



Email Privacy Seal Program Requirements

NOTICE: UNLESS SPECIFICALLY INDICATED OTHERWISE, THE FOLLOWING REQUIREMENTS APPLY TO BOTH ONLINE AND OFFLINE COLLECTIONS.

- I. Definitions: The following definitions shall apply herein:
- A. **Affiliate**: The term "Affiliate" means an entity that is not connected to the Participant by a common marketing brand, but is related to the Participant by corporate or organizational structure.
 - B. **Commercial or Promotional Email Message**: The term "Commercial or Promotional Email Message" means any electronic email message that is business-related or an endorsement and is sent by the Participant or on behalf of the Participant other than: (1) a Transactional or Relationship Email Message; or (2) a Personal Correspondence Email Message. Examples of Commercial or Promotional Email Messages include, but are not limited to, marketing messages, promotional messages, fundraising messages, newsletters, and surveys.
 - C. **Email Message**: The term "Email Message" means any email that is sent by the Participant or on behalf of the Participant.
 - D. **Personal Correspondence Email Message**: The term "Personal Correspondence Email Message" means an email that is sent in the normal course of running a business that meets the following criteria:
 - 1. The email is sent by a natural person who is clearly identified in the "from" line and message body;
 - 2. This person sends no more than 1,000 messages per day;
 - 3. Replying to the message sends a copy of the reply to the original person who sent the message;
 - 4. Reasonable measures are in place to ensure that requests from individual recipients to no longer be contacted are honored;
 - 5. Reasonable measures are in place to ensure that the email messages are targeted to the individual recipient;
 - 6. Email messages sent to one of the following role addresses cannot be considered Personal Correspondence Email Messages if they contain sales-related material, unless the address owner has publicized that the address should be sent such sales-related material. This requirement was adopted from commonly accepted Internet protocols established with RFC 2142 (<http://www.faqs.org/rfcs/rfc2142.html>).
 - a. root@domain
 - b. postmaster@domain
 - c. hostmaster@domain
 - d. abuse@domain



Email Privacy Seal Program Requirements

- e. ipadmin@domain
 - f. noc@domain
 - g. security@domain
 - h. webmaster@domain
- E. Privacy Statement: The term "Privacy Statement" shall mean the comprehensive statements of Participant's information practices posted on its Web Site(s), as such practices are updated from time to time.
- F. Recipient(s): The term "Recipient" means the individual who receives an Email Message covered by these Program Requirements.
- G. Related Personal Information: The term "Related Personal Information" means other personal information provided by the Recipient at the time of email address collection.
- H. Service Provider/Agent: The term "Service Provider/Agent" means a company that performs or assists in the performance of a function or activity involving the use or disclosure of email addresses and/or Related Personal Information on behalf of a Participant.
- I. Third Party: The term "Third Party" means a commercial entity that is unrelated by corporate structure to a Participant and that is not acting as the Participant's Service Provider/Agent.
- J. Third Party Personal Information: The term "Third Party Personal Information" means the e-mail address and Related Personal Information that is collected by Participant through the Site(s) from a person other than the person to whom it pertains or whom it identifies.
- K. Transactional or Relationship Email Message: The term "Transactional or Relationship Email Message" means any electronic mail message sent by the Participant or on behalf of the Participant, the primary purpose of which is:
- 1. to facilitate, complete, or confirm a commercial transaction that the Recipient has previously agreed to enter into with the Participant;
 - 2. to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the Recipient;
 - 3. to provide any of the following regarding a subscription, membership account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the Recipient of products or services offered by the Participant:
 - a. notification concerning a change in the terms;
 - b. notification of a change in the recipient's standing or status; or
 - c. at regular periodic intervals, account balance information or other type of account statement.



Email Privacy Seal Program Requirements

4. to provide information directly related to an employment relationship or related benefit plan in which the Recipient is currently involved, participating, or enrolled; or
5. to deliver goods or services, including product updates or upgrades, that the Recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the Participant.

