EXECUTIVE SUMMARY

This annual report of TRUSTe LLC (TRUSTe), a subsidiary of TrustArc Inc, summarizes the Privacy Shield Services of TRUSTe in its fourth year of operation for the reporting period August 1, 2019 through July 31, 2020. TRUSTe operates two core Privacy Shield services covered by this report for both the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Framework. These services include:

- An Independent Recourse Mechanism: TRUSTe Dispute Resolution
- Privacy Shield Compliance Verification

Participation in the TRUSTe Privacy Shield Services during this reporting period included:

<table>
<thead>
<tr>
<th>Service</th>
<th>Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUSTe Dispute Resolution Only</td>
<td>266</td>
</tr>
<tr>
<td>EU-U.S. Privacy Shield Verification</td>
<td>372</td>
</tr>
<tr>
<td>EU-U.S. Privacy Shield Verification HR Data Only</td>
<td>53</td>
</tr>
<tr>
<td>Swiss-U.S. Privacy Shield Verification</td>
<td>299</td>
</tr>
<tr>
<td>Swiss-U.S. Privacy Shield Verification HR Data Only</td>
<td>42</td>
</tr>
</tbody>
</table>

Among the participants in the TRUSTe Privacy Shield Services during the period, 32 transitioned to inactive status on the Privacy Shield list during the period, including 11 of the Verification and Dispute Resolution participants and 21 of the Dispute Resolution only participants.
The most significant development during the period involved the July 16, 2020 invalidation by the Court of Justice of the European Union (CJEU) of the European Commission Decision on the adequacy of the EU-U.S. Privacy Shield (Case C-311/18). In response to the CJEU judgment, TRUSTe, and its parent company TrustArc Inc, provided complimentary education and resources to participants in the TRUSTe Privacy Shield Services including:

- A microsite with one-stop access to the CJEU ruling, Privacy Shield Update FAQs, EDPB FAQs, and a table of regulator responses, a podcast, blog series, and FAQs
- Ongoing operation of the Privacy Shield Services to support participants’ continued compliance with the Privacy Shield principles
- Technology resources to evaluate and assess data flows, identify alternative data transfer mechanisms, and address implementation gaps
- Operational templates for implementation of supplemental measures and alternative data transfer mechanisms
- Provision of an alternative International Privacy Verification Program for verification of ongoing compliance with the Privacy Shield principles for participants that elect to withdraw from participation in the EU-U.S. Privacy Shield Framework
- A participant webinar series and consultations on Privacy Shield to provide assistance with understanding and responding to the outcomes of the CJEU judgment
REPORT OVERVIEW

This report includes information about:

- The Privacy Shield Services that TRUSTe operates, including how we avoid conflicts of interest
- Participation in TRUSTe Privacy Shield Compliance Verification
- Participation in TRUSTe Dispute Resolution
- How complaints can be filed with TRUSTe
- Privacy Shield complaint eligibility
- TRUSTe complaint handling process
- Privacy Shield complaint statistics and case summaries
TRUSTe PRIVACY SHIELD SERVICES

Privacy Shield Roles Served By TRUSTe
TRUSTe provides various external privacy compliance review programs for organizations seeking an independent review of whether they have met a particular privacy standard or set of privacy requirements. One of the programs we provide to organizations is an outside review of Privacy Shield compliance in accordance with Privacy Shield Supplemental Principle 7(d), which we call “Privacy Shield Verification.” More details on this service are provided below. A separate team at TRUSTe, which operates independently from the team conducting outside compliance reviews, provides dispute resolution services, including dispute resolution services in fulfillment of a Privacy Shield Participant’s IRM obligations. Participants may utilize TRUSTe as an IRM without using TRUSTe as an outside compliance reviewer.

