COMPLAINT STATISTICS

Complaint Numbers

CBPR-Related Complaints for period 3/01/17-2/28/18: **191**

Note: For purposes of this report, "complaint" refers to a complaint filed with TRUSTe via TRUSTe's Feedback and Resolution System against a TRUSTe client certified at that time by TRUSTe under our APEC-CBPR program.

Complaint Statistics

From March 1, 2017 through February 28 2018, TRUSTe handled 191 Dispute Resolution complaints against CBPR certified companies. The statistics below show how these complaints were classified and ultimately resolved by TRUSTe. Approximately 48 percent (92) of total complaints were closed by TRUSTe on "procedural grounds." Such procedural grounds may include complaints that fail to state a comprehensible issue or even a complete word (e.g. random typing such as "xyxyxy"). In other examples, the consumer complaint did not give TRUSTe permission to pass identifying information to the site in question, or provided an invalid e–mail address, impeding investigation of that complaint. Of the remaining complaints not closed on procedural grounds, 71 were resolved by consumer education. 7 required issue–specific changes by the site (e.g. unsubscribe the user, close the account). 21 fell into other categories such as those that fall outside the scope of TRUSTe's authority under our privacy program, (e.g. billing/transactional issues, requests for feature enhancements). TRUSTe typically suggests that the consumer contact the site directly in these instances. No complaints were pending resolution as of this reporting period.

Complaints Type

By Principle	By Country	By Type
Other: 171	Arab Emirates: 3	Abuse by Another User: 5
Access: 55	Australia: 1	Account Access / Creation: 16
Security: 13	Bosnia/Herzegovina: 1	Account Hacked / Disabled / Suspended: 13
Use: 6	Bermuda: 1	Can't Change / Remove Personal Info: 39
TOTAL: 191	Brazil: 2	Help with Features / Functionality: 40
	Canada: 12	Monetary / Billing / Transactional: 15
	Cambodia: 1	Received Unauthorized E-Mail: 2

	China: 1 Germany: 1 France: 3 Gibraltar: 1 Guatemala: 1 Ireland: 2 India: 2 Japan: 2 Malaysia: 4 Netherlands: 1 New Zealand: 1 Philippines: 2 Portugal: 3 Romania: 3 South Africa: 1 Switzerland: 1 Thailand: 2 Turkey: 2 UK: 8 U.S.: 127 Zaire: 1 **TOTAL: 191**	Shared Personal Info with Unauthorized Third Party: 2 Targeted Advertising: 2 Unable to Contact Participating Site: 31 Unable to Unsubscribe: 14 Unauthorized Profile With My Information: 2 Undefined/Incomprehensible: 10 **TOTAL: 191**

Complaint Process Quality Measures

These statistics are drawn from TRUSTe's internal Dispute Resolution program. This process begins with a consumer complaint filed against a CBPR Participant either with the company, or with TRUSTe. After TRUSTe receives a complaint, we initiate an investigation. TRUSTe then reviews the complaint to determine if the complaint is relevant and falls under the scope of the Program Requirements. This initial review can take up to 10 business days. The consumer (complainant) receives TRUSTe's initial response within 10 business days, our published time frame (available at https://feedback-form.truste.com/watchdog/request). 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. Once the complaint is resolved, TRUSTe will send an email notice to both the complainant and, if participating, the Participant, notifying them of closure of the complaint. TRUSTe asks the complainant to provide consent before TRUSTe shares their personal information with the CBPR Participant the complainant is filing a dispute about. All personal information collected during the request for assistance is collected in accordance with TRUSTe's Privacy Policy (available at https://www.truste.com/privacy-policy).

CASE NOTES

CASE NOTE 1

Citation: *Unsubscribe Request, 2017, TRUSTe, Case Note 1*

Case Report

Facts: Using TRUSTe's dispute resolution process, Complainant informed TRUSTe that they received unsolicited email from Participant after having registered to unsubscribe from such email. A member of TRUSTe's compliance team requested more information from Complainant, including a copy of a message sent by Participant after unsubscribing, including headers. Complainant provided the information at which time TRUSTe notified Participant of the issue (after having first obtained Complainant's consent to do so). Within 3 business days of the complainant initially filing their request, Participant replied indicating that they deleted the address and asked the consumer to allow a few days for it to propagate across their system. Participant also requested a copy of the most recent message the consumer received so they can check the unsubscribe link. Complainant sent the requested information to the Participant. TRUSTe notified the Complainant and Participant that the ticket would remain open for 2 week in case either party had any additional questions for other or comments. After allowing the Parties 2 weeks to respond with further comments, TRUSTe closed the complaint. This process took approximately 3 weeks from notification to final resolution.

