Rebilly
Data Processing Addendum

This data processing addendum and its Annexes ("**DPA**") forms part of the API Licence Agreement or other written or electronic agreement between Rebilly and Licensee for the purchase of the Rebilly Service ("**Agreement**") to reflect the parties agreement with regard to the Processing of Personal Data. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

By signing the DPA, Licensee enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Controller Affiliates (defined below). For the purposes of this DPA only, and except where indicated otherwise, the term "Licensee" shall include Licensee and Controller Affiliates.

In the course of providing the Service to Licenses pursuant to the Agreement, Rebilly may Process Personal Data on behalf of Licensee and the parties agree to comply with the following provisions with respect to any Personal Data. This DPA shall replace any comparable or additional rights relating to the Processing of Licensee Data contained in the Agreement (including any existing data processing addendum to the Agreement).

HOW TO EXECUTE THIS DPA:

1. This DPA has been pre-signed on behalf of Rebilly. The Standard Contractual Clauses in Annex C have been pre-signed by Rebilly, Inc, as the data importer.
2. To complete this DPA, Licensee must:
    a. Complete the information in the signature box and sign on Page 6.
    b. Complete the information in the signature box and sign the Standard Contractual Clauses on Page 16.
    c. Send the completed and signed DPA by email to support@rebilly.com.
3. Upon receipt of the validly completed DPA to the above email address, this DPA will become legally effective.

The parties agree as follows:

1. Definitions

"**Affiliate**" means any entity under the control of a party where "control" means ownership of or the right to control greater than 50% of the voting securities of such entity.

"**Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

"**Licensee Data**" means any and all Personal Data that Rebilly processes as a Processor on behalf of the Licensee in course of providing the Service under the Agreement.

"**Controller Affiliates**" means any of Licensee's Affiliate(s): (a) (i) that are subject to Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (ii) permitted to use the Service pursuant to the Agreement between Licensee and Rebilly, but have not signed their own Sales Order and are not a "Licensee" as defined under the Agreement, (b) if and to the extent Rebilly processes Licensee Data for which such Affiliate(s) qualify as the Controller.

"**Data Protection Laws**" means all data protection and privacy laws and regulations applicable to the processing of Licensee Data under the Agreement, including, where applicable, EU Data Protection Law.

"**EU Data Protection Law**" means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector, and applicable national implementations of (i) and (ii) (in each case, as may be amended, superseded or replaced).

"**Group**" means any and all Affiliates that are part of an entity's corporate group.

"Standard Contractual Clauses" means the standard contractual clauses for Processors as approved by the European Commission in the form set out in Annex C.

"**Personal Data**" means any information relating to an identified or identifiable natural person to the extent that such information is protected as personal data under applicable Data Protection Law.

"**Processor**" means an entity that processes Personal Data on behalf of the Controller.

"**Processing**" has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly.

"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Licensee Data transmitted, stored or otherwise processed by Rebilly and/or its Sub-processor's in connection with the provision of the Service.

"**Service**" means any product or service provided by Rebilly to Licensee pursuant to and as more particularly described in the Agreement.

"**Sub-processor**" means any Processor engaged by Rebilly or its Affiliates to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA. Sub-processors may include third parties or members of the Rebilly Group but shall exclude any Rebilly employee or consultant.

2. Scope and Applicability of this DPA

2.1 **Scope.** This DPA applies where and only to the extent that Rebilly processes Licensee Data as a Processor on behalf of the Licensee in the course of providing the Service and such Licensee Data is subject to Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom (collectively for the purposes of this DPA, the "**EU"**).

2.2 **Role of the Parties**. As between Rebilly and Licensee, Licensee is the Controller of Licensee Data, and Rebilly shall process Licensee Data only as a Processor on behalf of Licensee. Nothing in the Agreement or this DPA shall prevent Rebilly from using or sharing any data that Rebilly would otherwise collect and process independently of Licensee's use of the Service. Any processing of Personal Data under the Agreement shall be performed in accordance with applicable Data Protection Laws. However, Rebilly is not responsible for compliance with any Data Protection Laws applicable to Licensee or Licensee's industry that are not generally applicable to Rebilly as a service provider.

