

Complaint

IN THE MATTER OF

**TRUE ULTIMATE STANDARDS EVERYWHERE,
INC., D/B/A TRUSTe, INC.**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATION OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT

*Docket No. C-4512; File No. 132 3219
Complaint, March 12, 2015 – Decision, March 12, 2015*

This consent order settles allegations that TRUSTe, Inc (“TRUSTe”) deceived consumers about its privacy seal program, its privacy practices, and its status as a non-profit entity. The complaint alleges that from 2006 until January 2013, TRUSTe failed to conduct annual recertifications of companies holding TRUSTe privacy seals in over 1,000 incidences, despite providing information on its website that companies holding TRUSTe Certified Privacy Seals receive recertification every year. In addition, the complaint alleges that, although TRUSTe became a for-profit corporation in 2008, the company failed to require its clients using TRUSTe seals to update references to TRUSTe’s for-profit status. Under the terms of the order, TRUSTe is prohibited from making misrepresentations about its certification process, its corporate status, or whether an entity participates in its programs. TRUSTe is also barred from providing other companies or entities with the means to make misrepresentations about these facts. The order also requires the company in its role as a COPPA safe harbor to provide detailed information about its COPPA-related activities in its annual filing to the FTC, as well as maintaining comprehensive records about its COPPA safe harbor activities for ten years. Each of these provisions represents an added requirement over the reporting requirements laid out under the COPPA rule for safe harbor programs. The company is further required to pay \$200,000 in disgorgement.

Participants

For the Commission: Jamie Hine and Jessica Lyon.

*For the Respondent: Adam J. Fleisher and D. Reed Freeman,
Morrison & Foerster LLP.*

COMPLAINT

The Federal Trade Commission (“Commission”), having reason to believe that True Ultimate Standards Everywhere, Inc., a corporation, has violated the provisions of the Federal Trade Commission Act (“FTC Act”), and it appearing to the Commission that this proceeding is in the public interest, alleges:

Complaint

1. Respondent True Ultimate Standards Everywhere, Inc., also doing business as TRUSTe, Inc. (“TRUSTe”), is a privately-owned, Delaware corporation with its principal office or place of business at 835 Market Street, Suite 800, San Francisco, California 94103.

2. TRUSTe was formed as a California non-profit corporation on June 10, 1997. On June 20, 2008, TRUSTe formed a for-profit Delaware corporation and transferred all of the assets of the California non-profit entity to the for-profit corporation pursuant to an Asset Purchase Agreement effective July 3, 2008.

3. Respondent has advertised, offered for sale, and sold data privacy services to companies, including a variety of assessments and certifications, monitoring tools, and compliance controls.

4. The acts and practices of Respondent as alleged in this complaint are in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

TRUSTE’S CERTIFIED PRIVACY SEALS

5. Since approximately June 1997, Respondent has offered clients Certified Privacy Seals (“Privacy Seals”) for display on clients’ websites. TRUSTe has more recently offered these seals for mobile applications. Respondent provides these seals to clients that meet designated requirements for the programs that Respondent administers (“Program Requirements”). These requirements include specifications related to transparency of company practices, verification of privacy practices, and consumer choice regarding the collection and use of consumer personal information.

6. Respondent advertises itself as “the #1 privacy brand” and asserts that its “Certified Privacy Seal is recognized globally by consumers, businesses, and regulators as demonstrating privacy best practices.”

7. Respondent’s Privacy Seal programs include, but are not limited to, TRUSTed Websites (since 1997), which certifies

Complaint

websites; COPPA/Children's Privacy (2001), which certifies compliance with the FTC's Children's Online Privacy Protection Act Rule; EU Safe Harbor (2002), which assists with certification to the EU-US Safe Harbor framework for transatlantic data transfers; TRUSTed Downloads (2006), which certifies software; TRUSTed Cloud (2011), which certifies data processing services through cloud platforms; TRUSTed Apps (2011), which certifies mobile applications; and TRUSTed Data (2011), which certifies data collection practices of non-consumer facing entities.

8. Companies that meet the Program Requirements of a particular Privacy Seal must display to consumers a corresponding seal on their websites and mobile applications to demonstrate publicly to consumers their compliance with the relevant TRUSTe program.

9. In connection with its Privacy Seal programs, Respondent has provided clients with images of seals to display on their websites and mobile applications, including, but not limited to "Click-to-verify" seals containing a graphic icon, and text indicating to consumers an ability to click on the seal:

These "Click-to-verify" seals are required and must be displayed by a client on its privacy policy webpage. They are linked to a webpage hosted on the www.truste.com website, which provides verification of the sealholder's name, the specific privacy seal(s) held, and the validity date for each seal. The website also links to the Program Requirements for the Privacy Seals.

10. Respondent tests and verifies client compliance with its Program Requirements underlying its Privacy Seals through scanning technology, client interviews, document collection, and manual testing and review of client websites and mobile applications.

11. TRUSTe purports to recertify privacy sealholders on an annual basis to identify, for example: (1) material changes to privacy policies (e.g., new or expanded collection/uses of personal information such as use of cookies for behavioral advertising); (2) seal validation (e.g., improper placement, old versions, and bad

Complaint

links); (3) changes in company ownership or business model (e.g., adoption of advertising supported content); and (4) where relevant, compliance with external third-party program requirements (e.g., Federal Trade Commission Children's Online Privacy Protection Act safe harbor, or U.S. Department of Commerce self-certification to the US/EU Safe Harbor).

12. At all times relevant to this complaint, Respondent has controlled the design of its seals, as well as the design, content, and format of the www.truste.com webpage to which these seals link.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

MISREPRESENTATION OF CERTIFICATION STATUS OF
TRUSTE CLIENTS

13. Since approximately 2011, Respondent has disseminated or has caused to be disseminated to consumers, on the www.truste.com website, Program Requirements containing the following statement:

III. Minimum Program Requirements

...

B. Participant Accountability

...

3. Annual Recertification

a. Participant shall undergo recertification to verify ongoing compliance with these Program Requirements annually.

(Exhibit A, Program Requirements, February 2011, available at www.truste.com)

Prior to 2011, Respondent disseminated or had caused to be disseminated to consumers Program Requirements containing the following statement:

II. Participant Responsibilities

...

C. Recertification. Participant must seek recertification by TRUSTe annually

...

Complaint

14. The statements set forth in Paragraph 13 have been included in Respondent's Program Requirements for at least each of the following programs: TRUSTed Websites (since 1997), COPPA/Children's Privacy (2001), EU Safe Harbor (2002), TRUSTed Cloud (2011), TRUSTed Apps (2011), TRUSTed Data (2011), and TRUSTed Smart Grid (2012).

COUNT 1

15. Through the means described in Paragraph 13, Respondent has represented, expressly or by implication, that TRUSTe has recertified annually all companies displaying a TRUSTe Certified Privacy Seal to ensure ongoing compliance with the Program Requirements.

16. In fact, from 2006 until January 2013, Respondent did not conduct annual recertifications for all companies holding TRUSTe Certified Privacy Seals. In over 1,000 instances, TRUSTe conducted no annual review of the company's compliance with applicable Program Requirements. Therefore, the representation set forth in Paragraph 13 was false or misleading.

MISREPRESENTATIONS REGARDING NON-PROFIT
STATUS OF TRUSTE

17. Prior to its transition to a for-profit entity on July 3, 2008, Respondent required its clients to display in their privacy policies the following language TRUSTe developed:

"TRUSTe is an independent, non-profit organization whose mission is to build users' trust and confidence in the Internet by promoting the use of fair information practices."

18. In early July 2008, Respondent notified all active and current clients that its tax status would change from non-profit to for-profit status. On July 15, 2008, the company issued a public press release announcing the company's transition to a for-profit entity.