TRUSTe adheres to a Corporate Policy on Conflict of Interests, which requires segregation of duties between the team responsible for outside compliance reviews and the team responsible for dispute resolution services. The Global Privacy Solutions team conducting the outside compliance reviews reports to the SVP, Global Privacy Solutions, and the Compliance team that provides dispute resolution services reports to the SVP and Chief Financial Officer. The routine processes and systems used by these teams do not overlap. Oversight of the program is led by the SVP, Privacy Intelligence and General Counsel with support from the Privacy Intelligence team, including the Office of General Counsel. Governance of the programs is coordinated among the aforementioned executive team members and the CEO.

In addition to these services, TRUSTe offers individual consultations through our Privacy Shield Assessment Service, whereby a member of the Global Privacy Solutions team assists a prospective Privacy Shield Participant in its evaluation of its privacy policies and practices against the Privacy Shield Principles. A findings report and action plan is then delivered, which includes a gap analysis and remediation recommendations.¹

TRUSTe also provides publically-available FAQs in accordance with Privacy Shield Supplemental Principle 11(d)(ii)² as well as a series of Privacy Shield-related blog posts.³ Since the Privacy Shield Frameworks were announced, TRUSTe has hosted multiple webinars on Privacy Shield, including with the U.S. Department of Commerce, and has presented at the First and Third Annual Joint Reviews of the EU-U.S. Privacy Shield Framework.

### During the Reporting Period

<table>
<thead>
<tr>
<th>Dispute Resolution Participants:</th>
<th>Privacy Shield Compliance Verification Participants:</th>
</tr>
</thead>
<tbody>
<tr>
<td>638</td>
<td>425</td>
</tr>
</tbody>
</table>

### End of the Reporting Period

<table>
<thead>
<tr>
<th>Dispute Resolution Participants:</th>
<th>Privacy Shield Compliance Verification Participants:</th>
</tr>
</thead>
<tbody>
<tr>
<td>598</td>
<td>380</td>
</tr>
</tbody>
</table>

¹ This analysis does not constitute an outside compliance review as the prospective Participants using this assessment-only service have opted to instead use the self-assessment verification methodology, utilizing the remediation recommendations received via the service guidance for their own determination of compliance.
³ [https://trustarc.com/blog/?s=privacy+shield](https://trustarc.com/blog/?s=privacy+shield)
PARTICIPATION IN TRUSTe PRIVACY SHIELD COMPLIANCE VERIFICATION

TRUSTe offers outside compliance reviews in accordance with Supplemental Principle 7 - Verification. In order to participate in the TRUSTe Privacy Shield Compliance Verification program, a Participant must be a U.S. legal entity subject to the jurisdiction of either the Federal Trade Commission or the Department of Transportation, agree to be assessed for compliance with the Privacy Shield Principles in accordance with the TRUSTe EU-U.S. and Swiss-U.S. Privacy Shield Verification Program Assessment Criteria, and agree to comply with the TRUSTe Assurance Program Governance Standards.

Verification Process

The TRUSTe Verification Process involves three steps:

Assessment: TRUSTe performs an initial assessment of compliance.

Remediation and Verification: TRUSTe provides a comprehensive report and action plan to program applicants outlining our findings regarding compliance with the Privacy Shield Principles. TRUSTe then verifies that the required changes provided in the report and action plan have been properly implemented.

Monitor: TRUSTe verifies ongoing compliance with the Assessment Criteria and Assurance Program Governance Standards.

Upon successful completion of the TRUSTe assessment and verification process, and completion of Privacy Shield self-certification with the U.S. Department of Commerce indicating TRUSTe as its outside compliance reviewer, Participants in the TRUSTe Privacy Shield Compliance Verification program are issued and authorized to display the TRUSTe Privacy Shield Verification program seal.

Compliance Monitoring

After a Participant completes its self-certification and appears on the Active Privacy Shield List, TRUSTe uses a combination of approaches to monitor compliance with the requirements for participation in the TRUSTe Privacy Shield Compliance Verification program, including continued adherence to the Privacy Shield Verification Program Assessment Criteria and the TRUSTe Assurance Program Governance Standards. The extent to which one method is utilized over

---

4 Available online at https://download.trustarc.com/dload.php?f=KQG6QJS3-740
5 Available online at https://download.trustarc.com/?f=4OB4NEWY-742
another is dependent on the Participant’s risk profile and particular business practices. These methods may include:

**Web Crawling:** TrustArc Proprietary technology is utilized by TRUSTe to perform website analysis for data collection and cookie identification.