II. TRUSTe's Responsibilities

- A. Client Services Manager. TRUSTe agrees to name a Client Services Manager for Participant within fifteen (15) business days of the Effective Date of this Agreement, as long as Participant's disclosures concerning its Email Practices (contained in its privacy statement), Participant's Self Assessment, and Participant's Point of Collection Disclosures have been completed, by providing written or electronic notice to Participant. All notices between TRUSTe and Participant shall be directed to the designated Online PoC Page(s) Coordinator and designated TRUSTe Client Services Manager, which either party may change upon written or electronic notice to the other.
- B. TRUSTe Email Privacy Mark. Upon certification, TRUSTe will provide Participant with:
 1. the TRUSTe Email Privacy Mark indicated in Exhibit A; and
 2. a Participant Verification Page located on TRUSTe's secure server.
- C. TRUSTe Compliance Assessment, Monitoring and Complaint Resolution Procedures. TRUSTe will, itself or through an independent, qualified, neutral third party designated by TRUSTe, review Participant's Email Disclosures and the Online PoC Page(s), at times determined by TRUSTe in its discretion, throughout the term of this Agreement, to assess: (i) the consistency and quality of Participant's Email Disclosures and Participant's related Email Practices, (ii) the Participant's conformance with these Program Requirements, and (iii) the consistency and quality of Participant's use of the TRUSTe Email Privacy Mark on the Online PoC Page(s). Compliance procedures will include the following:
 1. **Assessment**. After a Participant has completed a formal application to become a TRUSTe Participant but before being granted the TRUSTe Email Privacy Mark, TRUSTe will independently review the Participant's Email Disclosures and Participant's Self Assessment for consistency with these Program Requirements.
 2. **Online Community Monitoring**. TRUSTe will investigate non-frivolous complaints of Participant's violations of its Email Disclosures or other specific privacy concerns that are received from consumers through TRUSTe's Online Watchdog Dispute Resolution Program. TRUSTe will respond to all such complaints within ten (10) business days of receipt through the TRUSTe Online Watchdog Dispute Resolution Program.



Email Privacy Seal Program Requirements

3. Ongoing TRUSTe Monitoring. TRUSTe will conduct ongoing monitoring of Participant's Online PoC Page(s) and Site(s), including but not limited to the use of seeding and unannounced Site(s) reviews.
 4. Escalated Investigations. If TRUSTe has reason to believe that Participant has violated its Email Disclosures or any of these Program Requirements, TRUSTe may conduct an escalated investigation, which may include an on-site compliance review. Participant shall pay for the reasonable costs of any such review as required by Section III.N.7 and shall promptly rectify the practice to TRUSTe's satisfaction.
 5. Recommendations/Remedies. If TRUSTe, after any investigation or complaint pursuant to this Section II.C., finds any violations of Participant's Email Disclosures or of these Program Requirements, TRUSTe will recommend that Participant take corrective action as required by Section III.L.
- D. Amendments. TRUSTe will review Participant's proposed Material Changes to its approved Email Disclosures, after Participant notifies TRUSTe of such change pursuant to Section III.L. herein.
- E. Correspondence. TRUSTe may from time to time provide Participant with newsletters, information regarding legal changes to this Agreement, information regarding updates to the TRUSTe Email Privacy Program, and other relevant information regarding current privacy issues.

III. Participant's Responsibilities

- A. In addition to payment of the required Fees, Participant shall submit the following Participant Program Materials as part of the application:
1. Two signed originals of the TRUSTe Email Privacy Seal Program Amendment;
 2. One signed Self-Assessment; and
 3. Its current Email Disclosures, covering all Program Requirements in this Exhibit B.
- B. Self Assessment. Participant shall provide the Self Assessment with the understanding and expectation that TRUSTe may rely on the statements contained therein for the purpose of determining Participant's practices and Participant's qualification for the TRUSTe Email Privacy Seal Program. After diligent inquiry and in good faith, an authorized representative of Participant shall sign and attest that the statements made on the Self Assessment are true and accurate as of the date submitted and shall remain true and accurate for the term of this Program Amendment, unless Participant's Email Practices and Email Disclosures are modified pursuant to Section III.L. of these Program Requirements.