Complaint

19. In numerous instances since July 3, 2008, the date when TRUSTe formed a for-profit Delaware corporation and ceased to be a non-profit California corporation, Respondent has recertified clients who have failed to update references to the company's for-profit status. Some TRUSTe clients' privacy policies continued to describe TRUSTe as a non-profit entity until fall of 2013.

Count 2

20. Through the means described in Paragraphs 17 and 19, Respondent has represented, expressly or by implication, that TRUSTe is a non-profit organization.

21. In fact, Respondent has not been a non-profit organization since July 3, 2008. Therefore, the representation set forth in Paragraph 20 was false or misleading.

22. By providing clients with the language in Paragraph 17 and continuing to certify clients using that language as described in Paragraph 19, Respondent has furnished the means and instrumentalities for the commission of the deceptive acts or practices alleged in Paragraph 21.

23. The acts and practices of Respondent as alleged in this complaint constitute deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this twelfth day of March, 2015, has issued this complaint against Respondent.

By the Commission.

Complaint

EXHIBIT A

Understanding TRUSTe's Privacy Requirements

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

Privacy Program Requirements

[Home](#) | [Privacy Program Requirements](#) | [Understanding Program Requirements](#)

TRUSTe Program Requirements

I. Structure

TRUSTed Websites requires compliance with the following program requirements. Upon satisfactory certification, TRUSTe provides companies with a TRUSTe Privacy Seal as evidence of compliance - certified companies must display this seal on their website privacy policy page and may elect to place the seal on additional webpages as well.

II. Definitions

The following definitions shall apply herein:

- A. "Behavioral Targeting" is the collection and use of information on an Individual's Online activity over a period of time for the purpose of developing and using predictive models to determine potential future behavior or interests.
- B. "Clear and Conspicuous" means a notice that is reasonably easy to find, and easily understandable in terms of content and style to the average reader.
- C. "Expressed Consent" means the affirmative consent (opt-in) to a practice by the Individual, after being provided notice, but prior to implementing the practice.
- D. "Foreign Language Privacy Statement" is the Participant's Privacy Statement translated into a language other than English.
- E. "Geo-location Data" is information obtained through an Individual's use of a Mobile Device and is used to identify or describe the Individual's actual physical location at a given point in time.
- F. "Individual" means the discrete person to whom the collected information pertains.
- G. "Informed Consent" means consent which is implied by an Individual, regarding the collection, use, disclosure, distribution of PII after notice and opportunity to withdraw consent (opt-out) is given by Participant, but not taken by the Individual.
- H. "Material Change" means degradation in the rights or obligations regarding the collection, use, or disclosure of PII for an Individual. This usually includes changes to Participant's:
 - 1. Practices regarding notice, collection, use, and disclosure of PII and/or Third Party Personally Identifiable Information;
 - 2. Practices regarding user choice and consent to how PII and/or Third Party Personally Identifiable Information is used and shared; or
 - 3. Measures for information security, integrity, access, or individual redress.
- I. "Mobile Device" is a portable electronic geo-location enabled device which allows the user to process, receive, and send data without being limited to a specific geographical location.
- J. "Online" is the state where an Individual is connected by computer or Mobile Device to one or more other computers, Mobile Devices, or networks, as through a commercial electronic information service or the internet.
- K. "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.
- L. "Personally Identifiable Information [PII]" means any information or combination of information that can be used to identify, contact, or locate a discrete Individual.
- M. "Primary Purpose" means use of PII that is reasonably expected by the Individual (i) at the point of collection, and (ii) including compatible uses in features and services to the Individual that do not materially change expectations of user control and third party sharing. Such use may be at least those uses described in the Participant's terms of service governing the Participant's products or services which give rise to the Individual's interaction with the Participant.
- N. "Privacy Statement" shall mean the statements of Participant's information collection and usage practices, as such practices are updated from time to time. Participant's Privacy Statement includes, but is not limited to:
 - 1. A single, comprehensive statement of all the Participant's information practices ("Comprehensive Privacy

[Events](#) | [Blog](#) | [Newsletter](#)

TRUSTe Products

[TRUSTed Websites](#)
For eCommerce and content websites

[EU Safe Harbor](#)
Global reach with EU Safe Harbor

[Children's Privacy](#)
For websites who market to children

[Mobile Privacy](#)
Certify your mobile apps and websites

[TRUSTed Email](#)
Achieve email privacy certification

[TRUSTed Ads](#)
Ad privacy compliance just got easier

[TRUSTed Downloads](#)
Certify your downloads to be safe

Complaint

EXHIBIT A

Understanding TRUSTe's Privacy Requirements

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

- Statement");
2. A summary notice highlighting the Participant's information practices ("Short Notice"); or
 3. Disclosure of specific information practices posted at the point of information collection ("Just in Time Notice").
- O. "Publicly Available Information [PAI]" means any information reasonably believed to be lawfully made available to the general public from:
1. Federal, state or local government records;
 2. Widely available source(s) having no additional prohibition around onward transfer or use; or
 3. Disclosures to the general public that are required to be made by federal, state or local law.
- P. "Recipient" means the individual who receives an Email Message.
- Q. "Retargeting" is a form of behavioral advertising by which online advertising is delivered to an individual based upon the individual's previous online actions.
- R. "Search Engine" is a publicly facing service that collects and organizes content from across the internet for the primary purpose of responding to a search request. Such service may not retain information beyond caching or other service enhancing techniques, or use the information to create a persistent profile of the individual for purposes other than enhancing search techniques.
- S. "Secondary Purpose" is the use of PII in a way that is not reasonably expected by the individual relative to the transactions or ongoing services provided to the individual by Participant or the Participant's Service Provider. Such purpose may or may not be described by Participant's terms of service governing Participant's products or services which give rise to the individual's interaction with the Participant.
- T. "Service Provider" is anyone other than the Participant or the individual that performs, or assists in the performance of, a function or activity which may involve the use or disclosure of PII or Third Party PII. Such use must only be on behalf of Participant or individual and only for the purpose of performing or assisting in that specific function or activity as agreed to by the Participant and individual.
- U. "Social Network" is an online service that offers the following features:
1. A platform that enables the interaction between two or more individuals for the purpose of creating social or business relationships, and sharing of information;
 2. Functionality that enables individuals to create a profile that includes information of their own choosing such as photos, and links to personal pages of other connected individuals (e.g. friends, business contacts);
 3. Mechanisms to communicate with other individuals such as instant messenger, email, or posting to a profile or newsfeed; and
 4. Search functionality that enables individuals to search for other individuals that is based upon that individual's preferences.
- V. "Third Party(ies)" is an entity(ies) other than the Participant or the individual which is not directly affiliated with the Participant, and, if affiliated with the Participant, where such affiliation is not reasonably known to the individual.
- W. "Third Party Personally Identifiable Information [Third Party PII]" means PII that is collected by Participant from an entity other than the individual.
- II. Minimum Program Requirements**
- A. All Participants warranting to be certified that their Online Information collection and use practices comply with TRUSTe's Privacy Program Requirements must comply with the following requirements:
- B. Participant Accountability
1. Participant shall have processes in place to comply with these Program Requirements
 2. Cooperation with TRUSTe
 - a. Provide, at no charge to TRUSTe or its representatives, full access to the Online properties (i.e., including password access to premium or members only areas) for the purpose of conducting reviews to ensure that Participant's Privacy Statement(s) is consistent with actual practices.
 - b. Provide, upon TRUSTe's reasonable request, information regarding how PII gathered from and/or tracked through Participant's Online properties is used.

Complaint

EXHIBIT A

Understanding TRUSTe's Privacy Requirements

<http://www.truste.com/privacy-program-requirements/>**3. Annual Recertification**

- a. Participant shall undergo re-certification to verify ongoing compliance with these Program Requirements annually.

