Recurly Data Processing Addendum

This Data Processing Addendum ("Addendum") forms a part of the Master Services Agreement (the "Agreement") entered into by and between the customer who executed the Agreement ("Customer") and Recurly, Inc. ("Recurly"). By executing the Addendum in accordance with Section 11 herein, Customer enters into this Addendum on behalf of itself and, to the extent required under applicable Data Protection Laws (defined below), in the name and on behalf of its Affiliates (defined below), if and to the extent Recurly processes Personal Data for which such Affiliates qualify as the Controller (defined below). Any terms not defined in this Addendum shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement or any other agreement between the parties (including any prior data processing addenda), the terms and conditions of this Addendum shall supersede and control. In the event of a conflict between the Standard Contractual Clauses (as defined below and where applicable) conflict with any provision of this Addendum, the Standard Contractual Clauses shall prevail to the extent of such conflict.

1. Definitions

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2 "Anonymous Data" means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person.

1.3 "Authorized Employee" means an employee of Recurly who has a need to know or otherwise access Personal Data to enable Recurly to perform their obligations under this Addendum or the Agreement.

1.4 "Authorized Sub-Processor" means a third-party who has a need to know or otherwise access Personal Data to enable Recurly to perform its obligations under this Addendum or the Agreement, and who is either (1) listed at https://recurly.com/legal/privacy/subprocessors or (2) authorized by Customer to do so under Section 4 of this Addendum.

1.5 "Controller" (or "data controller") means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, including as applicable any "business" as defined under the CCPA (as defined below).

1.6 "Data Subject" means an identified or identifiable person to whom Personal Data relates.

1.7 "Instruction" means a direction, either in writing, in textual form (e.g. by e-mail) or by using a software or online tool, issued by Customer to Recurly and directing Recurly to Process Personal Data.

1.8 "Personal Data" means any information relating to Data Subject which is subject to Data Protection Laws (defined below) and which Recurly Processes on behalf of Customer other than Anonymous Data.

1.9 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

1.10 "Swiss-U.S. Privacy Shield Framework" means the Swiss-U.S. Privacy Shield Framework and related Principles issued by the U.S. Department of Commerce, available at http://trade.gov/td/services/odsi/swiss-us-privacyshield-framework.pdf.

1.11 "Process" or "Processing" means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.12 "Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of a Controller, including as applicable any "service provider" as defined under the CCPA (defined below).

1.13 "Services" shall have the meaning set forth in the Agreement.

1.14 "Standard Contractual Clauses" means the agreement attached as Exhibit B and forming part of this Addendum executed by and between Customer and Recurly pursuant to the European Commission's decision (C(2010)593) of February 5, 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection (or any updated version thereof).

1.15 "Supervisory Authority" means an independent public authority which is established by a member state of the European Union, the United Kingdom, Iceland, Liechtenstein, or Norway.

2. Processing of Data

2.1 The rights and obligations of Customer with respect to this Processing are described herein. Customer shall, in its use of the Services, at all times Process Personal Data, and provide instructions for the Processing of Personal Data, in compliance with the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), the California Consumer Privacy Act (the "CCPA"), and

any other applicable legislation relating to data protection and privacy (together with the GDPR and CCPA, "Data Protection Laws"). Customer shall ensure that its instructions comply with all laws, rules and regulations applicable in relation to the Personal Data, and that the Processing of Personal Data in accordance with Customer's instructions will not cause Recurly to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Recurly by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Recurly regarding the Processing of such Personal Data. Customer shall not provide or make available to Recurly any Personal Data in violation of Data Protection Laws or the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Recurly from all claims and losses in connection therewith. This Addendum does not apply to Personal Data for which Recurly is a Controller.

2.2 Recurly, in its capacity as the Processor, shall not (a) retain, use, sell, or otherwise disclose Personal Data outside of its relationship with Customer other than as expressly stated in the Agreement or in this Addendum or as necessary to provide the Services or (b) Process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, and (ii) in a manner inconsistent with the terms and conditions set forth in this Addendum or any other documented instructions provided by Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Data Protection Laws to which Recurly is subject; in such a case, Recurly shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Recurly certifies that it understands and will comply with the restrictions and obligations contained in this Addendum. Customer hereby instructs Recurly to Process Personal Data in accordance with the foregoing and as part of any Processing initiated by Customer in its use of the Services.

2.3 The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this Addendum.

2.4 Following completion of the Services, at Customer's choice, Recurly shall return or delete the Personal Data, unless further storage of Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Recurly shall take measures to block such Personal Data from any further Processing (except to the extent necessary for its continued hosting or Processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Customer and Recurly have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Recurly to Customer only upon Customer's request.

3. Authorized Employees

3.1 Recurly shall ensure that all Authorized Employees have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in relation to any Personal Data.

