



May 23, 2014

Secretary Ted Dean, Deputy Assistant Secretary for Services,
Krysten Jenci, Director, Office of Digital Services Industries
Christopher Hoff, Vice Chair, APEC Data Privacy Subgroup
Office of Technology and Electronic Commerce
International Trade Administration
U.S. Department of Commerce
1401 Constitution Ave. NW
Room 4324
Washington, DC 20230

Janis Kestenbaum
Peder McGee,
Shaundra Watson
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

By Email

Re: Submission of APEC Accountability Agent Renewal Application

TRUSTe appreciates the opportunity to renew its application to be an APEC recognized Accountability Agent under the APEC Cross Border Privacy Rules (CBPR) System.

As a US-based for profit entity, TRUSTe is subject to the regulatory oversight and enforcement authority of the United States Federal Trade Commission (FTC), which is recognized as the APEC regulatory enforcement authority in the United States.

In order to continue its role and be recognized as an APEC Accountability Agent, TRUSTe has outlined how it continues to meet the Accountability Agent Recognition Criteria outlined in Annex A utilizing the Accountability Agent Recognition Criteria Checklist provided in Annex B.

Responses to the questions in the Accountability Agent Recognition Criteria Checklist (Annex B) are provided below in the following sections:

- Conflicts of Interest
- Program Requirements
- Certification Process



TRUSTe Confidential - APEC Renewal Application 2014
Page 2 of 18

- On-going Monitoring and Compliance Review Process
- Re-Certification and Annual Attestation
- Dispute Resolution Process
- Mechanism for Enforcing Program Requirements

Documentation to support the answers to the questions in Annex B is provided as appendices that are listed at the end of this document.

Also included in this reapplication packet is Annex C demonstrating how TRUSTe's current intake process continues to meet the baseline established by the CBPR's, and Annex F including application signature and contact information sheet.

Please accept this packet as TRUSTe's reapplication to continue its role as a recognized accountability agent under the CBPR system. For questions regarding this renewal application, please contact Saira Nayak, Director of Policy, at snayak@truste.com.

Sincerely,

Tim Sullivan
CFO



Annex B

Accountability Agent Recognition Criteria Checklist

Conflicts of Interest

- 1. Applicant Accountability Agent should describe how requirements 1(a) and (b) in Annex A have been met and submit all applicable written policies and documentation.*

1. Conflict of Interest Policy

TRUSTe provides pre-certification (assessment), certification and consulting services to clients. Often, our consulting engagements involve the review of privacy practices that are not specifically addressed by a TRUSTe certification program. e.g. EU-US HR data transfers. Under the requirements set out in section 1. paragraphs 5-14 of the APEC Accountability Agent Recognition Criteria, we interpret the term “consulting and technical services,” as exempting all services provided under an assessment or certification to standards other than APEC-CBPR. Under this definition, TRUSTe has had no consulting or technical engagements with companies we certify under our APEC Privacy Program. In the future, if we decide to enter into consulting and/or technical service engagements with our APEC certified clients, we will inform the JOP of the existence of these engagements and the internal safeguards in place to address any potential conflicts of interest.

These internal safeguards include documented internal policies to avoid potential conflicts of interest between our consulting and certification activities. For details, please see TRUSTe’s Certification and Service Delivery conflict of interest policies, attached as Appendix H to this application. These policies were revised most recently on May 1, 2014. Both our Global Privacy Solutions staff (that perform certifications) and our consulting staff (that perform consulting engagements) have been trained on these conflict of interest policies.

Some of the specific ways we have addressed potential conflicts of interest between our consulting and certification activities are as follows:

- TRUSTe consulting services are primarily supervised and provided by a member of the Legal or Product department staff, as opposed to Global Privacy Solutions staff.
- In cases where pre-certification and/or certification is part of the Service Delivery engagement, Global Privacy Solutions staff will assist Legal and/or Product department staff in their review. However, in no case,



will a Global Privacy Solutions staff work on both a consulting engagement and a certification engagement for the same client.

We know that the integrity of the TRUSTe seal and certification process is critical to maintaining the value of the TRUSTe brand - and its good standing with consumers, regulators and other stakeholders. This is why TRUSTe has documented internal policies to avoid potential conflicts of interest between its consulting and certification activities.