4. Termination for Material Breach

- a. In the event TRUSTe reasonably believes the Participant has materially breached these Program Requirements, TRUSTe may terminate the Participant's participation in this program upon twenty (20) business days' prior written notice ("Notice of Termination") unless the breach is corrected within the same twenty (20) business day period ("Cure Period").
- b. Material breaches of these Program Requirements include but are not limited to:
 - 1. Participant's continual, intentional, and material failure to adhere to these Program Requirements;
 - 2. Participant's material failure to permit or cooperate with a TRUSTe investigation or review of Participant's Online properties or practices pursuant to the Program Requirements;
 - 3. Participant's continual, intentional, and material failure to comply with any Suspension Obligations;
 - 4. Participant's material failure to cooperate with TRUSTe regarding an audit, complaint or the compliance monitoring activities of TRUSTe; or
 - 5. Any deceptive trade practices by the Participant

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 trademarks.
- 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.

C. Privacy Practices

The following requirements apply if the Participant collects PII:

1. Collection Limitation

- a. Participant shall only collect PII where such collection is:
 - 1. Limited to information reasonably useful for the purpose for which it was collected and in accordance with the Participant's Privacy Statement in effect at the time of collection; or
 - 2. With notice to and consent of the Individual

2. Use of PII

Complaint

EXHIBIT A

Understanding TRUSTe's Privacy Requirements

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

- a. Participant shall use PII in the provision of those services advertised or provided for, and in accordance with their posted Privacy Statement in effect at the time of collection, or with notice and consent as described in these Program Requirements.
 - b. Information collected by the Participant or the Participant's Service Provider may be used to tailor the Individual's experience on the Participant's Online property.
3. Choice
- a. Participant shall offer the Individual control over their collected Personally Identifiable Information as follows:
 - 1. Participant must provide the Individual an opportunity to withdraw consent to having PII used by the Participant for a Secondary Purpose.
 - 2. Participant must provide the Individual a Just in Time Notice and the opportunity to withdraw consent to having PII disclosed or distributed to Third Parties, other than Service Providers, at the time PII is collected;
 - 3. Participant shall honor and maintain the Individual's choice selection in a persistent manner until such time the Individual changes that choice selection; and
 - 4. Participant shall provide a means by which the Individual may change their choice selection.
 - b. Consent is not necessary where the use, disclosure or distribution of PII is required by law, court order, or other valid legal process.
 - c. Express Consent must be obtained from the Individual prior to the transfer of PII to Third Parties other than Service Providers if an unauthorized use or disclosure of that information would be likely to cause financial, physical, or reputational harm to an Individual.
 - d. Privacy Statement shall state when the Individual can exercise control over the use and sharing of their PII and how to exercise that control
 - e. Such mechanism shall be easy to use and offered at no cost to the Individual
4. Collection and Use of Third Party PII
- a. Participant shall use Third Party PII collected solely to facilitate the one-time completion of the transaction that is the Primary Purpose for which the information was collected by the Participant except as allowed in Section III.C.4.d regarding Search Services.
 - b. Participant must obtain Express Consent from the Individual to whom such Third Party PII pertains before such Third Party PII may be used, disclosed, or distributed by the Participant for any purpose other than the Primary Purpose for which such information was collected by the Participant, except as allowed in Section III.C.4.d regarding Search Services.
 - 1. Participant may use Third Party PII to send a one-time email message to the Individual to solicit their Express Consent.
 - c. Regarding Third Party PII the Privacy Statement shall state:
 - 1. The types of the entity(ies) collecting Third Party PII;
 - 2. What kind of Third Party PII is collected, either through active or passive means;
 - 3. How collected Third Party PII is used and/or disclosed;
 - 4. What types of additional Third Parties if any, including Service Providers, collected Third Party PII is shared with.
 - d. Search Services

Complaint

EXHIBIT A

Understanding TRUSTe's Privacy Requirements

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

1. A Search Engine may provide search results containing Third Party PII, without the notice and choice requirements noted above, providing:
 - a. The results were obtained from public or published sources on the Internet;
 - b. The information is not used to create a persistent profile of the Individual outside the scope of enhancing Search Engine techniques;
 - c. Participant shall have a mechanism for the Individual to request removal from displayed search results if the display of such results will:
 - i. Cause physical harm to the Individual; or
 - ii. Interfere with the safeguarding of important countervailing public interests, including national security, defense, or public security.
 - d. Privacy statement shall state how Individual can request removal from displayed search results.
 2. A Participant that compiles information about Individuals, who are neither customers of or registered users of, that Participant's services; and then sells access to that information to Third Parties may provide search results containing Third Party PII without the notice and choice requirements noted above, providing:
 - a. Information obtained about the Individual is from public or published sources which have no prohibition around onward transfer or use associated with the information;
 - b. The Participant shall provide the Individual a mechanism to stop having their information displayed in search results:
 - i. Such mechanism shall be easily accessible to the Individual; and
 - ii. Privacy Statement shall state how the Individual can stop having their information displayed in search results.
 - c. This does not include situations where Participant disclosed Third Party PII back to an entity that has rights to such information.
5. Access
- a. Participant must implement reasonable and appropriate mechanisms to allow the Individual to correct or update inaccurate PII.
 - b. Participant must implement reasonable mechanisms to allow the Individual to request deletion of PII or that collected PII no longer be used.
 - c. Such mechanism should be consistent with how the Individual normally interacts or communicates with the Participant
 - d. Such mechanism or process shall be clear, conspicuous, and easy to use
 - e. Such mechanism or process shall confirm to the Individual inaccuracies have been corrected; and
 - f. Participant's privacy statement shall state how access is provided.
 - g. Participant is not required to permit Individual access to Personally Identifiable Information to the extent that:
 1. Such access would prejudice the confidentiality necessary to comply with regulatory requirements, or breach Participant's confidential information or the confidential information of others;
 2. The burden or cost of providing access would be disproportionate to the legitimate rights or interests of others would be violated. However, Participant may not deny access on the basis of cost if the Individual offers to pay the costs of access; or
 3. The requested PII is derived from public records or is Publicly Available Information and is not combined with non-public record or non-publicly available information.
 - h. If Participant denies access to PII, Participant must provide the Individual with an explanation of why access was denied and contact information for further inquiries regarding the denial of access.
6. Promotional and Newsletter Email Communications
- a. All newsletters and promotional email messages that Participant sends to the Individual must include Participant's postal address and a functional unsubscribe mechanism.
 - b. The location and instructions concerning the unsubscribe mechanism must be Clear and

Complaint

EXHIBIT A

Understanding TRUSTe's Privacy Requirements

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

- Conspicuous, and the mechanism itself must be functional for no fewer than thirty (30) days following the sending of the newsletter or promotional email message.
- c. Participant must honor the Individual's request to unsubscribe from a newsletter or promotional email message beginning on the tenth (10) business day after the Participant receives the unsubscribe request, unless the Individual subsequently requests to receive newsletters or promotional email messages from Participant.
 - d. An unsubscribe mechanism is not required for administrative or customer service-related email messages (e.g. account management or provisioning of requested services, warranty or recall information, safety or security announcements).
7. **Public Disclosure of PII**
- a. A Participant may allow a user to post PII in an online forum, chat room, blog or other public forum, where the PII being displayed was placed there by a user who is also the Individual.
 - 1. If appropriate and commercially reasonable, provide a process or mechanism to allow the Individual to request timely removal of any publicly displayed PII where it has been legally and rightfully shared; and
 - 2. State in the Privacy Statement how the Individual can request removal of publicly displayed PII.
 - b. The Privacy Statement shall state information posted by Individuals in online forums, chat rooms, blogs, or other public forum may be displayed publicly.
 - c. The Privacy Statement shall accurately describe the extent to which an Individual's displayed PII is publicly available.
 - d. If Participant provides a publicly accessible online directory or similar service, the Participant shall:
 - 1. Provide the Individual a reasonable and appropriate mechanism to request removal of their PII from the directory;
 - 2. Ensure the mechanism is consistent with how the individual normally interacts or communicates with the Participant;
 - 3. State in the Privacy Statement how the Individual can request removal; and
 - 4. Such mechanism to request removal of a listing where access to the online directory or similar service is limited to other registered individuals may be contingent on the Individual no longer using that service.
8. **Material Changes**
- a. Participant must notify Individuals of any Material Changes to its PII collection, use, or disclosure practices prior to making the change.
 - b. Participant must obtain prior approval from TRUSTe:
 - 1. For any Material Change in its PII collection, use, or disclosure practices; and
 - 2. For method and notice to Individuals, such as email, "in product" messaging, etc.
- D. **Privacy Statement**
- 1. Participant shall maintain and abide by an accurate up-to-date Privacy Statement approved by TRUSTe in its sole discretion that states Participant's information practices and is in conformance with these Program Requirements including, but not limited to:
 - a. What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used;
 - b. What types of Third Parties if any, including Service Providers, collected information is shared with;
 - c. Whether PII is appended with information obtained from third party sources;
 - d. How and when the Individual can exercise choice as required in these Program Requirements;
 - e. How the Individual can request access to their information as required in these Program Requirements;
 - f. What types of security measures are in place to protect collected information as required in these Program Requirements;
 - g. What tracking technologies are used by the Participant or Third Parties including Service Providers and the purpose for using those technologies;