Law (*Excerpted from the United States' 2012 Application to Join the APEC CBPR System*): The FTC enforces Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits unfair or deceptive acts or practices in or affecting commerce. An act or practice is deceptive if it is likely to mislead a consumer acting reasonably under the circumstances and is likely to affect a consumer's conduct or decision regarding a product or service. An act or practice is unfair when it causes, or is likely to cause, substantial injury to consumers that (i) is not reasonably avoidable by consumers themselves; and (ii) is not outweighed by countervailing benefits to consumers or to competition. A company that joins the APEC CBPRs must publicly declare that it will comply with the CBPR program requirements and must make these program requirements publicly accessible. If the company fails to comply with any of these program requirements, its public representation of compliance may constitute an unfair or deceptive act or practice subject to Section 5 enforcement. If a company engages in any of the following practices it may violate Section 5 of the FTC Act, 15 U.S.C. § 45 and be subject to an enforcement action: a. Making a public representation relating to the notice requirements and failing to comply with the representation; b. displaying a seal, trustmark or other symbol on the company's website or on any other of its own publicly available documentation that indicates that it participates in the APEC CBPRs and thus complies with the notice requirements and failing to comply; or c. causing the company's name to appear on a list of companies that are certified for participation in the APEC CBPRs (e.g., lists on the websites of participating government authorities, privacy enforcement

authorities, APEC-recognized Accountability Agents, or on an APEC website specifically dedicated to the operation of APEC Cross-Border Privacy Rules) thereby indicating that it complies with the notice requirements and failing to comply.

Discussion: The issues raised in this instance involve the following CBPR program requirements:

1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)?

15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information?

In addition to Participant's legal obligation to comply with its stated privacy practices under the FTC's Section 5 authority, 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 (see Appendix G). This is reflected in TRUSTe's MSA, section 4.2.1: "If participating in a TRUSTe Assurance Program, Customer shall fully comply with the additional provisions set forth in an applicable Order." This case illustrates how TRUSTe uses our Feedback and Resolution system to facilitate consumer unsubscribe requests according to the process reviewed by TRUSTe at the time of certification. Ultimately, Complainant's issue was successfully resolved using this process and no further action was required.

CASE NOTE 2

Citation: *Unauthorized Account Creation, Unauthorized Email Use, 2017, TRUSTe, Case Note 2*

Case Report

Facts:

Using TRUSTe's dispute resolution process, Complainant informed TRUSTe that an unauthorized account was created on Participant's website using their e-mail address. Complainant requested deletion of the account and deletion of their email address. Complainant indicated that they had contacted the Participant less than 24 hours before filing the complaint in TRUSTe's system. TRUSTe replied within a day making sure the consumer had Participant's privacy escalation email and asked the Complainant to reply within 2 weeks if the Participant did not resolve the issue within that timeframe.

Complainant responded 12 days later asking for further assistance from TRUSTe. Several days later, TRUSTe escalated the issue with the Participant's privacy escalations contact (after having

first obtained Complainant's consent to do so). 8 days later, Participant replied that they had since closed the account and deleted the email address as requested. TRUSTe notified the Complainant and Participant that the ticket would remain open for 2 weeks in case either party had any additional questions for other or comments. After allowing the Parties 2 weeks to respond with further comments, TRUSTe closed the complaint. This process took approximately 3 weeks from notification to final resolution.

Law (*Excerpted from the United States' 2012 Application to Join the APEC CBPR System*): The FTC enforces Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits unfair or deceptive acts or practices in or affecting commerce. An act or practice is deceptive if it is likely to mislead a consumer acting reasonably under the circumstances and is likely to affect a consumer's conduct or decision regarding a product or service. An act or practice is unfair when it causes, or is likely to cause, substantial injury to consumers that (i) is not reasonably avoidable by consumers themselves; and (ii) is not outweighed by countervailing benefits to consumers or to competition. A company that joins the APEC CBPRs must publicly declare that it will comply with the CBPR program requirements and must make them publicly accessible. If the company fails to comply with any of these program requirements, its public representation of compliance may constitute an unfair or deceptive act or practice subject to Section 5 enforcement. If a company engages in any of the following practices it may violate Section 5 of the FTC Act, 15 U.S.C. § 45 and be subject to an enforcement action: a. Making a public representation relating to the notice requirements and failing to comply with the representation; b. displaying a seal, trustmark or other symbol on the company's website or on any other of its own publicly available documentation that indicates that it participates in the APEC CBPRs and thus complies with the notice requirements and failing to comply; or c. causing the company's name to appear on a list of companies that are certified for participation in the APEC CBPRs (e.g., lists on the websites of participating government authorities, privacy enforcement authorities, APEC-recognized Accountability Agents, or on an APEC website specifically dedicated to the operation of APEC Cross-Border Privacy Rules) thereby indicating that it complies with the notice requirements and failing to comply.

Discussion: The issues raised in this instance involve several CBPR program requirements, including:

1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)?

15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information?

22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.

37. Upon request, do you provide individuals access to the personal information that you hold about them?
    a) Do you take steps to confirm the identity of the individual requesting access?
    b) Do you provide access within a reasonable time frame following an individual's request for access?
    c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)?
    d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)?
    e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.

38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e).
    a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary.
    b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion?
    c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion?
    d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted?
    e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?

In addition to the Participant's legal obligation to comply with its stated privacy practices under the FTC's Section 5 authority, 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 (see Appendix G). This is reflected in TRUSTe's MSA, section 4.2.1: "If participating in a TRUSTe Assurance Program, Customer shall fully comply with the additional provisions set forth in an applicable Order." As part of Participant's CBPR certification, TRUSTe verified that Participant had the necessary policies and practices to implement each CBPR program requirement, including Program Requirements 1, 15, 22, 37 and 38. In this instance, TRUSTe ensured that those policies were implemented to resolve Complainant's deletion request.