2. Trademark and Section 5 Obligations

In addition to the importance we place on certification in terms of brand value, we would also note that, under US trademark law, TRUSTe is required to apply its certification standards in an impartial manner. Any application of the certification process that is not impartial places the credibility of TRUSTe's certification business at risk. It may also lay the grounds for a Section 5 claim by the FTC, TRUSTe's privacy enforcement authority under the APEC-CBPR framework.

For all of the reasons, and as documented in the attachments referenced above, TRUSTe believes that it continues to meet the requirements outlined in sections 1 (a) and (b) of Annex A to the APEC Accountability Agent Recognition Criteria.

- 2. Applicant Accountability Agent should submit an overview of the internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in 2(b) of Annex A*

Please reference Appendix H to this application for copies of TRUSTe's internal conflict of interest policies, as well as our response to question 1. above.

In addition, as an entity doing business in California, TRUSTe is subject to California law, which requires that all employees owe a duty of loyalty to their employer. As a result, no employee of TRUSTe, including officers, can be employed by any other entity, whether that entity is a licensee of TRUSTe or not.

Directors of TRUSTe are also subject to several legal requirements.

Non-executive Directors do not have day-to-day operational responsibilities. In point of fact, corporate governance requirements in the United States



significantly restrict a Director's ability to influence day-to-day management of the corporation.

Finally, Article 9 of TRUSTe's Articles of Incorporation imposes penalties on any Director that violates his/her duty of loyalty to the corporation. Based on this fundamental fiduciary duty, directors of TRUSTe will recuse themselves from voting on any matter which can give rise to conflict of interest as contemplated by section 2(b) of the APEC Accountability Agent Recognition Criteria. This includes a potential conflict of interest in a commercial transaction normally classified as an "insider transaction."

3. Applicant Accountability Agent should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.

Please reference Appendix H to this application for copies of TRUSTe's internal conflict of interest policies, as well as our response to questions 1. and 2. above.

In addition, where a Director identifies a conflict of interest, that Director shall either 1) recuse themselves in the event that the conflict of interest arises from a relationship that Director has, or (2) require that the Director with the conflict of interest to recuse themselves. This is a fundamental requirement of the fiduciary duty inherent in the membership of TRUSTe's Board of Directors.

Program Requirements

4. *Applicant Accountability Agent should indicate whether it intends to use the relevant template documentation developed by APEC or make use of Annex C to map its existing intake procedures program requirements.*

TRUSTe meets this requirement and has used Annex C to map its current APEC Privacy Program Requirements¹ to the Assessment Criteria. Please see the APEC Cross-Border Privacy Rules System Program Requirements Map (Annex C) for additional detail.

Certification Process

5. *Applicant Accountability Agent should submit a description of how the requirements as identified in 5 (a) – (d) of Annex A have been met.*

¹ APEC Privacy Program Requirements are posted on TRUSTe's website at <http://www.truste.com/privacy-program-requirements/apec>



TRUSTe meets these requirements. TRUSTe has an existing, comprehensive process in place to review a program applicant organization's policies and practices with respect to the program applicant participation in the Cross Border Privacy Rules System and to verify its compliance with the Accountability Agent's Program Requirements.

Overall, TRUSTe uses a combination of three different methodologies to conduct the privacy certification review: a manual evaluation of the program applicant's practices, the program applicant's own attestations provided during the interview and through responses to the APEC CBPR System Intake Questionnaire² and interviews, and monitoring through TRUSTe's proprietary technology and tools. The extent to which we use one methodology over another is dependent on a program applicant's risk profile. We examine how the program applicant collects, uses and shares personal data; we also identify the program applicant's third party, data-sharing relationships.

To meet the requirements as identified in 5 (a)-(d) of Annex A, the TRUSTe certification process involves five steps: analyze, advise, remedy, award and monitor.

- a) *Analyze*: TRUSTe performs the initial assessment of compliance.³
- b) *Advise*: TRUSTe provides a comprehensive report to the program applicant outlining our findings regarding compliance with TRUSTe's APEC Privacy Program Requirements.⁴
- c) *Remedy*: TRUSTe verifies that the required changes provided in the comprehensive report have been properly implemented.
- d) *Award*: TRUSTe has certified that the program applicant is in compliance with the APEC Privacy Program Requirements.
- e) *Monitor*: TRUSTe verifies ongoing compliance with Program Requirements.