Complaint

EXHIBIT A

Understanding TRUSTe's Privacy Requirements

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

- h. How the individual can contact the Participant, including company name, email address or a link to an online form, and physical address;
 - i. How the individual will be notified of any Material Changes in the Participant's privacy practices;
 - j. That collected information is subject to disclosure pursuant to judicial or other government subpoenas, warrants, orders, or if the Participant merges with or is acquired by a Third Party, or goes bankrupt;
 - k. Effective date of Privacy Statement;
 - l. If required, statement of participation in the TRUSTe program and define participation scope; and
 - m. Information on how to contact TRUSTe to express concerns regarding Participant's Privacy Statement or privacy practices.
2. At a minimum, Participant shall link to a Comprehensive Privacy Statement that discloses the Participant's information practices.
3. Access to the Privacy Statement shall be Clear and Conspicuous.
4. As commercially reasonable, Privacy statement must be available when the individual engages with the Participant, such as through an application, Web site homepage or landing page.
5. Privacy statement must be available at the point where the individual provides PII, or through a common footer.
6. Participant shall treat all collected information in accordance with the posted Privacy Statement in effect at the time of collection unless the individual otherwise has given Express Consent.
7. Short Notice
- a. If Participant chooses, they may provide a Short Notice highlighting their information practices including but not limited to:
 - 1. Summarize what information is collected by the Participant and how the Participant collects that information, either through active or passive means;
 - 2. Summarize how Participant uses collected information;
 - 3. Whether Participant shares PII with third parties, excluding Service Providers;
 - 4. How the individual can exercise choice and request access pursuant to these Program Requirements; and
 - 5. How to contact the Participant including company name, email address or link to online form, and postal address.
 - b. Access to the Short Notice shall be Clear and Conspicuous.
 - c. Short Notice shall link to Comprehensive Privacy Statement.
 - 1. Access to the Comprehensive Privacy Statement shall be Clear and Conspicuous.
 - d. Any Short Notice shall be consistent with Comprehensive Privacy Statement.
8. Just in Time Notice
- a. If Participant chooses to provide Just in Time Notice, the Just in Time Notice shall be consistent with Comprehensive Privacy Statement.
9. Foreign Language Privacy Statement
- a. If Participant seeks TRUSTe certification of a Privacy Statement in a language other than English, TRUSTe shall use commercially reasonable efforts to verify that Participant's Foreign Language Privacy Statement is an accurate translation of Participant's English language Privacy Statement.
 - b. Participant shall ensure that its privacy practices are the same, and that the Foreign Language Privacy Statement provides materially the same description of Participant's privacy practices as Participant's English Language Privacy Statement.
 - c. Participant must notify TRUSTe of any Material Changes to its Foreign Language Privacy Statement and submit changes to TRUSTe for review and approval.
- E. Data Governance
- 1. Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this Section III E.
 - a. Such controls and processes shall be
 - 1. Appropriate to the size of the Participant's business; and

Complaint

EXHIBIT A

Understanding TRUSTe's Privacy Requirements

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

2. Appropriate to the level of sensitivity of the data collected and stored
2. Data Security
 - a. Participant must implement commercially reasonable procedures to protect PII within its control from unauthorized access, use, alteration, disclosure, or distribution.
 - b. Participant shall maintain and audit internal information technology systems within Participant's control such as:
 1. Regularly monitor and repair systems including servers and desktops for known vulnerabilities;
 2. Limit access and use of PII, or Third Party PII, to personnel with a legitimate business need where inappropriate access, use, or disclosure of such PII, or Third Party PII, could cause financial, physical, or reputational harm to the individual;
 3. Implement protection against phishing, spam, viruses, data loss, and malware; and
 4. Use reasonable encryption methods for transmission of information across wireless networks, and storage of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual;
 - c. Participant shall utilize encryption such as Secure Socket Layer for the transmission of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual.
 - d. Access to PII or Third Party PII retained by Participant must be at least restricted by username and password if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual.
 - e. Privacy Statement shall state that security measures are in place to protect collected PII and/or Third Party PII.
3. Data Quality
 - a. Participant shall take commercially reasonable steps when collecting, creating, maintaining, using, disclosing or distributing PII to assure that the information is sufficiently accurate, complete, relevant, and timely for the purposes for which such information is to be used.
 - b. If any information collected by the Participant about an individual is disputed by that individual and is found to be inaccurate, incomplete, or cannot be verified, Participant shall promptly delete or modify that item of information, as appropriate, based on the results of the investigation.
4. Data Retention
 - a. If a Participant receives and retains PII or Third Party PII, the Participant must limit its retention to no longer than commercially useful to carry out its business purpose, or legally required; and must disclose in their Privacy Statement how long they will retain that information.
 - b. Regardless of the time period of retention, so long as a Participant has PII or Third Party PII in its possession or control, the requirements included herein shall apply to such information.
5. Service Providers
 - a. Participant must take commercially reasonable steps to ensure that its Service Providers with whom it shares PII either:
 1. Abide by Participant's privacy policies as reflected in Participant's Privacy Statement; or
 2. Abide by privacy policies that are substantially equivalent to Participant's privacy policies as reflected in Participant's Privacy Statement; and
 3. Abide by the rights and obligations attached to the PII by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PII.
6. User Complaints and Feedback
 - a. Participant shall provide users with reasonable, appropriate, simple and effective means to submit complaints, express concerns, or provide feedback regarding Participant's privacy practices.
 - b. Participant shall also cooperate with TRUSTe's efforts to investigate and resolve non-trivial privacy complaints, questions and concerns raised either by:
 1. Users through TRUSTe's dispute resolution process; or
 2. TRUSTe.
7. Data Breach