3.2 Recurly shall take commercially reasonable steps to limit access to Personal Data to only Authorized Employees.

4. Authorized Sub-Processors

4.1 Customer acknowledges and agrees that Recurly may (1) engage its affiliates and the Authorized Sub-Processors listed at https://recurly.com/legal/privacy/subprocessors to access and Process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the Processing of Personal Data. By way of this Addendum, Customer provides general written authorization to Recurly to engage sub-processors as necessary to perform the Services.

4.2 A list of Recurly's current Authorized Sub-Processors (the "List") is available at https://recurly.com/legal/privacy/subprocessors. Such List may be updated by Recurly from time to time. Customer acknowledges and agrees that it is solely responsible for subscribing to notifications of changes, which notification mechanism will be available through the List, in order to be notified of new Authorized Sub-Processors. Customer also acknowledges and that, aside from updating the List and informing Customer that the List has been updated, Recurly shall have no obligation to inform Customer of any additional Authorized Sub-Processors. At least ten (10) days before enabling any third party other than Authorized Sub-Processors to access or participate in the Processing of Personal Data, Recurly will add such third party to the List. Customer may reasonably object to the addition of a third party to the List on legitimate grounds by informing Recurly in writing within five (5) days of receipt of the aforementioned notice that the List has been updated. Customer acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Recurly from offering the Services to Customer.

4.3 If Customer reasonably objects to an engagement in accordance with Section 4.2, and Recurly cannot provide a commercially reasonable alternative within a reasonable period of time, Recurly may terminate the Agreement or this Addendum. Termination shall not relieve Customer of any fees owed to Recurly under the Agreement.

4.4 If Customer does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Recurly, that third party will be deemed an Authorized Sub-Processor for the purposes of this Addendum.

4.5 Processor will enter into a written agreement with the Authorized Sub-Processor imposing the same data protection obligations on the Authorized Sub-Processor as those imposed on Processor under this Addendum with respect to the protection of Personal Data. In case an Authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Processor, Processor will remain liable to Customer for the performance of the Authorized Sub-Processor's obligations under such agreement.

4.6 If Customer and Processor have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Processor of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Processor to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Recurly beforehand, and that such copies will be provided by Recurly only upon request by Customer.

5. Security of Personal Data. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Recurly shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data.

6. Transfers of Personal Data

6.1 Customer acknowledges and agrees that Recurly will process Personal Data in the United States as necessary to provide the Services. To the extent any Personal Data originates from the European Economic Area ("EEA"), the United Kingdom or Switzerland, Recurly will ensure that appropriate safeguards have been implemented for the transfer of such Personal Data to a jurisdiction that the European Commission has not determined provides an adequate level of protection for Personal Data in accordance with Data Protection Laws.

6.2 Where required, any transfer of Personal Data made subject to this Addendum to any countries which do not ensure an adequate level of data protection shall be undertaken by Recurly pursuant to the Standard Contractual Clauses.

6.3 To the extent Recurly processes any Personal Data originating from Switzerland, Recurly will process such data in accordance with Recurly's certification to the Swiss-U.S. Privacy Shield Framework. If the Swiss-U.S. Privacy Shield Framework is invalidated, Recurly shall process Personal Data originating from Switzerland pursuant to the Standard Contractual Clauses.

7. Rights of Data Subjects

7.1 Recurly shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction of Processing, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If Recurly receives a Data Subject Request in relation to Personal Data, Recurly will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services.

7.2 Recurly shall, at the request of the Customer, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Customer is itself unable to respond without Recurly's assistance and (ii) Recurly is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Recurly.

8. Actions and Access Requests

8.1 Recurly shall, taking into account the nature of the Processing and the information available to Recurly, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, *provided that* Customer does not otherwise have access to the relevant information. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Recurly.

8.2 Recurly shall, taking into account the nature of the Processing and the information available to Recurly, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Recurly.

8.3 Recurly shall maintain records sufficient to demonstrate its compliance with its obligations under this Addendum. Customer shall, with reasonable notice to Recurly, have the right to review, audit and copy such records at Recurly's offices during regular business hours. Upon Customer's request, Recurly shall, no more than once per calendar year, either (i) make available for Customer's review copies of certifications or reports demonstrating Recurly's compliance with prevailing data security standards applicable to the Processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Customer or its authorized representative, upon reasonable notice and at a mutually agreeable date and time, to conduct an audit or inspection of Recurly's data security infrastructure and procedures that is sufficient to demonstrate Recurly's compliance with its obligations under this Addendum, provided that Customer shall provide reasonable prior notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Recurly's business. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Recurly for any time expended for on- site audits. If Customer and Recurly have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with this Section 8.3.