Participant will be required to submit a new partial or full Self Assessment, as determined by TRUSTe, in the following circumstances: (i) there has been any Material Change in Participant's Email Disclosures or Email Practices; (ii) there has



Email Privacy Seal Program Requirements

been an assignment by Participant in compliance with the terms of Section 11(b) of the Agreement; (iii) it has been three (3) years since Participant's last full Self Assessment; or (iv) there has been an investigation pursuant to Section III.R of these Program Requirements.

- C. **Recertification.** Participant must seek recertification by TRUSTe annually, and comply with the following requirements in order for recertification to be effective:
1. Participant must execute an addendum to the Email Privacy Seal Program Amendment, in a form as provided by TRUSTe ("Addendum"), which shall:
 - a. Contain a representation and warranty that Participant has either (i) made no Material Changes to its Email Practices or Email Disclosures, as such Email Practices or Email Disclosures have been previously approved by TRUSTe, or (ii) made no Material Changes to its Email Practices or Email Disclosures, as such Email Practices or Email Disclosures have been previously approved by TRUSTe, except those submitted with Participant's request for recertification;
 - b. Contain a representation and warranty that the authorized representative signing the Addendum has reviewed the Participant's current Self Assessment; and
 - c. Be signed by an authorized representative of Participant.
 2. If Participant proposes to make any Material Changes to its Email Disclosures or Email Practices, such Material Changes must be submitted with the Addendum, for review and approval by TRUSTe in its sole discretion. TRUSTe may require that Participant take certain corrective measures in order for recertification to be effective.
 3. If the Program Requirements in effect at the time of recertification differ from those integrated into Participant's Email Privacy Seal Program Amendment, Participant must accept the new Program Requirements as part of the Addendum. In addition, Participant must provide responses to any Self Assessment questions that are required by TRUSTe that are related to any changes in the Program Requirements.
 4. Notwithstanding any other terms of this Section III.C., a new, full Self Assessment will be required of Participant no less than every three (3) years.
- D. **Required Disclosures.**
1. **Privacy Statement.** Participant shall maintain and abide by a Privacy Statement in the English language that is written by Participant that states Participant's Email Practices and is in conformance with this Program Amendment. The Privacy Statement must be linked only to and from Web pages that are in the English language. At a minimum, Participant's Privacy Statement shall disclose to users its Email Practices, including each of the following:



Email Privacy Seal Program Requirements

- a. A full description of how users can contact Participant, as required in Sections III.E. (“Choice”), III.J. (“Access”), and III.M. (“Recipient Complaints”);
 - b. The fact that Participant collects users’ email addresses;
 - c. The identity (including name, address and e-mail address) of the organization(s), other than a Service Provider/Agent of Participant, that collects users’ email addresses through Online PoC Page(s);
 - d. Where applicable, a statement that Participant obtains email addresses from a third party;
 - e. How email addresses collected (from any source) are used;
 - f. With whom Participant shares users’ email addresses if at all (including any service provider/agent agreements);
 - g. What tracking technologies, if any, are used on Online PoC Page(s) or in email by either the Participant or a third party;
 - h. How and when a Recipient may exercise Choice, as required in Section III.E;
 - i. How Access is provided, as required in Section III.J.;
 - j. That security measures are in place, as required in Section III.K.;
 - k. The notification procedures with respect to a Material Change in Participant’s Email Practices, as required in Section III.L; and
 - l. The effective date of the Privacy Statement.
2. Point of Collection Disclosures. Participants must ensure that the following is clearly and conspicuously disclosed at every point of collection, whether online or offline, of email addresses and Related Personal Information (for Online PoC Pages, a link to a privacy statement is mandatory but insufficient):
- a. The nature of Commercial or Promotional Email Messages to be sent and the types of entities that will be providing content;
 - b. The nature of Personal Correspondence Email Messages and/or Transactional or Relationship Email Messages to be sent by Participant;
 - c. Whether Participant sells, rents or otherwise shares Recipients’ email addresses and/or Related Personal Information, with third parties other than Service Providers/Agents; and
 - d. If receiving Commercial or Promotional Email Messages is a requirement to receive a service, a disclosure of such requirement.