Complaint

EXHIBIT A

Understanding TRUSTe's Privacy Requirements

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

- a. Participant must notify an individual of a data breach within 45-days of a known breach as required by law or if the unauthorized disclosure of PII can cause financial, physical, or reputational harm to the individual unless otherwise required by law.
 - b. Unless otherwise required by law, notice to the individual must disclose the following:
 - 1. That a breach occurred;
 - 2. What type of information was breached;
 - 3. When the breach happened;
 - 4. What steps individual's can take to protect themselves;
 - 5. What the actions the Participant is taking regarding the breach (e.g. investigation); and
 - 6. What steps the Participant is taking to ensure the event does not happen again.
 - c. Participant must notify TRUSTe when it believes a data breach occurred. Participant must provide TRUSTe a copy of the notice to be sent or sent to affected individual(s).
- F. Behavioral Targeting**
- 1. Participants engaging in Behavioral Targeting or Retargeting shall disclose the following regarding Participant's Behavioral Targeting and/or Retargeting Practices in its Privacy Statement:
 - a. If information, collected either through active or passive means, is used by either the Participant or Third Party(ies) for the purpose of Behavioral Targeting or Retargeting;
 - b. If PII collected by the Participant is linked to information collected through Web usage activity from sources, e.g. Web sites other than Participant's, for the purpose of Behavioral Targeting or Retargeting;
 - c. Whether PII or Third Party PII is collected by, or shared with, additional Third Parties for the purposes of Behavioral Targeting or Retargeting; and
 - d. How and when the individual can exercise choice as required in this Section III.F.
 - 2. Participant shall provide instructions or link to a mechanism that enables the individual to withdraw consent for the use of their information for the purposes of behavioral advertising.
 - a. At a minimum, such instructions or link shall be made available in the Participant's Privacy Statement.
 - 3. Participant engaging in Behavioral Targeting or Retargeting shall offer choice to the individual as follows:
 - a. An individual must be provided an opportunity to withdraw consent to having PII linked to information collected through web usage activity for the purpose of Behavioral Targeting or Retargeting;
 - b. An individual must be provided an opportunity to withdraw consent to having PII shared with Third Parties, other than Service Providers, for the purpose of Behavioral Targeting or Retargeting at the time such PII is collected; and
 - c. Express Consent must be obtained prior to sharing PII with Third Parties, other than Service Providers, for the purposes of Behavioral Targeting or Retargeting, if the unauthorized use or disclosure of that information could cause financial, or physical harm to an individual.
- G. Social Networks**
- 1. Participants that enable users to network with other users of a community need to comply with the following:
 - a. Express Consent with confirmation is required for an individual to establish a profile.
 - b. Provide a reasonable and appropriate mechanism to allow the individual to manage their privacy settings.
 - 1. Mechanism should be consistent with how the individual normally interacts or communicates with the Participant
 - 2. Mechanism shall be clear, conspicuous, and easy to use
 - 3. Mechanism shall confirm to individual that privacy settings have been set; and
 - 4. Privacy Statement shall state how the individual can update their privacy settings.
 - c. Provide a reasonable and appropriate mechanism to allow the individual request deletion or deactivation of a profile.
 - 1. Mechanism should be consistent with how the individual normally interacts or

Complaint

EXHIBIT A

Understanding TRUSTe's Privacy Requirements

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

- communicates with the Participant
 - 2. Mechanism shall be clear, conspicuous, and easy to use
 - 3. Mechanism shall confirm to Individual profile has been deleted or deactivated, and
 - 4. Privacy Statement shall state how the Individual can request deletion or deactivation of their profile
 - d. Provide a reasonable and appropriate mechanism to allow the Individual to request removal of an unauthorized profile.
 - 1. Mechanism should be consistent with how the Individual normally interacts or communicates with the Participant
 - 2. Mechanism shall be clear, conspicuous, and easy to use
 - 3. Mechanism shall confirm to individual the unauthorized profile has been removed; and
 - 4. Privacy Statement shall state how the Individual can request removal of an unauthorized profile.
 - e. Individuals between the ages 13-17 must provide Express Consent to the collection, use, disclosure of either:
 - 1. PII pertaining to that individual; or
 - 2. Third Party PII pertaining to an individual between the ages of 13-17.
 - f. If Participant enables users to import Third Party PII from another source to their profile, the Participant must do the following:
 - 1. Treat all collected information as if it is Third Party PII as outlined in Section III C.4.
 - a. Collected information cannot be used to create a publishable profile unless the Participant obtains the Express Consent of the Individual.
 - 2. Provide Clear and Conspicuous notice to the user as to why they are providing a password or other access to their email account, and
- IV. US-EU and US-Swiss Safe Harbor Requirements**
- A. Participants want to self-certify with the Department of Commerce (DOC) for compliance with the U.S.-E.U. Safe Harbor or Swiss Safe Harbor Frameworks and list TRUSTe as its third party dispute resolution mechanism must comply with the Minimum Program Requirements and the following:
 - 1. Participant must provide an Individual with access to PII within thirty (30) calendar days of request.
 - a. If Participant does not provide an Individual the requested access within thirty (30) calendar days of the Individual's request, Participant must provide the Individual with a timeline establishing when the requested access will be provided.
 - b. Privacy Statement shall disclose the timeline establishing when the Individual can expect a response to their request for access.
 - 2. Privacy Statement shall include the following statement: "[Participant] complies with the [E.U.][Swiss] Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal information from [the European Union][Switzerland]."¹¹
 - a. The statement must include the following link to the Department of Commerce's Web site: <http://export.gov/safeharbor>
- V. Additional Email Requirements**
- A. Participants wanting to be certified for practices around the sending of commercial and promotional email must comply with the Minimum Program Requirements and the following:
 - 1. Participants must ensure that the following disclosures are accessible from the point of email address collection except where email address is used only to authenticate an Individual for purposes of accessing that Individual's account information
 - a. The nature of commercial or promotional email messages to be sent and the types of entities that will be providing content;
 - b. Whether Participant sells, rents or otherwise shares Recipients' email address with Third Parties other than Service Providers; and
 - c. If receiving commercial or promotional email messages is a requirement to receive a service, a disclosure of such requirement.

Complaint

EXHIBIT A

Understanding TRUSTe's Privacy Requirements

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

2. Prior to sending commercial or promotional email messages the Recipient must be provided the opportunity to withdraw consent to having his/her email address added to a mailing list. 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.
 3. If Participant has not collected the Recipient's email address directly, the Participant must perform due diligence to ensure that Clear and Conspicuous notice was provided regarding the use and disclosure of the Recipient's email address, and that the Individual had the opportunity to withdraw consent.
 - B. **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.
 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 comply with relevant internet standards such as the 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.
 - C. **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.
- VI. Mobile Services**
- A. Participants wanting to be certified for collecting PII through an application on a Mobile Device or through a Web site optimized for a Mobile Device must comply with the Minimum Program Requirements and the following:
 1. Participants will provide enhanced notice outside of the Privacy Statement by linking from a TRUSTe icon or text link to a TRUSTe-hosted Short Notice.
 2. The following disclosures will appear within the TRUSTe-hosted Short Notice:
 - a. Whether geo-location data is collected and how geo-location data is used;
 - b. What types of information is collected and how it is used;
 - c. Whether Participant shares PII with Third Parties, including Service Providers;
 - d. How the Individual can exercise choice and request access pursuant to these Program Requirements;
 - e. What tracking technologies are used by the Participant or Third Parties including Service Providers and the purpose for using those technologies;
 - f. What security measures are in place to protect collected information as required in these Program Requirements; and
 - g. How the Individual can contact the Participant, including company name, email address or a link to an online form, and physical address.
 - C. **Geo-location Data**
 1. Participant must obtain Express Consent from the Individual the first time Geo-location Data is used by the Participant to provide services.
 2. Participant may provide additional notifications through a Just in Time Notice or a persistent icon, to remind Individuals that their Geo-location Data is being used by the Participant to provide a service.
 3. Participant must obtain Express Consent from the Individual prior to the sharing of Geo-location Data with Third Parties other than Service Providers.
 4. Participant must obtain Express Consent from the Individual prior to any use of Geo-location Data for Secondary Purposes.
 - D. Privacy Statement shall state:

Complaint

EXHIBIT A

Understanding TRUSTe's Privacy Requirements

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

1. What information is collected from an individual's Mobile Device;
2. Whether information is shared with another application installed on the individual's Mobile Device;
3. How Geo-location Data is used;
4. If Geo-location Data is used to create a profile about the individual;
5. How long Geo-location Data is retained;
6. What type of Third Parties, including Service Providers is Geo-location Data is shared with and for what purpose;
7. How the individual can restrict the disclosure of Geo-location data to Third Parties; and
8. How the individual can revoke consent to the Participant's collection and use of Geo-Location Data.
 - a. Such mechanism shall be easy to use.