2.3 **Licensee Obligations**. Licensee agrees that (i) it shall comply with its obligations as a Controller under Data Protection Laws in respect of its processing of Licensee Data and any processing instructions it issues to Rebilly; and (ii) it has provided notice and obtained (or shall obtain) all consents (where required) and rights necessary under Data Protection Laws for Rebilly to process Licensee Data and provide the Service pursuant to the Agreement and this DPA.

2.4 **Rebilly Processing of Licensee Data**. As a Processor, Rebilly shall process Licensee Data only for the following purposes: (i) processing to provide the Service in accordance with the Agreement; (ii) processing to perform any steps necessary for the performance of the Agreement; (iii) processing initiated by Users in their use of the Service; and (iv) processing to comply with other reasonable instructions provided by Licensee (e.g. via email or support tickets) that are consistent with the terms of this Agreement (individually and collectively, the "**Purpose**") and only in accordance with Licensee's documented lawful instructions. The parties agree that the Agreement (including this DPA) set out the Licensee's complete and final instructions to Rebilly in relation to the processing of Licensee Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Licensee and Rebilly.

2.5 **Details of Data Processing**. The subject matter of the processing of Licensee Data by Rebilly is the Purpose. Unless otherwise agreed in writing between the parties, the duration of processing, the nature and purpose of the processing, the types of Licensee Data and the categories of data subjects processed under the Agreement are further specified in Annex A (Description of the Processing Activities) to this DPA.

3. Subprocessing

3.1 **Authorized Sub-processors**. Licensee agrees that Rebilly may engage Sub-processors to process Licensee Data on Licensee's behalf. The Sub-processors currently engaged by Rebilly and authorized by Licensee are listed here https://www.rebilly.com/sub-processors. Rebilly shall notify Licensee if it adds or removes Sub-processors at least 10 days prior to any such changes.

3.2 **Sub-processor Obligations.** Rebilly shall: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Licensee Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Rebilly to breach any of its obligations under this DPA.

3.3 **Objection to Sub-processors**. Licensee may object in writing to Rebilly's appointment of a new Sub-processor on reasonable grounds relating to data protection (e.g. if making Licensee Data available to the Sub-processor may violate applicable Data Protection Law or weaken the protections for such Licensee Data) by notifying Rebilly promptly in writing within five (5) calendar days of receipt of Rebilly's notice in accordance with Section 3.1. Such notice shall explain the reasonable grounds for the objection. In such event, the parties shall discuss such concerns in good faith with a view to achieving commercially reasonable resolution.

4. Security and Audits

4.1 **Security Measures**. Rebilly shall implement and maintain appropriate technical and organizational security measures to protect Licensee Data from Security Incidents and to preserve the security and confidentiality of the Licensee Data. Such measures shall, at a minimum, include the measures identified in Annex B ("**Security Measures**"). Rebilly shall ensure that any person who is authorized by Rebilly to process Licensee Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty). To the extent that Rebilly processes payment card data, Rebilly shall adhere to and maintain compliance with the current applicable version of the Payment Card Industry's Data Security Standard ("**PCI DSS**").

4.2 **Security Incident Response**. Upon becoming aware of a Security Incident, Rebilly shall notify Licensee without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Licensee.

4.3 **Updates to Security Measures**. Licensee acknowledges that the Security Measures are subject to technical progress and development and that Rebilly may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service purchased by the Licensee.

4.4 **Licensee Responsibilities**. Notwithstanding the above, Licensee agrees that except as provided by this DPA, Licensee is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Licensee Data when in transit to and from the Service and taking any appropriate steps to securely encrypt or backup any Licensee Data uploaded to the Service.

4.5 **Security Reports and Audits.** Rebilly audits its compliance against recognised data protection and information security standards on a regular basis. Such audits are conducted by independent, experienced personnel, and may include Rebilly's internal audit team and/or third party auditors engaged by Rebilly. Upon request, Rebilly shall supply (on a confidential basis) a summary copy of its then-current audit report(s) ("**Report**") to Licensee, so that Licensee can verify Rebilly's compliance with this DPA. The Report should, among others, demonstrate a valid PCI compliance certification and/or the relevant and required sections from the latest annual PCI DSS compliance audit performed on Rebilly (and on its subcontractors, where applicable). Rebilly shall also provide written responses (on a confidential basis) to all reasonable requests for information made by Licensee related to its Processing of Licensee Personal Data, including responses to information security and audit questionnaires that are necessary to confirm Rebilly's compliance with this DPA, provided that Licensee shall not exercise this right more than once per year, except that this right may also be exercised in the event Licensee is expressly requested or required to provide this information to a data protection authority, or Rebilly has experienced a Security Incident, or other reasonably similar basis.