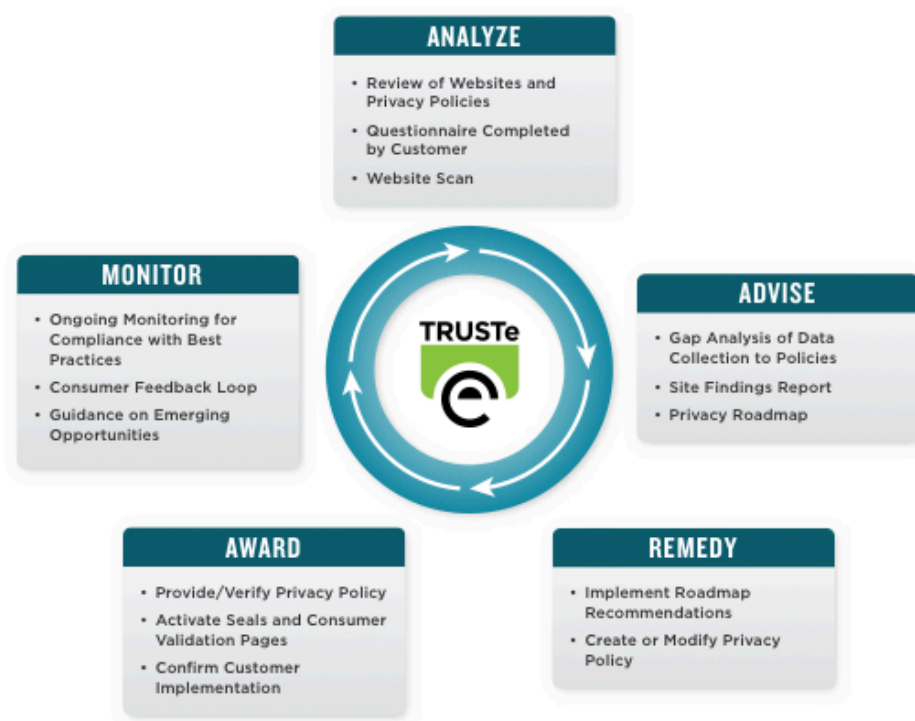
² APEC CBPR System Intake Questionnaire: http://apec.org/Groups/Committee-on-Trade-and-Investment/~/_media/Files/Groups/ECSG/CBPR/CBPR-Intake-Questionnaire.ashx

³ Appendix E is an example of TRUSTe's APEC Privacy program applicant interview form used during the Analyze portion of the certification process.

⁴ Appendix F is an example of TRUSTe's APEC Privacy findings report used during the Advise portion of the certification process.



The diagram below illustrates the specifics of this approach:



For additional details on our certification process, please refer to our 2013 TRUSTe Transparency Report, which is included as Appendix C to this application.

On-going Monitoring and Compliance Review Processes



6. *Applicant Accountability Agent should submit a description of the written procedures to ensure the integrity of the certification process and to monitor the participant's compliance with the program requirements described in 5 (a)-(d).*

TRUSTe meets this requirement and has included a description of our written procedures to ensure the integrity of the certification process and to monitor the Participant⁵'s compliance with the Program Requirements as described in 5(a)-(d). Once a Participant completes the initial certification process as defined in requirements 5 (a)-(d), TRUSTe uses a combination of approaches to ensure that compliance with TRUSTe's APEC Privacy Program Requirements is consistently and continually maintained. Unlike an audit - which only captures compliance at a single point in time - TRUSTe certification involves ongoing monitoring using a combination of inquiries/reviews and technological tools. These tools include:

- *Web crawling:* Proprietary TRUSTe technology that verifies the existence of key website elements (e.g. a privacy policy at the point of PII collection), and website processes (e.g. the transmission of credit cards and other sensitive information over an encrypted connection). TRUSTe's web crawler also performs intensive website analysis for data collection and ad targeting processes, and in conjunction with other techniques serves as TRUSTe's technological accountability platform for monitoring Participants.
- *E-mail seeding:* A process by which compliance is monitored using unique e-mail addresses that do not reference TRUSTe, to check for e-mail sent by an unauthorized party, or after an unsubscribe request has been processed.⁶
- *Traffic analysis:* A network packet monitoring process primarily used to verify compliance for TRUSTe's mobile privacy and Trusted Download certifications.
- *Dispute resolution process:* Defined in detail in the TRUSTe Transparency Report: 2013 (Appendix C) and online Dispute Resolution Form (Appendix B).