FOLLOW US

AWARDS AND PRESS

[About Us](#) | [Contact Us](#) | [Partner Program](#) | [Careers](#) | [Site Map](#) | [Privacy Policy](#) | [Terms of Service](#) | [Terms of Use](#)

© TRUSTe Internet Privacy and Security for Businesses

loading

Decision and Order

DECISION AND ORDER

The Federal Trade Commission (“Commission” or “FTC”), having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft of complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge Respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45 *et seq.*;

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), which includes: a statement by Respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the Respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments filed by interested persons, now in further conformity with the procedure prescribed in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its Complaint, makes the following jurisdictional findings, and enters the following Order:

1. Respondent True Ultimate Standards Everywhere, Inc., also doing business as TRUSTe, Inc., is a privately-owned, Delaware corporation with its principal office or place of business at 835 Market Street, Suite 800, San Francisco, California 94103.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the

Decision and Order

Respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

For purposes of this order, the following definitions shall apply:

1. “Seal” shall mean any trustmark, logo, seal of approval, emblem, shield, or other insignia Respondent has offered or provided for placement on a company’s website, including, but not limited to TRUSTed Websites, COPPA/Children’s Privacy, EU Safe Harbor, TRUSTed Cloud, TRUSTed Apps, and TRUSTed Data.
2. Unless otherwise specified, “Respondent” shall mean True Ultimate Standards Everywhere, Inc., and its successors and assigns.
3. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
4. “COPPA” shall mean the Federal Trade Commission’s Children’s Online Privacy Protection Rule, 16 C.F.R. Part 312.
5. “COPPA safe harbor program” shall mean any self-regulatory program [guidelines] established pursuant to 16 C.F.R. § 312.11 of the Federal Trade Commission’s Children’s Online Privacy Protection Rule and operated by Respondent.

I.

IT IS ORDERED that Respondent, directly or through any corporation, subsidiary, division, or other device, including franchisees, or licensees, in connection with the advertising, promotion, offering for sale, sale, or distribution of seals or certifications, or any other substantially similar product, in or

Decision and Order

affecting commerce, shall not misrepresent, in any manner, expressly or by implication:

- A. The steps it takes to evaluate, certify, review, or recertify a company's privacy practices;
- B. The frequency with which Respondent conducts any such evaluation, certification, review, or recertification of a company's privacy practices;
- C. The corporate status of Respondent and its independence; and
- D. The extent to which the person or entity is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy program sponsored by Respondent.

II.

IT IS FURTHER ORDERED that Respondent, directly or through any corporation, subsidiary, division, or other device, including franchisees, or licensees, shall not provide to any person or entity the means and instrumentalities with which to make directly or by implication any misrepresentation prohibited by Part I of this order. For purposes of this Part, "means and instrumentalities" shall mean any information, including but not necessarily limited to, any required or model language, for use in any privacy policy or statement for display on a website or mobile application covered by any seal or certification provided by Respondent, or any other product or service covered under this order, in or affecting commerce.

III.

IT IS FURTHER ORDERED that Respondent for ten (10) years after the date of service of this order, as part of its annual report required to be submitted pursuant to 16 C.F.R. §312.11(d)(1) of the COPPA Rule, shall, in a sworn statement provide:

Decision and Order

- A. The total number of new seals awarded to participants in any COPPA safe harbor program in the preceding reporting period;
- B. A detailed explanation of the mechanisms used by Respondent to assess the fitness of new applicants to any COPPA safe harbor program for membership in the program;
- C. A detailed explanation of the mechanisms used by Respondent to assess the continuing fitness of an existing participant in any COPPA safe harbor program for membership in the program; and
- D. Any additional steps Respondent undertook to comply with the requirements of 16 C.F.R. § 312.

Unless otherwise directed by a representative of the Commission, all statements required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of TRUSTe, Inc.*, FTC File No. 1323219. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IV.

IT IS FURTHER ORDERED that Respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of, for a period of ten (10) years from the date of preparation:

- A. A detailed explanation of assessments Respondent conducted during the preceding reporting period to determine the fitness of new applicants to any COPPA safe harbor program for membership in the program;
- B. A detailed explanation, including the frequency, of assessments Respondent conducted during the

Decision and Order

preceding reporting period to determine the continuing fitness of an existing participant in any COPPA safe harbor program for membership in the program;

- C. Any documents related to consumer complaints, received in the preceding reporting period, alleging violations of any COPPA safe harbor program by Respondent or by participants in any COPPA safe harbor program;
- D. Any documents related to records of disciplinary actions taken in the preceding reporting period against participants in any COPPA safe harbor program; and
- E. Any documents related to approvals of COPPA safe harbor program participants' use of verifiable parental consent mechanism under 16 C.F.R. § 312.11(d)(1).

V.

IT IS FURTHER ORDERED that within five (5) days of the date of service of this order, Respondent shall pay \$200,000 to the United States Treasury as disgorgement, as follows:

- A. The payment shall be made by wire transfer to the Treasurer of the United States, in accordance with instructions provided by the Federal Trade Commission.
- B. In the event of any default in payment, interest shall accrue, computed pursuant to 28 U.S.C. § 1961, from the date of default to the date of payment.
- C. Respondent relinquishes all dominion, control, and title to the funds paid to the fullest extent permitted by law. Respondent shall make no claim to or demand return of the funds, directly or indirectly, through counsel or otherwise.

Decision and Order

VI.

IT IS FURTHER ORDERED that Respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all documents, whether in written or electronic form, that relate to compliance with this order, including but not limited to:

- A. all advertisements and promotional materials containing any representations covered by this order, with all materials used or relied upon in making or disseminating the representation;
- B. consumer complaints (whether received directly, indirectly, or through any third party) that relate to Respondent's activities as alleged in the draft Complaint and Respondent's compliance with the provisions of this order; and any responses to such complaints;
- C. copies of all subpoenas and other communications with law enforcement entities or personnel, if such documents bear in any respect on Respondent's activities as alleged in the Complaint and Respondent's compliance with the provisions of this order; and
- D. any documents, whether prepared by or on behalf of Respondent, that call into question Respondent's compliance with this order.

VII.

IT IS FURTHER ORDERED that Respondent shall deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30)

Decision and Order

days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VIII, delivery shall be at least ten (10) days prior to the change in structure. Respondent must secure a signed and dated statement acknowledging receipt of this order, within thirty (30) days of delivery, from all persons receiving a copy of the order pursuant to this Part.

VIII.

IT IS FURTHER ORDERED that Respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. *Provided, however*, that, with respect to any proposed change in the corporation(s) about which Respondent learns fewer than thirty (30) days prior to the date such action is to take place, Respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of True Ultimate Standards Everywhere, Inc.*, FTC File No. 1323219. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IX.

IT IS FURTHER ORDERED that Respondent, within one hundred twenty (120) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of

Decision and Order

written notice from a representative of the Commission, it shall submit an additional true and accurate written report.

X.

This order will terminate on March 12, 2035, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this order that terminates in fewer than twenty (20) years;
- B. This order's application to any Respondent that is not named as a defendant in such complaint; and
- C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such Respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Analysis to Aid Public Comment

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission has accepted, subject to final approval, an agreement containing an order from True Ultimate Standards Everywhere, Inc. (“TRUSTe”).

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission again will review the agreement and the comments received and will decide whether it should withdraw from the agreement or make final the agreement’s proposed order.