5. International Transfers

5.1 **Processing Locations**. Rebilly may transfer and process Licensee Data to and in the United States and anywhere else in the world where Rebilly, its Affiliates or its Sub-processors maintain data processing operations. Rebilly shall at all times ensure appropriate safeguards to protect the Licensee Data processed, in accordance with the requirements of Data Protection Laws.

5.2 **Standard Contractual Clauses**. If and to the extent Rebilly processes or transfers (directly or via onward transfer) Licensee Data that is subject to Data Protection Laws of the EU in or to any country or recipient not recognized as providing an appropriate safeguards or adequate protection for Personal Data (as described in applicable Data Protection Law), the parties agree that Rebilly shall be deemed to provide appropriate safeguards (within the meaning of applicable Data Protection Law) for any such Licensee Data by complying with the Standard Contractual Clauses. For the purposes of the Standard Contractual Clauses, Rebilly agrees that it is a "data importer" and Licensee is the "data exporter" (notwithstanding that Licensee may be an entity located outside of the EU).

5.3 **Alternative Transfer Mechanism**. The parties agree that the data export solution identified in this Section 5 shall not apply if and to the extent that Rebilly adopts an alternative data export solution for the lawful transfer of Licensee Data (as recognized under applicable Data Protection Law) outside of the EU (“**Alternative Transfer Mechanism**”), in which event, the Alternative Transfer Mechanism shall apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which Licensee Data is transferred).

6. Return or Deletion of Data

6.1 Upon termination or expiration of the Agreement, Rebilly shall (at Licensee's election) delete or return to Licensee all Licensee Data (including copies) in its possession or control, save that this requirement shall not apply to the extent Rebilly is required by applicable law to retain some or all of the Licensee Data, or to Licensee Data it has archived on back-up systems, which Licensee Data Rebilly shall securely isolate and protect from any further processing, except to the extent required by applicable law.

7. Rights of Data Subjects and Cooperation

7.1 **Data Subject Request**. To the extent that Licensee is unable to independently access the relevant Licensee Data within the Service, Rebilly shall (at Licensee's expense) taking into account the nature of the processing, provide reasonable cooperation to assist Licensee by appropriate technical and organisational measures, in so far as is possible, to respond to any requests from individuals or applicable data protection authorities relating to the processing of Licensee Data under the Agreement. In the event that any such request is made directly to Rebilly, Rebilly shall not respond to such communication directly without Licensee's prior authorization, unless legally compelled to do so. If Rebilly is required to respond to such a request, Rebilly shall promptly notify Licensee and provide it with a copy of the request unless legally prohibited from doing so.

7.2 **Subpoenas and Court Orders**. If a law enforcement agency sends Rebilly a demand for Licensee Data (for example, through a subpoena or court order), Rebilly shall give Licensee reasonable notice of the demand to allow Licensee to seek a protective order or other appropriate remedy unless Rebilly is legally prohibited from doing so.

7.3 **Data Protection Impact Assessment**. To the extent Rebilly is required under EU Data Protection Law, Rebilly shall (at Licensee's expense) provide reasonably requested information regarding Rebilly's processing of Licensee Data under the Agreement to enable the Licensee to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

8. Controller Affiliates

8.1 **Contractual Relationship**. The parties acknowledge and agree that, by executing the DPA, Licensee enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Controller Affiliates, thereby establishing a separate DPA between Rebilly and each such Controller Affiliate subject to the provisions of the Agreement and this Section 8 and Section 9. Each Controller Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Controller Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Service by Controller Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by a Controller Affiliate shall be deemed a violation by Licensee.

8.2 **Communication**. The Licensee that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Rebilly under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Controller Affiliates.