8.4 Recurly shall immediately notify Customer if an instruction, in Recurly's opinion, infringes the Data Protection Laws.

8.5 In the event of a Personal Data Breach, Recurly shall, without undue delay, inform Customer of the Personal Data Breach (including, to the extent available to Recurly, the information required by Article 33(3) of GDPR) and take such steps as Recurly in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Recurly's reasonable control).

8.6 In the event of a Personal Data Breach, Recurly shall, taking into account the nature of the Processing and the information available to Recurly, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.7 The obligations described in Sections 8.5 and 8.6 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Recurly's obligation to report or respond to a Personal Data Breach under Sections 8.5 and 8.6 will not be construed as an acknowledgement by Recurly of any fault or liability with respect to the Personal Data Breach.

9. Limitation of Liability. The total liability of each of Customer and Recurly (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this Addendum, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement.

10. Recurly's Role as a Data Controller. The parties acknowledge and agree that to the extent Recurly processes Personal Data in connection with the Agreement to: (i) monitor, prevent and detect fraud, and to prevent harm to Customer, Recurly and Recurly's affiliates, and to third parties; (ii) comply with legal or regulatory obligations applicable to the Processing and retention of Personal Data to which Recurly is subject; (iii) analyze, develop and improve Recurly's products and services; or (iv) provide Recurly products and services to Recurly users, Recurly is acting as a data controller with respect to the Processing of such Personal Data it receives from or through Customer. Customer agrees to disclose Recurly's privacy policy, available at https://recurly.com/legal/privacy, to any Data Subjects whose Personal Data could be Processed by Recurly as a data controller.

11. Execution of this Addendum. Recurly has pre-signed this Addendum, including the Standard Contractual Clauses (where applicable), in the signature blocks below. To complete this Addendum, Customer must: (i) complete the information requested in the signature block below and sign there and (ii) send the completed and signed Addendum to Recurly by email to compliance@recurly.com. Upon receipt of the validly completed Addendum by Recurly at this email address, this Addendum will become legally binding.

Customer	**Recurly, Inc.**
Signature:	Signature: Tony Allen Tony Allen (January 21, 2020)
Customer Legal Name:	Print Name: Tony Allen
Print Name:	Title: Chief Technology Officer
Title:	Date: July 24, 2020
Date:	

EXHIBIT A

Details of Processing

Nature and Purpose of Processing: Personal Data will be subject to those Processing activities which Recurly needs to perform in order to provide the Services pursuant to the Agreement. Personal Data will be Processed by Recurly for purposes of providing the Services set out into the Agreement.

Subject-matter: The subject-matter of Processing of Personal Data by Recurly is the provision of the Services.

Duration of Processing: Until deletion or return of Personal Data pursuant to the Agreement and this Addendum.

Categories of Data Subjects: Recurly may Process the Personal Data of Customer's employees, customers, and authorized users in connection with the Services.

Type of Personal Data:

- Name
- Company Name, VAT Number
- Phone Number
- Email
- Address
- IP Address
- Username
- Account Code (can include email addresses)
- Notes on an account, invoice or transaction
- Account Number Last Four
- Payment card details

EXHIBIT B

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:.....

Address:.....

Tel.: ..... ; fax:..... ; e-mail:.....

Other information needed to identify the organisation:

.....
(the data **exporter**)

And

Name of the data importing organisation: **RECURLY, Inc**., a company organized and existing under the laws of California, having its registered office at 400 Alabama St., Suite 202, San Francisco, CA 94110, United States of America

Tel.: (415) 651-3491 e-mail: privacy@recurly.com

Other information needed to identify the organisation:

.....
(the data **importer**)

each a "party"; together "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.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'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;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'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;

(d) *'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;

(e) '*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;

(f) *'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.

Clause 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.

Clause 3

Third-party beneficiary clause

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.

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. 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.

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.

Clause 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 services 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 services 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).

Clause 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,

  (ii) any accidental or unauthorised access, and

  (iii) 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 services 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.

Clause 6

Liability

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.

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.

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

3. 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.

Clause 7

Mediation and jurisdiction

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.

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.

Clause 8

Cooperation with supervisory authorities

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.

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.

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).

Clause 9

Governing Law

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

Clause 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.

Clause 11

Subprocessing

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.

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.

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.

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.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, 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.

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.....

(stamp of organisation)

On behalf of the data importer: Recurly Inc.
Name (written out in full): Tony Allen
Position: Chief Technology Officer

Address: 400 Alabama St., Suite 202, San Francisco, CA 94110
Other information necessary in order for the contract to be binding (if any):

Signature... *TonyAllen* .....

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Data exporter
The data exporter is Customer.

Data importer
The data importer is Recurly Inc., a provider of subscription billing management services.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

Data subjects are described in Exhibit A of the Addendum.