⁵ "Participant" means the entity that has entered into an agreement with TRUSTe to participate in the TRUSTe program(s) and agreed to comply with the program requirements included therein

⁶ TRUSTe's e-mail seeding process has had notable successes in cases where the Participant was not initially aware of an unsubscribe malfunction or data leakage (through a service provider, for example). In such cases, TRUSTe's e-mail seeding report has alerted Participants to the issue, and supported TRUSTe's recommendations for issue resolution.



7. Applicant Accountability Agent should describe the review process to be used in the event of a suspected breach of the program requirements described in 5(a)-(d) of Annex A.

TRUSTe meets this requirement and has a review process in place to investigate a suspected breach of the program requirements described in 7 of Annex A. TRUSTe certification is fortified by strong enforcement of our Privacy Certification Program Requirements as well as our consumer dispute resolution process.

The TRUSTe enforcement process usually begins with an internal compliance investigation. TRUSTe may initiate this investigation based on results of our technological monitoring, on information contained in a consumer complaint, news or press reports, regulator inquiry, or reports from other credible sources. This process assists in the verification of compliance or non-compliance with the program requirements.

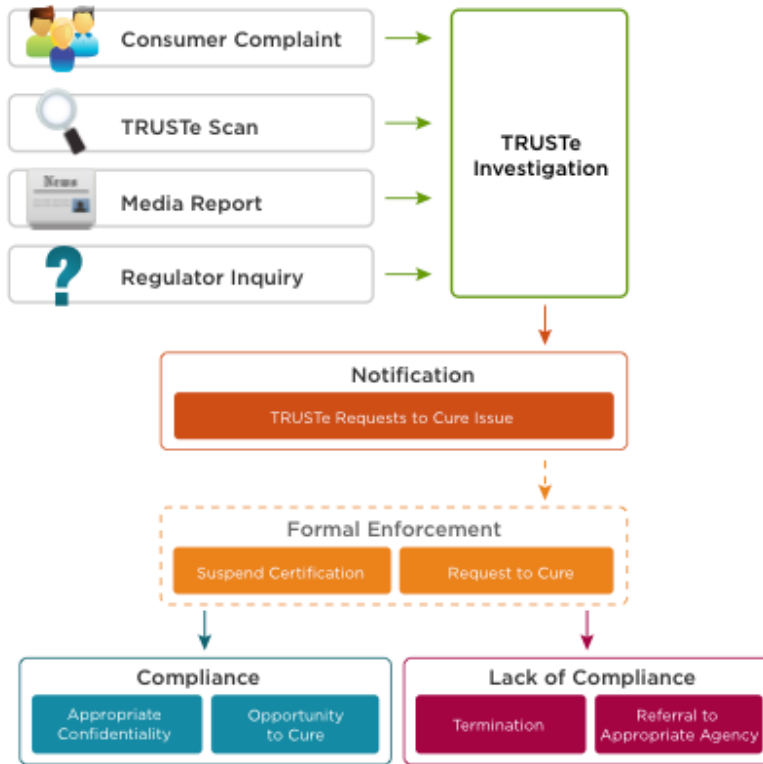
Where non-compliance with any of the program requirements is found, TRUSTe will sufficiently investigate the compliance issue, notify the Participant, outline the corrections necessary to come back into compliance with the APEC Privacy Program Requirements and provide a reasonable timeframe. TRUSTe will continue to collaboratively work with the Participant to come back into compliance.

Our investigations have one of three possible outcomes:

- An agreement between TRUSTe and the Participant over the privacy complaint resulting in Participant resolution that addresses the concern or request. TRUSTe provides a reasonable timeframe to complete the required changes based on the risk and level of non-compliance.
- A disagreement triggering a notice of formal enforcement, resulting in the Participant's suspension or notice of intent to terminate for cause if the matter is not cured.
- A failure to implement the required cure resulting in the Participant's termination from TRUSTe's program and, in extreme cases, publication and/or referral to an appropriate authority.⁷

⁷ One of our prior FTC referrals was ClassicCloseouts in 2008; TRUSTe assisted the FTC with the investigation, and the agency brought action for permanent injunction and relief against the site, ultimately obtaining a \$2.08 million settlement to provide redress for consumers. See Merchandiser Who Illegally Charged Consumers' Accounts Settles with FTC, available at: <http://www.ftc.gov/opa/2011/01/classicclose.shtm>.