Email Privacy Seal Program Requirements

- E. Choice. Participants must ensure that consent with clear and conspicuous disclosure or a prior business relationship exists prior to sending Commercial or Promotional Email Messages.
1. Acceptable forms of consent for Participant to email Commercial or Promotional messages from the Participant:
 - a. Double Opt-In: (sometimes referred to as “Confirmed Opt-In”): The Recipient affirmatively requests in writing, online or offline, to add his/her email address to a mailing list. The Recipient receives a confirmation email and the Recipient confirms his/her request by replying or visiting a provided URL. In the event that Recipient does not respond to the confirmation email, Participant may send a reminder email once, asking Recipient to respond.
 - b. Opt-In with Verification: The Recipient affirmatively requests in writing, online or offline, to add his/her email address to a mailing list. The Recipient receives a verification email notifying him/her of the subscription and providing clear unsubscribe instructions.
 - c. Opt-In: The Recipient affirmatively requests in writing, online or offline, to add his/her email address to a mailing list.
 - d. Pre-Selected Option with Verification: The Recipient consents in writing to have his/her email address added to a mailing list by leaving a clear and conspicuous pre-selected option intact. The Recipient receives a verification email notifying him/her of the subscription and providing clear unsubscribe instructions. Commercial or Promotional Email Messages sent under this form of consent must include clear and conspicuous identification that the message is an advertisement or solicitation.
 - e. Pre-Selected Option: The Recipient consents in writing to have his/her email address added to a mailing list by leaving a clear and conspicuous pre-selected option intact. Commercial or Promotional Email Messages sent under this form of consent must include clear and conspicuous identification that the message is an advertisement or solicitation.
 2. Third Party Sharing: Acceptable forms of consent for Participant to share, rent, or sell email addresses pursuant to Sub-sections III.E. 5 and 6 herein with an Affiliate or Third Party that is not acting as a Participant’s Service Provider/Agent:
 - a. Double Opt-In: (sometimes referred to as “Confirmed Opt-In”): The Recipient affirmatively requests in writing, online or offline, to add his/her email address to a mailing list. The Recipient receives a confirmation email and the Recipient confirms his/her request by replying or visiting a provided URL. In the event that Recipient does not respond to the confirmation email, Participant may send a reminder email once, asking Recipient to respond.



Email Privacy Seal Program Requirements

- b. Opt-In with Verification: The Recipient affirmatively requests in writing, online or offline, to add his/her email address to a mailing list. The Recipient receives a verification email notifying him/her of the subscription and providing clear unsubscribe instructions.
 - c. Opt-In: The Recipient affirmatively requests in writing, online or offline, to add his/her email address to a mailing list.
 3. Use of Related Personal Information and/or Third Party Personal Information. Participant shall:
 - a. Opt-In choice must be given before such information may be used, disclosed or distributed for any purpose other than the primary purpose for which such information was collected.
 - b. Notwithstanding (a), Participant may use Third Party Personal Information to send a one-time e-mail message to the person to whom the Information pertains to solicit her Opt-In consent.
 4. A prior business relationship exists where: (1) the Recipient has purchased a product or service from the Participant within the past eighteen (18) months, (2) the Recipient consensually provided his/her email address, and (3) the Recipient has not unsubscribed or opted out from Commercial or Promotional Email Messages, or otherwise terminated the relationship. An Affiliate or Third Party may not rely on a prior business relationship for sending Commercial or Promotional Email Messages.
 5. If Participant has not collected the Recipient's email address and/or Related Personal Information directly, the Participant must perform due diligence to ensure that clear and conspicuous notice was provided, and relevant consent obtained, as required herein.
 6. Exception to Consent Requirement for Peer-Initiated Commercial or Promotional Email Messages

Participants that send Peer-Initiated Commercial or Promotional Email Messages must employ either the Double Opt-in, Opt-In with Verification, or Opt-In methods for obtaining consent in subsections 1(a)-(c) of this section E, in order to obtain an individual's consent for Commercial or Promotional Email Messages other than the Peer-Initiated Commercial or Promotional Email Message. The pre-Selected Option with Verification and Pre-Selected Option consent methods in subsections 1(d)-(e) of this section E are not permitted in the case of Peer-Initiated Commercial or Promotional Email Messages.