**Traffic Analysis:** A device testing process primarily used to verify mobile device compliance.

**TRUSTe Feedback and Resolution System:** Defined in detail in the section below on TRUSTe Dispute Resolution, TRUSTe investigations may also be initiated after a TRUSTe scan, a media report, regulator inquiry or information obtained through other credible sources.

**Compliance Investigations**

Beyond compliance monitoring, TRUSTe also has a review process to investigate a suspected breach of the Privacy Shield Verification Program Assessment Criteria and the TRUSTe Assurance Program Governance Standards. This process is led by the Compliance team, which reports to the SVP and Chief Financial Officer, and is typically conducted under the direction of the SVP, Privacy Intelligence and General Counsel. It begins with an internal compliance investigation. TRUSTe may initiate this investigation based on results of our monitoring, based on information contained in a consumer complaint, media reports, regulator inquiries, or reports from other credible sources. Where non-compliance with the requirements set forth in the Privacy Shield Verification Program Assessment Criteria and the TRUSTe Assurance Program Governance Standards is found, TRUSTe will investigate the compliance issue, notify the Participant, outline the necessary corrections, and provide a reasonable timeframe for the Participant to make such changes, during which time TRUSTe works with the Participant to ensure the necessary changes are made. TRUSTe compliance investigations may result in one of the following three outcomes:

**Agreement and Resolution:** An agreement between TRUSTe and the Participant over the privacy complaint resulting in resolution by the Participant that addresses the concern or request. TRUSTe provides a reasonable timeframe to complete the required changes based on the risk and level of non-compliance.

**Formal Enforcement:** A disagreement triggering a notice of formal enforcement, resulting in the Participant’s suspension or notice of intent to terminate for cause if the matter is not cured.
Termination: A failure to implement the required cure resulting in TRUSTe terminating the Participant from the program, and in extreme cases, publication and/or referral to the appropriate authority.

Participation
TRUSTe provides a weekly list of Participants to the Department of Commerce. As of the close of this annual reporting period, the following number of Participants had been verified, either as a stand-alone service for HR Data (52 Participants, with 51 also seeking verification for Non-HR Data), or for Non-HR Data, in combination with TRUSTe dispute resolution.

Privacy Shield Compliance Verification Participants:
380
PARTICIPATION IN TRUSTe DISPUTE RESOLUTION

TRUSTe offers dispute resolution services in fulfillment of a participant’s Independent Recourse Mechanism obligations set forth in Principle 7 - Recourse, Enforcement, and Liability and Supplemental Principle 11 - Dispute Resolution and Enforcement. In order to participate in the TRUSTe Privacy Shield Dispute Resolution program, a Participant must be a U.S. legal entity subject to the jurisdiction of either the Federal Trade Commission or the Department of Transportation and agree to the TRUSTe Dispute Resolution Procedures, which in summary include:

- At the time of agreement, or as soon as practicable thereafter, provide a copy of the privacy notice(s) applicable to its participation in the Privacy Shield Frameworks
- Provide individuals with simple means to submit complaints and express their concerns regarding the Participant’s privacy practices and respond timely to submissions
- Cooperate with TRUSTe to resolve complaints, disputes, questions, and concerns in accordance with the detailed process described in the TRUSTe Privacy Dispute Resolution FAQs
- Communicate with the complainant in the manner preferred by that individual
- Abide by the dispute eligibility determinations of TRUSTe
- Timely acknowledge and respond to applicable inquiries from TRUSTe
- Submit to reviews to resolve disputes regarding its compliance with the applicable requirements as further described under Review Process described in the TRUSTe Privacy Compliance Verification section above

6 https://trustarc.com/consumer-info/dispute-resolution/dispute-resolution-faqs/
HOW COMPLAINTS CAN BE FILED WITH TRUSTe

