduct their own third party penetration tests. Reward Gateway has successfully been through penetration tests by a variety of clients who used industry leading consultants.

In addition we have successfully completed the American Express Project Governance Board process which included security audits on site.

We are always happy to work with clients who would like to undertake their own testing or audit.

Classification of findings

We always use CREST certified penetration testers who report vulnerabilities by their Common Vulnerability Scoring System (CVSS) score, which is qualitatively represented by the following categories:

- **Critical vulnerabilities** have a CVSS score of 9.0 or above
- **High vulnerabilities** have a CVSS score of 7.0 - 8.9
- **Medium vulnerabilities** have a CVSS score of 4.0 - 6.9
- **Low vulnerabilities** have a CVSS score of 1.0 - 3.9

Our current penetration test results

Reward Gateway conducts a penetration test annually. The last test was conducted in January 2018 by First Base Technologies. Oli Cansdale was the Penetration Tester and the project was overseen by Chris Watt, Penetration Tester (Team Lead).

Testing credentials

The Consultants at First Base are UK Government Security Cleared. First Base Technologies is a Registered Security Specialist with the British Computer Society and employ Certified Information Systems Security Professionals. They are also members of the Information Systems Security Association.

ISMS penetration test policy

Reward Gateway's policy is to disclose two aspects of the annual penetration test results:

1. We disclose the number and nature of any critical vulnerabilities found, along with details and progress of what is being done to mitigate them.
2. We disclose the number and nature of any high or medium vulnerabilities found that remain open 21 days after the penetration test.

For security reasons, further information on the penetration test results is not made available. Clients requiring more detailed information are able to arrange or conduct their own testing.

Results of the test in January 2018

Part 1 # Critical vulnerabilities found	0 (zero)
Part 2 # High or medium vulnerabilities found that remained open 21 days after the test	0 (zero)

Reward Gateway's Leadership Team has therefore concluded that the penetration test in 2018 has been successful and no further actions are required. The company

continues to view security as an unfinished, ongoing issue which is subject to continual assessment and improvement. We intend to continue driving improvements wherever they can be identified.

Next scheduled penetration test

Our next annual penetration test will be scheduled for June 2019.

Financial integrity

With 99% of clients paying annually in-advance for services, Reward Gateway has always been a cash-flow positive business. We have grown quickly but carefully. Our financial and other accounts reflect this.

On July 29th 2015, Reward Gateway (USA) Inc. was acquired, along with the rest of the group, by Great Hill Partners, L.P. providing further financial backing and resources to the company.

Fully-funded Cashback

Many clients ask us for information about Cashback, including how it is funded and where it is kept. We take a very strict approach to Cashback handling and provision which is unique to our industry.

This is because we fully fund all Cashback recorded in member accounts as soon as we receive the incoming payment from the retailer, via their processing system. No amount of received Cashback is used for the day to day running of Reward Gateway. This gives us and our clients the security that if all members withdrew their Cashback simultaneously there would be no impact on our operations or finance.

Dormant and closed accounts

Where a member has left employment and has left an amount of Cashback in their account without withdrawing it, we advertise that they can withdraw the funds for 60 days. To comply with regulations we will only retain personal information for 60 days after the administrator lets us know or an account is set as revoked. In practice, this policy does not have a material effect as we find almost all employees withdraw their Cashback within a short period. The few that leave a small amount behind tend not to come back after that time.

After 60 days, any money left in a closed member account is taken to Reward Gateway's profit and loss account to offset bank charges and other finance costs.

Privacy

In addition to data security, Reward Gateway's Privacy Policy is critical to our security operations. Whilst data security protects employee information from potential attack, privacy looks at how we intentionally use the data to which we have access. Link to our Privacy Policy can be found at the bottom of your programme page. The policy is aligned with data privacy laws in California which are known to be the most stringent in the United States.

100% Privacy guaranteed. No exceptions.