If the individual to whose email address the Participating Sender has sent a Peer-Initiated Commercial or Promotional Email Message does not respond, the Participant may send one follow-up Email Message soliciting that individual's consent for additional Commercial or Promotional Email Messages from the Participant. If the individual to whom this follow-up



Email Privacy Seal Program Requirements

- message is sent does not respond, the Participant may not send any additional Email Messages to him or her.
7. Rental or sharing of Email addresses from or to Third Parties or Affiliates may occur only on a temporary basis, and provided that consent has been obtained pursuant to Section III.E.2 and further provided that the emails sent are relevant to the consent obtained.
 8. Co-registration: Email addresses may only be purchased from a Third Party or sold to a Third Party through a co-registration process subject to the restrictions listed below. The following requirements must be met to be considered a co-registration:
 - a. The purchaser of the email addresses was explicitly, clearly, and conspicuously named at the point of email address collection;
 - b. Each act of consent pursuant to Section III.E.2 resulted in the addition of an email address to only one list; and
 - c. Proof of consent, including the date, time, originating IP address, and location (e.g., a URL) where the address collection occurred can be produced by the Participant upon request.
 9. A Participant may not send Email Messages to email addresses that have been obtained by harvesting or dictionary-style attacks.
- F. Unsubscribe. Participants must ensure that the Recipient's requests to discontinue receipt of Commercial or Promotional Email Messages are honored.
1. Every Commercial or Promotional Email Message sent under these Program Requirements must include an Unsubscribe option. Removal instructions must be clear, conspicuous, and easily understood. This should be as close to a "one-click" process (such as selecting a URL) as possible.
 2. All unsubscribe mechanisms must adhere to the following:
 - a. Easy to Use: Unsubscribe mechanisms may include a reply to the Commercial or Promotional Email Message sent to the Recipient or an online process described in that Commercial or Promotional Email Message with a URL. The Unsubscribe process must not require a Recipient to provide any information other than the Recipient's email address, unless the Recipient has been clearly and conspicuously notified at the point of collection that receiving Commercial or Promotional Email Messages is a requirement to receive a service, in which case a username and/or password may be required.
 - b. Timely: A Recipient's request to unsubscribe must be processed, and the request must become effective within ten (10) business days from receipt.
 - c. Persistent: Unsubscribe mechanisms must be functional for no fewer than thirty (30) days following the sending of the Commercial or Promotional Email Message.



Email Privacy Seal Program Requirements

- d. Indefinite: A Recipient's request to unsubscribe is valid and must be honored indefinitely, or until the Recipient provides his or her new consent, as defined in these Program Requirements, to receive Commercial or Promotional Email Messages.
 - e. Absolute: Once a Recipient has unsubscribed, Commercial or Promotional Email Messages may not be sent to the Recipient and the Recipient's email address or Related Personal Information may not be sold, leased, or otherwise shared with Third Parties or Affiliates. This requirement applies to all unsubscribes, including email addresses that have been unsubscribed from Participant but which Participant happens to obtain separately pursuant to Sub-section III.E.4 herein. If, for example, a Participant purchases, rents or otherwise obtains a list of email addresses from a Third Party, it must scrub that list against its own list of unsubscribed email addresses before sending Commercial or Promotional Email Messages to email addresses on the third-party list.
 - f. Flexible: If a Recipient contacts the Participant with an "Out of Band Request" for an unsubscribe, for example, via postal mail, email to another account at the Participant (e.g., abuse@sender.domain or postmaster@sender.domain), or through a telephone call, those unsubscribe requests should be acted on in a timely manner.
3. In cases where a Recipient is clearly and conspicuously notified at the point of collection that receiving Commercial or Promotional Email Messages is a requirement to receive a service, the Unsubscribe option may be provided through a link in every Commercial or Promotional Email Message to a more general account administration tool (for example, "account settings" or "account preferences"), and may require a login at a specified web page.
- G. Participant Accountability. Participant shall ensure that the mail infrastructure used to send Email Messages is well maintained and operated in a responsible manner:
1. Email address list maintenance systems must be employed to reliably receive and process bounces and other replies from receiving networks. Permanent delivery errors from Email Messages sent by the Participant must be processed by removing the Recipient's email address and must not exceed 10% of all messages sent by Participant.
 2. The Participant's IP address(es) for outgoing email must have valid reverse DNS entries. The IP address of the host name of the reverse DNS entry must match the IP address of the sending mail server.
 3. Participant must create and maintain the standard role email accounts abuse@sender.domain and postmaster@sender.domain for all of its domains that send email in order to facilitate handling complaints and other issues.
 4. Participant must register with abuse.net, and maintain accurate contact information in the whois database.