TRUSTe provides privacy resources for consumers related to Privacy Shield online,\(^7\) including access to the following:

- An online form to file a complaint
- Dispute Resolution FAQs
- Privacy Shield Supplemental Principle 11)d) on Recourse Mechanisms
- Access to PrivacyShield.gov
- Access to TRUSTe Annual Privacy Shield Reports

Filing a complaint requires just two simple steps:

### Step 1

A Privacy Shield-related complaint can be filed by a consumer by either clicking the “Privacy Feedback” button or directly through [https://feedback-form.truste.com/watchdog/request](https://feedback-form.truste.com/watchdog/request), based on which mechanism is made available by the Participant in its privacy notice. All TRUSTe Privacy Shield Dispute Resolution Participants are required to display either the foregoing link or the Privacy Feedback button to the right as a condition of participation.

### Step 2

The complainant must then provide the following information as requested in the feedback form:

- The name of the Participant the complainant wishes to report (including the site URL)
- The complaint type as provided in a drop down menu
- A narrative description of the issue

\(^7\) [https://trustarc.com/consumer-info/privacy-shield/](https://trustarc.com/consumer-info/privacy-shield/)
<table>
<thead>
<tr>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ The date when the complainant attempted to contact the Participant regarding the listed concern&lt;sup&gt;8&lt;/sup&gt;</td>
</tr>
<tr>
<td>✓ The Participant’s response</td>
</tr>
<tr>
<td>✓ The resolution sought by the complainant</td>
</tr>
<tr>
<td>✓ The complainant’s email address&lt;sup&gt;9&lt;/sup&gt;</td>
</tr>
<tr>
<td>✓ The complainant’s name&lt;sup&gt;10&lt;/sup&gt;</td>
</tr>
<tr>
<td>✓ The complainant’s country</td>
</tr>
<tr>
<td>✓ Permission for TRUSTe to share the information provided by the complainant with the Participant in question in order to resolve the issue&lt;sup&gt;11&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

<sup>8</sup> Before submitting a complaint to TRUSTe, a complainant should attempt to contact the Participant directly to allow them to resolve the concern.

<sup>9</sup> If the complainant wishes to receive a response or be reachable for questions and updates, they must provide a working email address where they can receive email. Certain requests, such as those related to a specific action affecting the complainant may be unable to be resolved without being able to provide identifying information to the Participant about whom the complaint is made.

<sup>10</sup> Complainants are welcome to use their real name or use a “No Name” option if they prefer.

<sup>11</sup> Refusal to provide permission may limit the ability of the named Participant to address the stated concern.
PRIVACY SHIELD COMPLAINT ELIGIBILITY

General Eligibility
In order for a complaint to be considered eligible for resolution by TRUSTe, all of the following 6 conditions must be met:

✓ The complaint is about an organization that either is a Participant in a TRUSTe Assurance Program who holds an authentic TRUSTe seal or is a Participant in a TRUSTe Dispute Resolution program
✓ The complainant has already made a good faith attempt to resolve the problem directly with the Participant
✓ The complaint raises a privacy issue that affects the Personal Information of either the complaint or of a child whose parent or guardian is the complainant
✓ The complaint alleges that the Participant collected, used, or disclosed the Personal Information in a manner inconsistent with its published Privacy Notice
✓ The complaint is in English or the Participant has secured appropriate translation services
✓ The complaint is submitted to TRUSTe via the online TRUSTe Dispute Resolution form

Determination of Privacy Shield-Related Complaints
For purposes of the statistics provided in this report, a complaint must further meet the following criteria to be considered an eligible Privacy Shield-related complaint:

✓ The complainant is an EEA or Swiss individual (i.e., the individual submitting on his or her own behalf or on behalf of a minor of whom the individual is a parent or guardian)
✓ The complaint concerns a Participant in the TRUSTe Privacy Shield Dispute Resolution program;
✓ The complaint concerns an organization participating in a Department of Commerce-administered Privacy Shield program; and
✓ The complaint alleges that an organization has violated the Privacy Shield Principles with respect to the complainant’s own Personal Information or the Personal Information of a minor of whom the complainant is the parent or guardian.