The below diagram illustrates the specifics of enforcement process



Re-Certification and Annual Attestation

8. *Applicant Accountability Agent should describe their re-certification and review process as identified in 8(a)-(d) of Annex A.*

TRUSTe meets this requirement. At least once a year, TRUSTe investigates whether its Participants are meeting and/or exceeding TRUSTe’s APEC Privacy Program Requirements through a re-certification process. If the Participant notifies TRUSTe of a change or TRUSTe detects a change outside the ‘annual’ re-certification cycle, the change will be verified by TRUSTe immediately, regardless of whether it is time for the Participant’s annual re-certification or not.

Details of the re-certification process and annual attestation to answer questions Annex A 8 (a)-(d) are defined below.



- a) *Analyze*: TRUSTe performs an assessment of compliance.
- b) *Advise*: TRUSTe provides a comprehensive report to the Participant outlining our findings regarding compliance with TRUSTe's APEC Privacy Program Requirements.
- c) *Remedy*: TRUSTe verifies required changes outlined in the comprehensive report have been properly implemented.
- d) *Notify*: TRUSTe notifies Participant that it is in compliance with TRUSTe's APEC Privacy Program Requirements.

Dispute Resolution Process

9. *Applicant Accountability Agent should describe the mechanism to receive and investigate complaints and describe the mechanism for cooperation with other APEC recognized Accountability Agents that may be used when appropriate.*

TRUST has an existing Feedback and Dispute Resolution System⁸ that meets this requirement. We manage this dispute resolution process in-house and do not contract out this service to a third party. Our dispute resolution process is a mechanism to receive and investigate privacy-related complaints about Participants and to resolve these disputes between complainants and Participants. Consumer dispute resolution is a key component of TRUSTe's privacy management solution suite, and helps us monitor Participants' compliance with APEC Privacy Program Requirements and hold Participants accountable. Processing complaint disputes also provides TRUSTe with a window into the privacy issues that concern today's online consumers. This dispute resolution process is described in detail below.

10. *Applicant Accountability Agent should describe how the dispute resolution process meets the requirements identified in 10 (a) – (h) of Annex A, whether supplied directly by itself or by a third party under contract (and identify the third party supplier of such services if applicable and how it meets the conflict of interest requirements identified in sections 1-3 of Annex A) as well as its process to submit the required information in Annexes D and E.*

TRUSTe has its own in-house Feedback and Resolution System that meets the requirements identified in 10(a)-(h) of Annex A as described here:

⁸ TRUSTe's Feedback and Dispute Resolution System can be found at <http://www.truste.com/consumer-privacy/dispute-resolution/>



Receiving a Complaint

The TRUSTe Feedback and Resolution System's process begins with a consumer complaint filed against a TRUSTe program Participant either with the company, or with TRUSTe. After TRUSTe receives a complaint, we initiate an investigation. A TRUSTe investigation may also be initiated after a TRUSTe scan, a media report, regulator inquiry or information obtained through other credible sources. TRUSTe then reviews the complaint to determine if the complaint is relevant and falls under the scope of the Program Requirements. This generally takes 1-2 business days, but could take up to 10 business days.

Responding to & Investigating a Complaint

The consumer (complainant) receives TRUSTe's initial response within 10 business days, our published time frame⁹. TRUSTe's system notifies the complainant of the response by the Participant, if any. Complainant and the Participant may correspond directly, with TRUSTe copied, such as in the event that the Participant asks the complainant for further information. Complainant and Participant are copied when TRUSTe sends its determination

The nature and duration of the investigation needed can vary widely. TRUSTe quickly checks all issues that can be immediately verified but ultimate resolution of the complaint depends on the nature of the issue.

Resolving a Complaint

After the complaint has been investigated, the Participant ordinarily has 10 business days to provide a written response for the complainant. For more urgent issues, such as security vulnerabilities, we escalate to the Participant via phone as well and generally expect responses much sooner, especially if we are able to verify the problem.