Email Privacy Seal Program Requirements

5. Participant must be in compliance with Network Working Group Request for Comment (“RFC”) Nos. 2821 and 2822, which describe how Email Messages must be formatted in order to be processed properly by receiving networks.
- H. Transparency. Participant shall ensure that Email Messages are truthful and accurately identify the source of the message.
 1. The domain name or message headers must not be falsified or obscured in any way.
 2. The subject line and content of every Email Message must not be false or misleading.
- I. Data Quality. Participant shall take reasonable steps when collecting, creating, maintaining, using, disclosing or distributing email addresses and Related Personal Information, to assure that the data are accurate, complete and timely for the purposes for which they are to be used.
- J. Access. Participant shall implement reasonable and appropriate processes or mechanisms to allow Recipients to correct material inaccuracies in email addresses and Related Personal Information, such as account or contact information. These processes or mechanisms must be simple and easy to use, and shall confirm to Recipients that inaccuracies have been corrected.
- K. Security. Participants shall provide reasonable security for networks used to send Email Messages and store Recipient information:
 1. Participants shall provide commercially reasonable measures to protect the security and integrity of any Recipients’ email addresses and Related Personal Information held in databases or on electronic systems; and
 2. Commercially reasonable efforts shall be made to prevent open proxies, open relays and the dissemination of computer viruses, worms, or trojans on the Participant’s network and any IP addresses over which Email Messages are sent by Participant.
- L. Material Changes.
 1. Participant must obtain prior approval from TRUSTe for any Material Change to its Email Practices, which must be reflected in its Email Disclosures. If Participant makes any such Material Change, it may be subject to a revision fee to compensate TRUSTe for its costs of processing the revisions. Any such Material Change may require a new partial or full Self Assessment, in TRUSTe’s sole discretion.
 2. Material Changes involving Recipients’ Choices regarding the collection, use, disclosure and/or sharing of email addresses and/or Related Personal Information shall have effect only after the Recipient has given Opt-In consent. A Material Change may not be applied to previously-collected data without such Opt-In consent. Recipients must be provided Opt-In Choice for such changes pursuant only to Sub-sections III.E. 1(a)–(c) herein.



Email Privacy Seal Program Requirements

3. Participant shall notify users of any Material Change in its Email Practices. To do so, Participant must: (a) send an administrative e-mail to all users affected by the Material Change fourteen (14) calendar days prior to the implementation of the Material Change; and (b) post prominent notices on Online PoC Page(s) for the fourteen (14) calendar days prior to the implementation of the Material Change. Both the email and the notice shall contain a description of how users may exercise Choice pursuant to Section III.E. herein.
 4. TRUSTe must approve all such notification of Material Changes to Participant's Email Practices and its Email Disclosures.
- M. Recipient Complaints. Participant shall provide Recipients with reasonable, appropriate, simple and effective means to submit complaints and express concerns regarding Participant's Email Practices and Email Disclosures. Participant shall respond to all such submissions in a timely fashion, not to exceed ten (10) business days. Participant shall also cooperate with TRUSTe's efforts to resolve user complaints, questions and concerns.
- N. Translation Into Other Languages. If Participant wishes to translate into other languages and post its disclosures concerning its Email Practices (contained in its privacy statement), and its Point of Collection Disclosures, that TRUSTe has approved in English, it shall contact TRUSTe to arrange for an appropriate addendum to this Agreement.
- O. Location of TRUSTe Email Privacy Mark and link to verification page; link to Privacy Statement.
1. Participant must post the TRUSTe Email Privacy Mark clearly and conspicuously on every Online PoC Page (i.e., every web page where Participant collects email addresses and Related Personal Information) and in close proximity to the fields used to enter email addresses and/or Related Personal Information on such Page(s). The Verification Mark must link to Participant's Verification Page located on TRUSTe's secure server at the TRUSTe Web site. The verification page will confirm Participant's participation in the TRUSTe Email Privacy Program and will include a link to the TRUSTe Watchdog complaint page on the TRUSTe Web site.
 2. Participant must link every such page to the privacy statement containing disclosures concerning its Email Practices by means of a hypertext link or button with the phrase "Privacy Statement" or its reasonable equivalent.
 3. Participant must provide TRUSTe with the URL(s) of the TRUSTe Email Privacy Mark. If Participant changes the URL(s) of the TRUSTe Email Privacy Mark, it must provide TRUSTe two (2) business days' prior written or electronic notice of the change.
- P. Acceptance Of Recommended Changes. Participant must take within twenty (20) business days such corrective action recommended by TRUSTe pursuant to Section II.C. of this Exhibit B. If Participant does not take such corrective action, TRUSTe may: (i) terminate for cause this Program Amendment or this Agreement as provided