8.3 **Rights of Controller Affiliates**. If a Controller Affiliate becomes a party to the DPA with Rebilly, it shall, to the extent required under applicable Data Protection Laws, also be entitled to exercise the rights and seek remedies under this DPA, provided that except where applicable Data Protection Laws require the Controller Affiliate to exercise a right or seek any remedy under this DPA against Rebilly directly by itself, the parties agree that (i) solely the Licensee that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Controller Affiliate, and (ii) the Licensee that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Controller Affiliate individually but in a combined manner for all of its Controller Affiliates together.

9. Limitation of Liability

9.1 Each party’s and all of its Affiliates’ liability, taken together in the aggregate, arising out of or related to this DPA (including the Standard Contractual Clauses), and all DPAs between Controller Affiliates and Rebilly, whether in contract, tort or under any other theory of liability, is subject to the limitations and exclusions of liability in the Agreement, and any reference in provisions to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

9.2 For the avoidance of doubt, Rebilly and its Affiliates’ total liability for all claims from the Licensee and all of its Controller Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Licensee and all Controller Affiliates, and, in particular, shall not be understood to apply individually and severally to Licensee and/or to any Controller Affiliate that is a contractual party to any such DPA.

10. Miscellaneous

10.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

10.2 With effect from the effective date of this DPA, this DPA shall be deemed a part of and incorporated into the Agreement so that references in the Agreement to "Agreement" shall be interpreted to include this DPA.

10.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

10.4 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

10.5 This DPA shall only become legally binding between Licensee and Rebilly when the formalities and steps set out in Section "**HOW TO EXECUTE THIS DPA**" above have been fully completed.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative:

Rebilly, Inc

Signature:

Name: Adam Altman

Title: CEO

Date: December 20, 2018

Licensee

Signature:

Licensee Legal Name:
____

Print Name:___________________________

Title: __________________________

Date: _________________________]

Annex A

Details of Processing

(a) Duration. The duration of the processing under this DPA is determined by the Agreement.

(b) Categories of data subjects.

- **Users –** Licensee's employees, personal and other staff that are authorized to use the Service under the Licensee's account.
- **End Customers** - any end users/ customer/ client of the Licensee whose data is processed through the Service.

(c) Categories of data: Identification and contact data (name, date of birth, address, e-mail address, telephone number, company name, ID and KYC documents); financial information (payment card details, alternative payment card details); order information; IT related data (IP addresses, unique device level identifiers, cookies data, online navigation data (including access date and times), location data, browser data language); and any other Personal Data Licensee configures the Service to collect. Licensee data fields may also be configured as part of the implementation of the Service or as otherwise permitted within the scope of the Service.

(d) Special categories of data (if appropriate). Rebilly and/or its Sub-processors contractors do not intentionally collect or process any special categories of data in connection with the provision of the Service under the Agreements.

(e) Purposes of Processing: For the Purposes (as defined in this DPA).

(f) Processing operations: The Licensee Data transferred will be processed in accordance with the Agreement and may be subject to the following processing activities:

(i) storage and other processing necessary to provide, maintain and improve the Service provided to Licensee

(ii) to provide Licensee and technical support to the Licensee; and

(iii) disclosures in accordance with the Agreement and as compelled by law.

Annex B
Security Measures

Rebilly will implement and maintain technical and administrative safeguards to protect Licensee Data against Security Incidents, including by taking the following security measures:

Network protection

- Have in place a current network diagram with all connections to cardholder data, including any wireless networks
- Access to web administration interfaces must be encrypted or disabled. All administrative access made on a non-console must be encrypted.
- Configuration files must be secure and synchronized.
- The firewalls must be configured to not be alterable by its users, including on mobile and employee-owned devices. The firewall, regardless of its installed location, must be enabled at all time.
- Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered being insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.
- Create a firewall configuration that restricts connections between approved networks and all the components of the system in the environment of the data of cardholders. Need to examine the rules of firewalls and routers at least every six months. A rule "blocks all" must still apply in the end. Firewalls must be used at least at every endpoint connecting to the Internet, including mobile and employee-owned devices.
- Prohibit direct public access between Internet and any component of the system in the environment of the data of cardholders.
- Disable all services and protocols not required (services and protocols not directly needed to perform the specified function of the device).
- Encrypt all administrative access with the use of technologies such as SSH, VPN, or SSL/TLS for Web-based management and other administrative access.
- Validation of secure communications.
- Restrict physical access to publicly accessible network jacks.
- Restrict physical access to the gateways, mobile handheld devices and wireless access points.
- Use intrusion detection systems and/or intrusion prevention systems to monitor all traffic in the data environment from cardholders and report to staff all suspicions relating to potential alterations. Keep all detection and intrusion prevention engines updated.
- When you access the cardholder’s data through remote access technologies, prohibit copying, moving and storing of cardholder’s data on local hard drives and removable electronic media.
- Network architecture and its segmentation approach must be setup to permit: isolation, control, supervision and optimization of information flow and control. Those zones must consider internal and external users, privilege levels, business partners, service providers, customers and the general public.
- The firewall and antivirus logs should be reviewed daily.
- All PCI firewall rules must be reviewed at least every six months.
- The firewall used for the PCI zone must be statefull.
- When necessary, ACLs can be implemented in routers, but firewalls must be given priority at all times (for ACL).
- Account passwords should be configured using the 'Secret' command replacing the "Password" command (if equipment allows).
- When configuring a service that doesn’t offer encrypted and strong authentication, the use of a "high port" is mandatory.
- Mandatory strong (double) authentication for establishing remote connection over the network.

- Secure communications must be validated / tested before being put into production.
- When performing a remote access into a PCI zone, copying, moving and storing data of cardholders on local disks or a removable media is prohibited.

Trainings

Have in place security and privacy awareness training, inclusive of acknowledgment and agreement to abide by organizational security policies, for all personnel upon hire and annually thereafter.

Credit Card Information Protection

- Keep cardholder data storage to minimum by implementing data retention and disposal policies, procedures and processes.
- Do not store sensitive authentication data after authorization (even if encrypted). Note: It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.
- Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).
- Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using any of the following methods: a) One-way hashes based on strong cryptography; b) Truncation; c) Index tokens and pads, with the pads being securely stored and d) Strong cryptography, with associated key-management processes and procedures
- Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plaintext).
- Examine a sample of removable media.
- Examine a sample of audit logs to verify that the PAN is rendered unreadable.
- Physically secure all media.
- Maintain strict control over the internal or external distribution of any kind of media.

Access Control

- Limit access to system components and cardholder data to only those individuals whose job requires such access.
- Assignment of privileges is based on individual personnel’s job classification and function.
- Requirement for a documented approval by authorized parties specifying required privileges.
- Implementation of an automated access control system.
- Defining a system of access control for the components of systems with multiple users that restricts access to only users that need access to data and which is set to 'deny all access' unless they are explicitly allowed.
- Assign all users a unique ID before allowing them to access system components or data of cardholders.
- In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: password or two-factor authentication.
- Integrate authentication with two factors for the remote access (access to the network from outside the network level) employees, administrators, and third parties to the network.
- Render all passwords unreadable during transmission and storage on all system components using strong cryptography.
- Ensure that proper management of passwords and the user authentication is implemented for non-consumer users and administrators.

- Control the addition, removal, and modification of user IDs, to credentials and other objects identifier.
- Set initial passwords unique to each user and change immediately after the first use.
- Immediately revoke access for any user who no longer works for the company.
- Remove/disable inactive user accounts at least every 90 days.
- Do not use group, shared, or generic accounts and passwords, or other authentication methods.
- Change the passwords at least every 90 days.
- Requiring passwords with at least seven characters.
- Define passwords with alphanumeric characters.
- Prohibit a user to submit a new password identical to one of its last four passwords.
- Limit repeated access attempts by locking out the user ID after six attempts.
- Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID
- If a session is inactive for more than 15 minutes, require the user to re-enter his password to re-activate the terminal.
- Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.
- Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- All actions taken by any individual with root or administrative privileges
- Automatic disconnect of sessions of remote access technologies after a specific idle period.

Data Retention

- Keep cardholder data storage to a minimum
- Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis.