COMPLAINT OVERVIEW

<table>
<thead>
<tr>
<th>Complaints Received from Individuals Worldwide</th>
<th>Complaints Received from Individuals in the EEA and Switzerland</th>
<th>Privacy Shield-Related Complaints Addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>7911</td>
<td>266</td>
<td>8</td>
</tr>
</tbody>
</table>

12 Data about an identified or identifiable individual
13 https://feedback-form.truste.com/watchdog/request
14 TRUSTe included within scope all EEA countries: EU Member States, Norway, Iceland and Liechtenstein
TRUSTe COMPLAINT HANDLING PROCESS

Following receipt of a Dispute Resolution request, TRUSTe will inform the filing complainant within ten (10) business days as to whether the complaint meets the eligibility requirements or whether TRUSTe needs further information to make such a determination. If further information is needed, a complainant has fourteen (14) calendar days from the date of TRUSTe’s request to provide this additional information. If TRUSTe determines that the complaint is ineligible, the complainant will be emailed a written notification. If the complaint is deemed eligible, TRUSTe will request a response from the Participant within fourteen (14) calendar days.

Once TRUSTe has made a final determination about the complaint, it will inform the complainant and, if applicable, the Participant. At that time, either party has fourteen (14) calendar days to file an appeal. Upon receiving an appeal, TRUSTe’s Compliance Director will review the appeal and determine within ten (10) business days whether the complaint is eligible to be reopened for further investigation. After TRUSTe’s Compliance Director completes review of the appeal request, TRUSTe may direct the other party to respond by email within ten (10) business days thereafter, explaining why TRUSTe’s final determination should be sustained, or supplying responses to specific questions from TRUSTe. If TRUSTe’s Compliance Director determines that the original complaint disposition was proper according to TRUSTe’s processes, and introduces no substantive new information that could not have been raised earlier, or finds no other basis for appeal, the Compliance Director will request review by the General Counsel, or her Legal designee, of the issue appealed, and TRUSTe will respond with its final appeals determination within ten (10) business days. If a Participant fails to answer a question with a timely response, TRUSTe will send a second notice to the Participant and attempt phone notification. If the issue remains unresolved, TRUSTe will withdraw or suspend the Participant’s use of TRUSTe Dispute Resolution Services, notify the Department of Commerce of the organization’s failure to comply, and/or take other action as necessary, including referral to the appropriate enforcement authority depending on the nature of the complaint.

Participation

As of the close of this annual reporting period, 598 Participants were enrolled in the TRUSTe Privacy Shield Dispute Resolution Service. This included 270 participants in TRUSTe Dispute Resolution only and 328 participants in TRUSTe Compliance with Dispute Resolution for Non-HR Data.
PRIVACY SHIELD COMPLAINT STATISTICS AND CASES

From August 1, 2019 through July 31, 2020, TRUSTe handled 7911 complaints from individuals worldwide. The geographic distribution of the origin of complaints received is set forth in the charts below.

Complaints Handled by Region and Country of Origin

Of the 266 complaints that originated in the EEA and Switzerland, the breakdown by county was:

<table>
<thead>
<tr>
<th>Country</th>
<th>Complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria (AT)</td>
<td>4</td>
</tr>
<tr>
<td>Belgium (BE)</td>
<td>5</td>
</tr>
<tr>
<td>Bulgaria (BG)</td>
<td>3</td>
</tr>
<tr>
<td>Czech Republic (CZ)</td>
<td>5</td>
</tr>
<tr>
<td>Denmark (DK)</td>
<td>2</td>
</tr>
<tr>
<td>Finland (FI)</td>
<td>4</td>
</tr>
<tr>
<td>France (FR)</td>
<td>28</td>
</tr>
<tr>
<td>Germany (DE)</td>
<td>15</td>
</tr>
<tr>
<td>Greece (GR)</td>
<td>2</td>
</tr>
<tr>
<td>Hungary (HU)</td>
<td>2</td>
</tr>
<tr>
<td>Iceland (IS)</td>
<td>1</td>
</tr>
<tr>
<td>Italy (IT)</td>
<td>19</td>
</tr>
<tr>
<td>Lithuania (LT)</td>
<td>4</td>
</tr>
<tr>
<td>Netherlands (NL)</td>
<td>13</td>
</tr>
<tr>
<td>Norway (NO)</td>
<td>2</td>
</tr>
<tr>
<td>Poland (PL)</td>
<td>19</td>
</tr>
<tr>
<td>Portugal (PT)</td>
<td>1</td>
</tr>
<tr>
<td>Romania (RO)</td>
<td>9</td>
</tr>
<tr>
<td>Sweden (SE)</td>
<td>9</td>
</tr>
<tr>
<td>Spain (ES)</td>
<td>59</td>
</tr>
<tr>
<td>Switzerland (CH)</td>
<td>0</td>
</tr>
</tbody>
</table>

Of the 266 complaints originating from individuals in the EEA, 98 complaints involved a TRUSTe Privacy Shield Dispute Resolution Participant company or property. Distribution of complaints received by month are shown below.

© 2020 TrustArc Inc | US 888.878.7830 | EU +44 (0)203.078.6495 | www.trustarc.com
Privacy Shield-Related Complaints

Of the 98 complaints received from individuals in the EEA, 8 involved requests eligible for resolution. Ineligible complaints include issues where:

- **Subject matter**: The subject matter of the request was not eligible, such as billing requests not alleging an eligible issue, where the individual seeks to access information or make data changes about another individual for whom the complainant is not the parent or guardian, or the issue was incomprehensible, such as random typing.
- **Procedural grounds**: The complaint was closed on procedural grounds such as duplicates, where the individual withheld consent for TRUSTe to share his or her identity to allow the Participant to research the issue, where the complainant failed to contact the Participant, where the complaint was misfiled against a Participant when the complaint related to another company, or where the complainant dropped the request.

All 8 complaints were resolved during the reporting period. Summaries of each case and its resolution are described further below. Among the 8 cases:

- 5 raised concerns related to Privacy Principle 6 - **Access**, primarily regarding data deletion
- 1 raised a concern related to Privacy Principle 1 - **Notice**
- 1 raised a concern related to Privacy Principle 2 - **Choice**
- 1 raised a concern related to Privacy Principle 4 - **Security**

### Case Summaries

#### Access Cases

**Case 1** - An individual raised concerns about how the Participant obtained Personal Information about them and requested deletion. The case was resolved by the Participant providing the requested information and arranging deletion. *Days until final determination: 20.*

**Case 2** - An individual requested account and data deletion. The Participant involved closed the individual’s account and provided an explanation for the necessity of retaining the Personal Information. *Days until final determination: 16.*

**Case 3** - An individual requested data deletion while wanting to continue to use the Participant’s online services. The Participant deactivated the account, explained its data retention policies, the legal obligations that prevented it from honoring certain aspects of the deletion request at this time, and its
commitment to deletion of the data at the end of the retention period. Days until final determination: 35.

**Case 4** - An individual requested deletion of online account data by the Participant in follow up to a prior request that resulted in account suspended status rather than account deletion. The Participant confirmed within twenty-two (22) days that the data had been deleted, provided an explanation of its processes, and apologized to the complainant for the confusion. The individual responded with further process feedback for the Participant, to which the Participant responded. Days until final determination: 41.

**Case 5** - An individual requested account and data deletion. The Participant involved explained that they had provided information about their updated self-service deletion option to the complainant. TRUSTe communicated the Participant’s explanation to the complainant and provided instructions on how to follow up with TRUSTe if the complainant did not view the issue to be resolved. No further communication was received from the complainant. Days until final determination: 32.