This matter involves respondent’s marketing and distribution of a variety of online privacy seals (“seals”) for companies to display on their websites. The FTC complaint alleges that respondent violated Section 5(a) of the FTC Act by falsely representing to consumers the frequency with which it reviews and verifies the practices of companies displaying its website and mobile seals. Specifically, the complaint alleges that from June 1997 until January 2013, respondent failed to conduct annual recertifications for almost 1,000 companies holding respondent’s TRUSTed Websites, COPPA/Children’s Privacy, EU Safe Harbor, TRUSTed Cloud, TRUSTed Apps, TRUSTed Data, and TRUSTed Smart Grid seals. In addition, the complaint alleges that respondent provided to its sealholders the means and instrumentalities to misrepresent that respondent is a non-profit corporation. The FTC complaint describes, with specificity, that following respondent’s transition to a for-profit corporation in July 2008, respondent recertified numerous clients whose privacy policies continued to describe TRUSTe as a non-profit entity.

The proposed consent order contains provisions designed to prevent respondent from engaging in similar acts and practices in the future. Part I of the proposed order prohibits respondent from misrepresenting (1) the steps respondent takes to evaluate, certify, review, or recertify a company’s privacy practices; (2) the frequency with which respondent evaluates, certifies, reviews, or recertifies a company’s privacy practices; (3) the corporate status of respondent and its independence; and (4) the extent to which

Analysis to Aid Public Comment

any person or entity is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy program sponsored by respondent. Part II of the proposed order prohibits respondent from providing to any person or entity the means and instrumentalities (including any required or model language for use in any privacy policy or statement) to misrepresent any of the same items in Part I of the proposed order.

Parts III and IV of the proposed order contain additional reporting requirements with respect to respondent's COPPA/Children's Privacy seal. First, the proposed order expands respondent's COPPA recordkeeping and reporting requirements to ten years. Second, the proposed order requires respondent to report (1) the number of new seals it awards; (2) how it assesses the fitness of members; and (3) any additional steps it takes to monitor compliance with the safe harbor requirements. Third, the proposed order expands respondent's COPPA requirement to retain consumer complaints and descriptions of disciplinary actions to include consumer complaints related to respondent and its safe harbor program participants as well as all documents related to disciplinary actions taken by respondent. Fourth, the proposed order imposes additional COPPA recordkeeping requirements, such as a requirement that respondent retain detailed explanations of assessments of new and existing applicants in any COPPA safe harbor program.

Part V of the proposed order requires respondent to pay \$200,000 to the United States Treasury as disgorgement.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed complaint order or to modify in any way the proposed order's terms.

Concurring Statement

**STATEMENT OF CHAIRWOMAN RAMIREZ,
COMMISSIONER BRILL, AND COMMISSIONER
MCSWEENEY**

We write to express our strong support for the complaint and consent order in this case.

The Commission unanimously supports Count I of the complaint in this matter, which is of paramount importance, in light of TRUSTe's unique role in increasing consumer trust in the global marketplace and ensuring the effectiveness of relevant self-regulatory frameworks. TRUSTe operates privacy-related self-regulatory and oversight programs for businesses and offers certified privacy seals for program participants, including (1) COPPA/Children's Privacy, which certifies compliance with the Children's Online Privacy Protection Act and implementing regulations; (2) EU Safe Harbor, which certifies compliance with the U.S.-EU Safe Harbor Framework; (3) TRUSTed Apps, which certifies the privacy practices of mobile applications; and (4) APEC Privacy, which certifies compliance with the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules System.¹

In Count I, the Commission alleges that TRUSTe promised consumers it would annually recertify its self-regulatory program participants for compliance with TRUSTe's privacy program requirements, but that, in many instances, it failed to do so. Annual recertification is a cornerstone of the service TRUSTe provides. It helps ensure that companies (1) continue to follow TRUSTe's program requirements, (2) do not make material changes to their practices or policies without appropriate consent, and (3) periodically consider the impact of technology and marketplace developments in their privacy practices. TRUSTe did not fulfill its obligations; today's order helps to ensure that TRUSTe will do so in the future. Consumers who see the TRUSTe seal on a website or mobile app should be confident that a trusted third party has kept its promise to review and vouch for the privacy practices of that website or mobile app. We also

¹ TRUSTe's APEC Privacy certification program was not the subject of the allegations in the complaint. TRUSTe became an "Accountability Agent" for the APEC Cross-Border Privacy Rules System in June 2013, and issued its first certification under that program in August 2013.

Concurring Statement

believe that Count II represents an appropriate use of “means and instrumentalities” liability. At the time TRUSTe provided model language for its clients’ privacy policies stating that TRUSTe was a nonprofit entity, there is no question that the statement was true. However, after TRUSTe informed clients of its for-profit status in 2008, many clients neglected to update their policies and continued to represent that TRUSTe was a nonprofit entity. These ongoing representations by TRUSTe’s clients clearly became deceptive once TRUSTe converted to a for-profit entity. Yet for five years, TRUSTe continued to recertify some companies that included this deceptive statement, that TRUSTe itself had disseminated, in their privacy policies. TRUSTe was well-positioned to rectify the misrepresentation about its own corporate status – it could have elected simply not to recertify the companies in question until the misrepresentation was cured. It failed to take this straightforward step and instead continued to bless the language at issue by giving the companies its seal of approval.

In *Shell Oil Company* and *FTC v. Magui Publishers, Inc.*, which Commissioner Ohlhausen cites in her statement, the Commission concluded that by providing customers with engage in deceptive acts or practices.¹ In this case, although TRUSTe disclosed to clients its change in status, it continued to recertify privacy policies using language TRUSTe had itself supplied about its corporate status that was no longer true. TRUSTe’s recertification of these inaccurate privacy policies is the conduct we take aim at – it provided a stamp of approval of a false representation which TRUSTe’s clients then passed along to consumers via their websites. As such, TRUSTe provided its clients with the means and instrumentalities to deceive others. The application of means and instrumentalities liability in this case is consistent with the principle underlying *Shell* and *Magui Publishers*, namely, that one who places the means of deception in the hands of another is also liable for the deception under Section 5.² The inclusion of this count is particularly appropriate

¹ *In the Matter of Shell Oil Co.*, 128 F.T.C. 749 (1999); *FTC v. Magui Publishers, Inc.*, No. 89-3818RSWL(GX), 1991 WL 90895 (C.D. Cal. Mar. 28, 1991), *aff’d* 9 F.3d 1551 (9th Cir. 1993).

² Commissioner Ohlhausen suggests that the allegations underlying Count II would be more appropriately viewed through the lens of secondary “aiding

Dissenting Statement

here, given TRUSTe's unique position in the privacy self-regulatory ecosystem. Companies that purport to hold their clients accountable to protect consumer privacy should themselves be held to an equally high standard.

**PARTIAL DISSENT OF
COMMISSIONER MAUREEN K. OHLHAUSEN**

I support Count I of the complaint in this matter because of TRUSTe's unique position of consumer trust as a third party certifier. However, I do not support the use of "means and instrumentalities" liability in Count II of the complaint and dissent as to that Count.

TRUSTe was initially organized in 1997 as a non-profit. Before July 2008, TRUSTe required every certified client website to include in its privacy policy a description of TRUSTe stating in part, "TRUSTe is [a] non-profit organization." On July 3, 2008, TRUSTe changed its corporate form from non-profit to for-profit. The company announced the change to its clients and requested that all clients update the relevant privacy policy language on their websites. Some clients did not update their websites. When TRUSTe recertified such websites, TRUSTe would typically request, but not require, that the client update their privacy policy to reflect the change to for-profit status.

Count II of our complaint alleges that by recertifying websites containing privacy policies that inaccurately describe TRUSTe as a non-profit, TRUSTe provided the means and instrumentalities to its clients to misrepresent that TRUSTe was a non-profit corporation. Specifically, the majority's statement argues that "TRUSTe's recertification of these inaccurate privacy policies ...

and abetting" liability. Regardless of whether one could construct alternative theories of liability, our concern is with TRUSTe's own actions. As discussed above, the deception here was the result of TRUSTe's own actions.