Our rules on privacy are simple and have never changed. We do not sell, rent, lease or lend your employees' personal data to any third parties. That's it, no exceptions. When we promote offers to your employees that we think they would like – assuming that they have opted in to receive them – it is Reward Gateway that sends the email. The name and personal information is never given to a third party.

Appendix 1: ISO 27001 Certificate for Reward Gateway

bsi.

By Royal Charter

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that:

Reward Gateway (UK) Ltd
265 Tottenham Court Road
London
W1T 7RQ
United Kingdom

Holds Certificate Number: IS 544153

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

The provision of integrated voluntary benefits to private, public and not-for-profit organisations. This is in accordance with the Statement of Applicability version 8 dated 12/02/2018

For and on behalf of BSI:

Andrew Launn, EMEA Systems Certification Director

Original Registration Date: 2009-06-25
Latest Revision Date: 2018-06-18

Effective Date: 2018-06-26
Expiry Date: 2021-06-25

Page: 1 of 2

...making excellence a habit.

Appendix 2: ISO 27001 Amazon Web Services (AWS)

Certificate

Certificate number: 2013-009

Certified by EY CertifyPoint since: November 18, 2010

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015, the Information Security Management System as defined and implemented by

Amazon Web Services, Inc.*

and its affiliates (collectively referred to as Amazon Web Services (AWS)) are compliant with the requirements as stated in the standard:

ISO/IEC 27001:2013

Issue date of certificate: December 11, 2011
Re-issue date of certificate: December 3, 2018
Expiration date of certificate: November 7, 2019

EY CertifyPoint will, according to the certification agreement dated November 9, 2016, perform surveillance audits and acknowledge the certificate until the expiration date noted above.

**With regard to the specific requirements for information security as stated in the Statement of Applicability, version 2018.01 dated November 1, 2018 this certification is applicable to (a) the services and their associated assets and locations as described in the scoping section of this certificate, and (b) any affiliates that are responsible for, or that contribute to, the provision of such services and their associated assets and locations.*

J. Sehgal | Director, EY CertifyPoint

Document History

Version	Date of Issue	Reason	Author
Issue 1	14 September 2009	Document prepared for clients called 'Information on Data Security and Privacy'	Helen Craik
Issue 1.1	17 March 2010	Update to include more information and renamed as 'Client Due Diligence Document'	Helen Craik
Issue 2	17 August 2010	Update following publication of 2010 accounts	Helen Craik
Issue 3	3 December 2010	Update with latest D&B rating.	Helen Craik
Issue 4	15 September 2011	General update to various sections, no significant additions or deletions	Sarah Millward
Issue 5	7 March 2012	Overview, first review with Danièle Thillmann	Sarah Millward & Danièle Thillmann
Issue 6	20 September 2012	Review of certificates and overall updates	Sarah Millward & Veronica Walker
Issue 7	2 October 2014	General update to various sections, review of certificates	Veronica Walker
Issue 7.1	12 March 2015	General update to various sections, review of certificates	Veronica Walker
Issue 7.2	02 April 2015	Change ownership of document	Veronica Walker
Issue 7.3	25 September 2015	Certificates updates and review	Ivan Dichev
Issue 7.4	22 December 2015	Update on pen test results	Ivan Dichev
Issue 7.5	20 June 2016	Update on PCI and Pen testing section	Ivan Dichev
Issue 7.6	21 November 2016	Certificates updates and review	Asen Varsanov
Issue 7.7	20 January 2017	Penetration test results update	Asen Varsanov
Issue 7.8	12 April 2017	Template update	Ivan Dichev
Issue 7.9	18 May 2017	Certificates updates and review	Asen Varsanov

Issue 8.0	01 August 2018	Certificates and payment gateway update	Asen Varsanov
Issue 8.1	20 February 2019	Update ASV checks with Tenable.io	Asen Varsanov
Issue 8.2	7 March 2019	Move to AWS from The Bunker	Asen Varsanov