Secure Application Development

- Validation of all input to prevent XSS (Cross-Site Scripting) attacks, attacks by injection, the execution of malicious files, etc.
- Validation of proper error handling.
- Validation of secure cryptographic storage.
- Separate development/test and production environments.
- Separate obligations between development/test and production environments.
- Deleting data and the test accounts before production systems become active.
- Deletion of custom application accounts and the names of user and password before enabling applications or making them available to customers.
- In order to identify any potential coding vulnerability, review of custom code prior to placing it into production or at the disposal of clients.
- Operational functionality testing.
- Develop all Web applications (internal and external, including Web administrative access) on the basis of secure coding best practices such as those described in the OWASP (Open Web Application Security Project). Prevent common coding vulnerabilities in software development processes.

System Monitoring

- Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.
- Ensure that all anti-virus mechanisms are current, running and capable of generating audit logs.
- Install critical security patches within one month of release.
- Define a process for the identification of new security vulnerabilities.

- For public-oriented Web applications, address new threats and vulnerabilities on a regular basis.
- Access to all audit trails.
- Invalid logical access attempts.
- Use of identification and authentication mechanisms.
- Initialization of the audit logs.
- Creation and deletion of system-level objects.
- Record at least the following audit trail entries for all system components for each event
- Synchronize all critical system clocks and hours.
- Protect audit logs so that they cannot be changed.

Change Management Policy

- Formal approval process and test all network connections and changes to the configurations of firewalls and routers.
- Check that the network diagram is updated.
- Test all security patches, as well as any system or software configuration changes before deployment.
- Documentation of impact
- Validation of the management by the appropriate parties.
- Removal procedures.

Incident Response

Implement an incident response plan. Be prepared to respond immediately to a system breach.

Secure Disposal of IT Equipment and Information

Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

Crypto Measures Standard

- Protect encryption keys used for encryption of card data against disclosure and misuse.
- Restrict access to cryptographic keys to the smallest possible number of operators.
- Store cryptographic keys securely in as few locations and forms as possible.
- Verify the existence of management procedures for keys used for encryption of the data of cardholders.
- Generation of strong cryptographic keys.
- Secure the distribution of cryptographic keys.
- Secure storage of cryptographic keys.
- Periodic change of cryptographic keys as deemed necessary and recommended by the associated application.
- Retirement or replacement of obsolete cryptographic keys or suspected to have been compromised.
- Prevent the substitution of cryptographic keys.
- Verify the use of encryption (such as SSL/TLS or IPSEC) whenever the data of cardholders are transmitted or received over open, public networks.

Annex C
Standard Contractual Clauses (processors)

THE PARTIES HAVE AGREED on the following Contractual Clauses (the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1. Definitions

For the purposes of the Clauses:

1.1 **'personal data'**, '**special categories of data**', '**process/processing**', '**controller**', '**processor**', '**data subject**' and '**supervisory authority**' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

1.2 **'the data exporter'** means the controller who transfers the personal data;

1.3 **'the data importer'** means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

1.4 **'the subprocessor'** means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

1.5 **'the applicable data protection law'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

1.6 **'technical and organisational security measures'** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing Service will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing Service which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(i) any accidental or unauthorised access, and

(ii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing Service by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

6.4 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Subprocessing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

11.2 The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

11.4 The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data processing Service

12.1 The parties agree that on the termination of the provision of data processing Service, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature………………………………………….………………

On behalf of the data importer:
Name (written out in full): Adam Altman
Position: CEO
Address: 3801 N Capital of Texas Hwy, E240 #72 Austin, TX 78746
Other information necessary in order for the contract to be binding (if any):

Signature………………………………………….………………

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

Data exporter: The data exporter is the entity identified as the "Licensee" in the Data Processing Addendum in place between data exporter and data importer and to which these Clauses are appended ("**DPA**").

Data importer: The data importer is Rebilly Inc. acting on behalf of itself and its Affiliates to the extent they receive and process Licensee Data in connection with the Permitted Purposes (all as defined in the DPA) ("**Rebilly**").

Description of Data Processing: Please see Annex A of the DPA for a description of the data subjects, categories of data, special categories of data and processing operations.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see Annex B of the DPA, which describes the technical and organisational security measures implemented by Rebilly.

Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").
4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 4 (Security and Audits) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.

3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

4. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*" the data exporter may provide a general consent to onward subprocessing by the data importer.

5. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Section 3 (Sub-processing) of the DPA.