Categories of data
The personal data transferred concern the following categories of data (please specify):

Categories of personal data are described in Exhibit A of the Addendum.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

None.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

The processing activities described in Exhibit A of the Addendum.

DATA EXPORTER
Name:……

Authorised Signature ……

DATA IMPORTER
Name: Recurly Inc.

Authorised Signature ……*TonyAllen* ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

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):

The Data Importer has implemented and will maintain appropriate technical and organisational measures, internal controls and information security routines intended to protect Personal Data. The technical and organisational measures, internal controls and the information security standards including, SOC 2 Type II and PCI DSS which the data importer is audited against, are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Security Standards

Data Importer maintains and enforces various policies, standards and processes designed to secure Personal Data and other data to which Data Importer employees are provided access. Following is a description of some of the core technical and organizational security measures implemented by Data Importer.

This Appendix represents the minimum security measures that will be taken by Data Importer:

1. **Information Security Policies and Standards.** The Data Importer will implement security requirements for staff and all subcontractors, vendors or agents who have access to Personal Data that are designed to:

    - Prevent unauthorized persons from gaining access to Personal Data processing systems (physical access control);
    - Prevent Personal Data processing systems from being used without authorization (logical access control);
    - Ensure that persons entitled to use a Personal Data processing system gain access only to such Personal Data as they are entitled to access in accordance with their access rights and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control);
    - Ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control);
    - Ensure the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in or removed from Personal Data Processing (entry control);
    - Ensure that Personal Data are Processed solely in accordance with the Instructions of the Data Controller (control of instructions);
    - Ensure that Personal Data are protected against accidental destruction or loss (availability control); and
    - Ensure that Personal Data collected for different purposes can be processed separately (separation control).

2. Data Importer will conduct periodic risk assessments and review and, as appropriate, revise its information security practices at least annually or whenever there is a material change in Data Importer's business practices that may reasonably affect the security, confidentiality or integrity of Personal Data, provided that Data Importer will not modify its information security practices in a manner that will weaken or compromise the confidentiality, availability or integrity of Personal Data.

3. **Physical Security.** The Data Importer will maintain commercially reasonable security systems at all Data Importer sites at which an information system that uses or houses Personal Data is located. The Data Importer reasonably restricts access to such Personal Data appropriately.

4. **Organizational Security.**

- When media are to be disposed of or reused, procedures have been implemented to prevent any subsequent retrieval of any Personal Data stored on them before they are withdrawn from the inventory. When media are to leave the premises at which the files are located as a result of maintenance operations, procedures have been implemented to prevent undue retrieval of Personal Data stored on them.

- Data Importer will implement security policies and procedures to classify sensitive information assets, clarify security responsibilities and promote awareness for employees.

- All Security Incidents are managed in accordance with appropriate incident response procedures.

5. **Network Security.** The Data Importer maintains network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection and/or prevention systems, access control lists and routing protocols.

6. **Access Control.**

- Data Importer will maintain appropriate access controls, including, but not limited to, restricting access to Personal Data to the minimum number of Data Importer personnel who require such access.

- Only authorized staff can grant, modify or revoke access to an information system that uses or houses Personal Data.

- User administration procedures define user roles and their privileges, and how access is granted, changed and terminated; address appropriate segregation of duties and define the logging/monitoring requirements and mechanisms.

- All employees of the Data Importer are assigned unique User-IDs.

- Access rights are implemented adhering to the "least privilege" approach.

- Data Importer implements commercially reasonable physical and electronic security to create and protect passwords.

7. Data Importer will encrypt, using industry-standard encryption tools, all sensitive data that Data Importer: (i) transmits or sends wirelessly or across public networks; (ii) stores on laptops or storage media; and (iii) stores on portable devices, where technically feasible. Data Importer will safeguard the security and confidentiality of all encryption keys associated with encrypted Sensitive Information / Personal Data.

8. **Virus and Malware Controls.** The Data Importer installs and maintains anti-virus and malware protection software on the system to protect Personal Data from anticipated threats or hazards and protect against unauthorized access to or use of Personal Data.

9. Data Importer will require personnel to comply with its Information Security Program prior to providing personnel with access to Personal Data. The Data Importer implements a security awareness program to train personnel about their security obligations. This program includes training about data classification obligations; physical security controls; security practices and security incident reporting.

10. **Business Continuity.** The Data Importer implements appropriate disaster recovery and business continuity plans. Data Importer regularly reviews and updates its business continuity plan to ensure it is current and effective.

11. **Primary Security Manager.** Data Importer will notify Data Exporter of its designated primary security manager upon request. The security manager will be responsible for managing and coordinating the performance of Data Importer's obligations set forth in its Information Security Program and in this Contract.