Written Notice of Complaint Resolution

Once the complaint is resolved, TRUSTe will send an email notice to both the complainant and the Participant notifying them of closure of the complaint.

Process for Obtaining Consent

Our Feedback and Resolution form asks the complainant to provide consent before TRUSTe shares their personal information with the program Participant the complainant is filing a dispute about. See screenshot below.

⁹ The published timeframe can be found on TRUSTe's Feedback and Resolution Form at <https://feedback-form.truste.com/watchdog/request>



The full online submission process for submitting feedback and requesting assistance with privacy-related disputes can be found in Appendix B. All personal information collected during the request for assistance is collected in accordance with TRUSTe's Privacy Policy (Appendix G).

Below is a screenshot from TRUSTe's Feedback and Resolution Form illustrating TRUSTe's online consent mechanism. Note, the complainant must indicate a preference (around whether they want their complaint shared) prior to submitting their complaint.

TRUSTe may share my information to resolve my issue *

Yes, I give permission for TRUSTe to share my report and contact information with the organization named above to assist with resolving the issue.

No, I do not want my report and contact information shared (Note: this may limit the ability of the organization named above to address your concern).

Screenshot 1 – Consent Mechanism

Reporting Complaint Statistics and Release of Case Notes

TRUSTe certified its first company under the APEC Privacy Program in August 2013. To date, 5 companies have received APEC certification: IBM, Merck, Lynda.com, Yodlee and Workday.

To date, TRUSTe not received or addressed any complaints or disputes about companies in TRUSTe's APEC Privacy Program. As such, TRUSTe cannot submit CBPR-related complaint statistics or case notes in this renewal application.

TRUSTe issues an annual Transparency Report¹⁰ to provide information on its certification programs, processes, and statistics on the number and types of complaints received during the previous calendar year. See TRUSTe's 2013 Transparency Report (Appendix C) for details around the publically available statistics about the types of complaints received and resolved by TRUSTe in 2013.

Mechanism for Enforcing Program Requirements

11. Applicant Accountability Agent should provide an explanation of its authority to enforce its program requirements against participants.

¹⁰ TRUSTe's published Transparency Report: 2012 and 2013 can be found online at <http://www.truste.com/about-TRUSTe/transparency-report> and is attached with this submission as Appendix C



Authority to Enforce Program Requirements

TRUSTe has the authority to enforce its program requirements against Participants through our Master Services Agreement (“MSA”) which we require all clients to sign before we begin the engagement. This is reflected in TRUSTe’s MSA, section 3(a): Participant’s Adherence to the Program:

- a) Participant’s Obligation to Comply. Participant shall fully comply with the Applicable Program Requirements for each Program Amendment.

12. Applicant Accountability Agent should describe the policies and procedures for notifying a participant of non-compliance with Applicant’s program requirements and provide a description of the processes in place to ensure the participant remedy the non-compliance.

a) *Process of Notifying Participant of Non-Compliance and Remedy*

Once TRUSTe identifies that a Participant is not complying with our program requirements, either through our re-certification process, ongoing monitoring, or dispute resolution process, the Participant will be contacted immediately by the designated contact individual at TRUSTe. We will outline the corrections necessary to come back into compliance with our program requirements and provide a reasonable timeframe. TRUSTe will continue to work with the Participant to come back into compliance.

If the Participant fails to come back into compliance with the program requirements, TRUSTe will take steps, as outlined below, to either temporarily remove the seal from the Participant’s website or terminate the Participant’s participation in the program.

13. Applicant Accountability Agent should describe the policies and procedures to impose any of the penalties identified in 13 (a) – (e) of Annex A.

Remedy of Non-Compliance Within a Specified Timeframe

If the Participant does not remedy the non-compliance within a specific time period, TRUSTe has a process in place to place the Participant on suspension. This is reflected in TRUSTe’s APEC Privacy Program Requirements¹¹ - section IV.B.5.a (1)-(5), Suspension Status excerpted below.

¹¹ TRUSTe’s APEC Privacy Program Requirements are available on TRUSTe’s website at <http://www.truste.com/privacy-program-requirements/program-requirements> and are attached as Appendix A to this application.