Email Privacy Seal Program Requirements

in Section 5(d) of this Agreement, and/or (ii) refer Participant to the Federal Trade Commission or other appropriate government enforcement agency, and may report such disciplinary action publicly on its Web site, including Participant's name, the nature of the violation (including a reference to the Section of this Exhibit B found to have been violated), and TRUSTe's resulting action.

- Q. Notice To TRUSTe Of Certain Events. Participant shall notify TRUSTe in writing, at the same time that such information becomes publicly known, or within ten (10) business days of the event, whichever is sooner, of:
1. a change in Participant's name (other than an assignment); or
 2. a change of URL's for one or more of the Online PoC Page(s); or
 3. a change in the brand seen by Recipients.
- R. Cooperation With TRUSTe. To enable TRUSTe to meet its responsibilities above, Participant agrees to:
1. Cooperate with TRUSTe to ensure compliance with these Program Requirements and Participant's Email Disclosures.
 2. Provide, at no charge to TRUSTe or its representatives, full access to Participant's Web site (i.e., including password access to premium or members only areas) for the purpose of conducting reviews to ensure that Participant's Email Disclosures are consistent with actual practices.
 3. Provide, upon TRUSTe's reasonable request, information regarding how email addresses and/or Related Personal Information gathered from Participant's Site(s) is used.
 4. Acknowledge the receipt of all TRUSTe inquiries that request acknowledgment within five (5) business days after receipt and provide a reasonable estimate of when the inquiry shall be addressed.
 5. Respond within a maximum of ten (10) business days to all TRUSTe inquiries about Participant's implementation of the TRUSTe Email Privacy Program at Online PoC Page(s) and inquiries about Participant's potential breach of this Agreement. Participant may request from TRUSTe an additional twenty (20) business days to respond if circumstances warrant, and consent to such additional time shall not be unreasonably withheld.
 6. Participate in TRUSTe's Watchdog process to resolve non-frivolous, as determined by TRUSTe, privacy concerns or complaints. If Participant does not respond directly to consumer concerns or complaints in a satisfactory and timely fashion, TRUSTe will act as the liaison between the Participant and the consumer to resolve the issue, including recommending any necessary corrective action.
 7. Be subject to an onsite compliance review in response to non-frivolous complaints, as determined by TRUSTe, or any findings by TRUSTe that Participant: (a) has failed to implement and adhere to the policies set forth in



Email Privacy Seal Program Requirements

Participant's Email Disclosures; or (b) has failed to adhere to these Program Requirements.

- a. TRUSTe shall provide, at a minimum, ten (10) business days' written notice to Participant prior to initiation of an on-site compliance review and shall perform its review during Participant's normal business hours and at a time agreeable to Participant.
- b. It is TRUSTe's intent that the portion of such on-site reviews requiring TRUSTe or an independent party designated by TRUSTe to be physically at Participant's facility will be completed within two (2) business days and shall not exceed five (5) business days as long as Participant cooperates and no unusual circumstances cause additional time to be reasonably necessary.
- c. TRUSTe shall use its reasonable effort to accommodate Participant's schedule and shall perform its review in such a manner as not to interfere unreasonably with Participant's operations.
- d. Participant agrees to bear the reasonable cost of up to three (3) such reviews in a one (1) year period and promptly rectify the practice to TRUSTe's reasonable satisfaction.