**Notice Case**

**Case 6** - An individual raised a concern about the lack of information in email messages sent by the Participant on behalf of UK-based data controllers regarding the identity of such organizations, about whom the complainant also questioned the lawfulness of such organizations’ transfer of personal information out of the EEA to Participant. This issue was resolved based on communications between TRUSTe and the complainant and also between TRUSTe and the Participant regarding the information and data transfer responsibility being with the UK-based data controller, which was not a party to the Privacy Shield complaint to TRUSTe. Days until final determination: 64.

**Choice Case**

**Case 7** - An individual requested that his account with the Participant be closed and that Participant refund certain transactions he indicated were authorized by his child under the age of thirteen (13). The Participant closed the account. Additionally, the Participant provided documentation to TRUSTe regarding: (1) the date on which the complainant had provided affirmative written consent to the Participant for his child’s use, and (2) the complainant’s request to Participant for assistance related to his child’s continued use of the account, as well as his expression of appreciation for the assistance. Based on the evidence provided, TRUSTe resolved the Choice concern in favor of the Participant, and notified the complainant that the issue regarding a refund from the Participant is outside of the scope of TRUSTe’s privacy Dispute Resolution authority. Days until final determination: 77.

**Security Case**

**Case 8** - An individual raised a concern that a representative of the Participant requested that the individual send credit card information to the Participant via unsecure email. The complainant informed TRUSTe that he refused to provide his credit card information via an unsecured connection and requested correction of this practice. The Participant responded with information about the launch of its new secure payment system and explained that the Participant’s local management team had contacted the complainant to address the issue. Days until final determination: 16.

---

15 For further details regarding TRUSTe’s Dispute Resolution Authority, please refer to the sections above on Participation in TRUSTe Dispute Resolution.
Dispute Resolution Quality Measures

The complaint statistics and cases are drawn from our internal TRUSTe Dispute Resolution program. The average initial response time for the Complaints received under the TRUSTe Privacy Shield Dispute Resolution program was nineteen (19) hours.

As described in the section above on the TRUSTe Complaint Handling Process, once a complaint has been reviewed and referred to the Participant for response, the Participant ordinarily has ten (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. If a Participant fails to answer a complaint with a timely response, TRUSTe will send a second notice to the Participant and attempt additional outreach, including phone notification. If the issue remains unresolved, TRUSTe will:

- Withdraw or suspend the Participant’s use of Dispute Resolution services;
- Notify the Department of Commerce of the organization’s failure to comply; and/or
- Take other action as necessary, including referral to the appropriate enforcement authority depending on the nature of the complaint.

No complaints received during the reporting period required escalation due to a Participant’s failure to resolve. The average resolution time for Privacy Shield complaints received during the reporting period was 37 business days. For complaints eligible for resolution (excluding those closed on procedural grounds as described above), TRUSTe notifies the complainant and, if applicable, the Participant of the resolution. In all instances, TRUSTe asked the complainant to provide consent before sharing Personal Information about them with the Participant in question. All Personal Information collected during the Dispute Resolution process is handled in accordance with the TrustArc Privacy Policy (available at https://www.trustarc.com/privacy-policy/).
ABOUT TRUSTARC

TrustArc automates the creation of end-to-end privacy management programs for global organizations. As the leader in privacy compliance and data protection, TrustArc is the only company to deliver the depth of privacy intelligence that’s essential for the growing number of privacy regulations in an ever-changing digital world. TrustArc powers privacy compliance and risk management with integrated technology, consulting and TRUSTe certification solutions – addressing all phases of privacy program management.

Headquartered in San Francisco, and backed by a global team across the Americas, Europe, and Asia, TrustArc helps customers worldwide demonstrate compliance, minimize risk and build trust. For additional information visit www.trustarc.com.

TRUSTe Assurance Programs, such as our Privacy Shield Compliance Verification Program and our TRUSTe Dispute Resolution services, are provided by TRUSTe LLC, a Delaware limited liability company and a wholly owned subsidiary of TrustArc Inc.

Questions regarding this report should be directed to the Office of General Counsel at legal@trustarc.com