5.Suspension Status

- a) In the event TRUSTe reasonably believes that Participant has materially violated these Program Requirements, Participant may be placed on suspension.
 1. Notice will be provided with a mutually agreed upon description of the violation and any remedial actions that TRUSTe will require Participant to take during the Suspension Period ("Suspension Obligations").
 2. Participant will be considered to be on Suspension immediately upon receiving notice from TRUSTe. Suspension shall last until such time as the Participant has corrected the material breach or Program Requirements violation to TRUSTe's satisfaction, but not for a period of greater than six (6) months ("Suspension Period") unless mutually agreed by the Parties.
 3. Suspension Obligations may include, but are not limited to:
 - a) Compliance with additional Program Requirements;
 - b) Cooperation with heightened compliance monitoring by TRUSTe; and
 - c) Payment to TRUSTe of mutually agreed additional amounts as compensation for TRUSTe's additional compliance monitoring.
 - d) Participant shall comply with all Suspension Obligations.
 4. During the Suspension Period, Participant's status may be indicated via a TRUSTe Validation webpage or TRUSTe may require Participant to cease using the TRUSTe trustmarks.
 5. At the end of the Suspension Period, TRUSTe will, in its discretion, either:
 - a) Determine that Participant has complied with Participant's Suspension Obligations, thereby satisfying TRUSTe's concerns;
 - b) Extend the Suspension Period by mutual agreement with the Participant; or
 - c) Determine that Participant has failed to comply with Participant's Suspension Obligations and immediately terminate Participant for cause.



Temporary Suspension to Display the TRUSTe Seal

During a period of non-compliance with Program Requirements, TRUSTe may suspend the Participant's right to display the TRUSTe seal and notify the Participant. This is part of our suspension process as detailed out above and reflected in our Privacy Program Requirements, section IV.5.a.4.

"During the Suspension Period, Participant's status may be indicated via a TRUSTe Validation webpage or TRUSTe may require Participant to cease using the TRUSTe trustmarks."

Referral to Relevant Privacy Authority

If a client does not cure a non-compliance issue and is terminated, TRUSTe evaluates factors such as whether the violation was egregious and intentional, or whether impact was de minimis. TRUSTe may refer the issue to the appropriate public authority or enforcement agency.

TRUSTe's referral to a privacy enforcement authority will also be contingent on whether or not the actions of the client rise to a level which would trigger jurisdiction by the privacy enforcement authority. TRUSTe does not refer clients to privacy enforcement authorities where such authority would be unable to take action against the referred client.

Other penalties – including monetary penalties – as deemed appropriate by the Accountability Agent.

If a client does not cure a non-compliance issue and is terminated, TRUSTe evaluates factors such as whether the violation was egregious and intentional, or whether impact was de minimis, in determining whether to publicize the non-compliance. TRUSTe does not have authority by contract to impose monetary penalties. Further, no commercial entity would enter into a contract with TRUSTe if TRUSTe were to have a contractual authority to impose monetary penalties.

*14. Applicant Accountability Agent should describe its policies and procedures for referring matters to the appropriate public authority or enforcement agency for review and possible law enforcement action.
[NOTE: immediate notification of violations may be appropriate in some instances.*

15. Applicant Accountability Agent should describe its policies and procedures to respond to requests from enforcement entities in APEC Economies where possible.

The response below applies to both items 14 and 15 of Annex B.



TRUSTe's policies and procedures for referral to the appropriate public authority or enforcement agency, including responding to requests from enforcement entities in APEC Economies, are explained above as response to Annex B Question 7 - On-going Monitoring and Compliance Review Processes and in TRUSTe's 2013 Transparency Report (Appendix C to this application) for publically available statistics about the types of complaints received and how these complaints were resolved.



Appendix

Appendix A

TRUSTe's APEC Privacy Program Requirements:

<http://www.truste.com/privacy-program-requirements/apec>

Appendix B

Description and online submission process for TRUSTe's online Feedback and Resolution System

Appendix C

TRUSTe 2012 Transparency Report

TRUSTe 2013 Transparency Report

Appendix D

TRUSTe Master Service Agreement and Privacy Certification Program Amendment
(attached with submission)

Appendix E

Client Interview Form

Appendix F

Findings Report

Appendix G

TRUSTe Privacy Policy:

<http://www.truste.com/privacy-policy>

Appendix H

Certification Conflict of Interest Policy

Service Delivery Conflict of Interest Policy