Dissenting Statement

provided its clients with the means and instrumentalities to deceive others.”³

I disagree with this use of means and instrumentalities. To be liable of deception under means and instrumentalities requires that the party *itself* must make a misrepresentation, as the Commission detailed in *Shell Oil Company*.⁴ According to the majority in that case, “[T]he means and instrumentalities doctrine is intended to apply in cases ... where the originator of the unlawful material is not in privity with consumers” and “it is well settled law that the originator is liable if it passes on a false or misleading representation with knowledge or reason to expect that consumers may possibly be deceived as a result.”⁵ For example, in *FTC v. Magui Publishers, Inc.*, the court found the defendant directly liable for providing the means and instrumentalities to violate Section 5 when it sold Salvador Dali prints with forged signatures to retail customers, who then sold the prints to consumers.⁶

Unlike *Shell* and *Magui Publishers*, the statement that TRUSTe provided to its clients was indisputably truthful at the time. During the period in which TRUSTe required client privacy policies to state that TRUSTe was a non-profit, TRUSTe was, in

³ *In the Matter of True Ultimate Standards Everywhere, Inc.* (“TRUSTe”), FTC File No. 1323219, Statement of Chairwoman Ramirez, Commissioner Brill, and Commissioner McSweeney, at 2 (Nov. 17, 2014).

⁴ *In the Matter of Shell Oil Co.*, 128 F.T.C. 749 (1999).

⁵ *Id.* at *10 (Public Statement of Chairman Pitofsky, Commissioner Anthony and Commissioner Thompson) (emphasis added). Similarly, Commissioner Orson Swindle’s dissent stated that under FTC precedent, “means and instrumentalities is a form of primary liability in which the respondent was using another party as the conduit for disseminating **the respondent’s misrepresentations** to consumers.” *Id.* at *14-15 (Dissenting Statement of Commissioner Orson Swindle) (emphasis added). Swindle’s dissent likewise emphasized that a defendant “may not be held primarily liable unless it has actually made a misrepresentation.” *Id.* (quoting *In re JWP Inc. Securities Lit.*, 928 F. Supp. 1239, 1256 (S.D.N.Y. 1996)). See also *FTC v. Magui Publishers, Inc.*, Civ. No. 89-3818RSWL(GX), 1991 WL 90895, at *14, (C.D. Cal. 1991), *aff’d*, 9 F.3d 1551 (9th Cir. 1993) (“One who places in the hands of another a means or instrumentality to be used by another to deceive the public in violation of the FTC Act is directly liable for violating the Act.”).

⁶ *Magui Publishers, Inc.*, 1991 WL 90895, at *17.

Dissenting Statement

fact, a non-profit. Once TRUSTe changed to for-profit status, it no longer required clients to state its non-profit status and actively encouraged clients to correct their privacy policies. TRUSTe did not pass to clients any false or misleading representations regarding its for-profit status. Nor was TRUSTe's recertification of websites a misrepresentation of TRUSTe's non-profit status to its clients; during recertification TRUSTe again clearly communicated its for-profit status to clients by requesting that its clients update their privacy policies. Because TRUSTe accurately represented its non-profit status to its clients, TRUSTe cannot be primarily liable for deceiving consumers under a means and instrumentalities theory.

TRUSTe's alleged recertifications of untrue statements are more properly analyzed as secondary liability for aiding and abetting.⁷ In *Magui Publishers* the court found that the defendant forgers were not only directly liable for their own misstatements, but also secondarily liable for the retailers' fraudulent misrepresentations to consumers because defendants "supplied their deceptive art work, certificates and promotional materials to their retail customers with full knowledge these customers would use the materials to deceive consumers."⁸ The court explained that aiding and abetting has three components: "(1) the existence of an independent primary wrong; (2) actual knowledge by the alleged aider and abettor of the wrong and of his or her role in furthering it; and (3) substantial assistance in the commission of the wrong."⁹

It is not clear that TRUSTe's clients committed an independent primary wrong. However, TRUSTe certainly had

⁷ "[A] respondent who has provided assistance to another party that has made misrepresentations is at most secondarily liable -- in particular, for aiding and abetting another's misrepresentations." *Shell Oil Co.*, 128 F.T.C. 749, *15 (1999) (Swindle Dissent) (citing *Wright v. Ernst & Young LLP*, 152 F.3d 169, 175 (2d Cir. 1998), cert. denied, 119 S.Ct. 870 (1999); *Shapiro v. Cantor*, 123 F.3d 717, 720 (2d Cir. 1997); *Anixter v. Home-Stake Production Co.*, 77 F.3d 1215, 1225 (10th Cir. 1996) ("the critical element separating primary from aiding and abetting violations is the existence of a representation, made by the defendant.")).

⁸ *Magui Publishers, Inc.*, 1991 WL 90895, at *15.

⁹ *Id.* at *14.

Dissenting Statement

knowledge of the misstatements in the privacy policies and of TRUSTe's role in facilitating those misstatements. And, arguably, its certifications may have provided substantial assistance in deceiving consumers. Regardless, because TRUSTe never misrepresented its corporate status, TRUSTe's actions regarding its corporate status at most comprise aiding and abetting its clients' actions.

Perhaps all this seems like legal hairsplitting, but it is not. Under the Supreme Court's decision in *Central Bank of Denver v. First Interstate Bank of Denver*,¹⁰ the FTC "may well be precluded from bringing Section 5 cases under an aiding and abetting theory."¹¹ By prosecuting activities more properly analyzed as aiding and abetting under the guise of means and instrumentalities liability, I am concerned that we are stepping beyond the limits the Supreme Court has established. I therefore dissent from Count II.

¹⁰ *Cent. Bank, N.A. v. First Interstate Bank, N.A.*, 511 U.S. 164 (1994).

¹¹ *Shell Oil Co.*, 128 F.T.C. 749, *19 (Swindle Dissent).

Complaint

IN THE MATTER OF

**MPHJ TECHNOLOGY INVESTMENTS, LLC,
JAY MAC RUST, AND FARNEY DANIELS, P.C.**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATION OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT

*Docket No. C-4513; File No.142 3003
Complaint, March 13, 2015 – Decision, March 13, 2015*

This consent order concerns deceptive sales claims and phony legal threats mailed to thousands of small businesses across the United States in an attempt to sell licenses for certain U.S. patents. MPHJ Technology Investments, LLC and the subsidiaries that it controls (collectively “MPHJ”) are patent assertion entities. Patent assertion entities purchase patent rights and seek to generate revenue by licensing to, or litigating against, those who are or may be using the patented technology. The complaint alleges that MPHJ bought patents relating to network computer scanning technology and then told thousands of small businesses that they were likely violating the patents and should purchase a license. MPHJ further sent letters that falsely represented that many other companies had already agreed to pay thousands of dollars for licenses. The complaint alleges that additional letters were sent in the name of MPHJ’s law firm, Farney Daniels, P.C., falsely threatened the recipients with patent infringement lawsuits. The complaint alleges that these representations constitute deceptive acts or practices in violation of Section 5 of the Federal Trade Commission Act. Under the consent order, MPHJ, Farney Daniels, P.C., and MPHJ’s owner, Jay Mac Rust, are prohibited, when asserting patent rights, from making false or unsubstantiated representations that a patent has been licensed in substantial numbers or has been licensed at particular prices. The order also prohibits misrepresentations that a lawsuit will be initiated and misrepresentations about the imminence of such a lawsuit.

Participants

For the *Commission*: *Daniel O. Hanks* and *Michael Tankersley*.

For the *Respondents*: *Bryan Farney* and *Robert P. Taylor, Arnold & Porter*; and *Allen Denson* and *Joel Winston, Hudson Cook, LLP*.

COMPLAINT

The Federal Trade Commission (“Commission”), having reason to believe that MPHJ Technology Investments, LLC, a