1823189

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Joseph J. Simons, Chairman
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of RagingWire Data Centers, Inc., a corporation.

DOCKET NO. 9386

COMPLAINT

The Federal Trade Commission ("FTC"), having reason to believe that RagingWire Data Centers, Inc., a corporation, has violated the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent RagingWire Data Centers, Inc. ("RagingWire") is a Nevada corporation with its principal office or place of business at 200 S. Virginia Street, 8th Floor, Reno, NV 89501.

2. RagingWire provides data colocation services. Specifically, RagingWire offers specialized storage facilities—often referred to as "data centers"—that are designed to house and protect servers owned and operated by other businesses, along with complementary services including on-site technical support, network connectivity, and physical security.

3. The acts and practices of RagingWire as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act.

4. As described in more detail below, RagingWire has made deceptive statements on its website, https://www.ragingwire.com/content/online-privacy-policy, and in its marketing materials, about its participation in and compliance with the U.S.-E.U. Privacy Shield Framework and/or EU-U.S. Safe Harbor Framework.

Personal Data Transfers Under European Union Law

5. The EU-U.S. Privacy Shield Framework ("Privacy Shield") was negotiated by the Department of Commerce ("Commerce") and the European Commission ("EC") to provide a mechanism for companies to transfer personal data from the European Union ("EU") to the U.S. in a manner consistent with the requirements of European Union law on data protection. Enacted in 1995, the EU Data Protection Directive set forth EU requirements for the protection of personal data. Among other things, it required EU Member States to implement legislation that prohibits the transfer of personal data outside the EU, with exceptions, unless the European Commission has made a determination that the recipient jurisdiction's laws ensure the protection of such personal data. This determination is referred to commonly as meeting the EU's "adequacy" standard.

6. The EU has since enacted a new data protection regime, the General Data Protection Regulation ("GDPR"), which took effect as of May 25, 2018, and contains similar provisions on data transfers. The GDPR explicitly recognizes EC adequacy determinations in effect as of that date. Unlike the Directive, the GDPR is directly applicable and generally does not requ (et)-6 (er)-(u)-4

Shield are obligated to provide at least the same level of privacy protection as is required by the Principles

20. From approximately January 2017 until October 2018, RagingWire disseminated or caused to be disseminated the following representations in its online privacy policy, available at https://www.ragingwire.com/content/online-privacy-policy, including, but not limited to, statements that it participated in and complied with the EU-U.S. Privacy Shield (the "Privacy Shield Statements"):

> EU-U.S. Privacy Shield
> RagingWire complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. RagingWire has certified that it adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/
>
> The Federal Trade Commission (FTC) has jurisdiction over RagingWire's compliance with the Privacy Shield.
>
> DISPUTE RESOLUTION
>
> In compliance with the EU-US Privacy Shield Principles, RagingWire commits to resolve complaints about your privacy and our collection or use of your personal information. . . .If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our US-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request. Please note that if your complaint is not resolved through these channels, under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel.

21. RagingWire also has disseminated or caused to be disseminated sales materials containing representations that RagingWire was a participant in Privacy Shield and/or the Safe Harbor Framework after it was no longer participating in the frameworks. For example, RagingWire's marketing slides, the "Sales Tool Deck," represented in 2018 that RagingWire participated in the Safe Harbor Framework when, in fact, RagingWire no longer participated in the Safe Harbor Framework or Privacy Shield as of January 2018. A copy of this representation is attached hereto as Exhibit A.

22. Following the lapse of RagingWire's Privacy Shield certification in January 2018, Commerce warned the company in February 2018, and again in May 2018, to take down its claims that it participated in Privacy Shield unless and until such time as it completed the steps necessary to renew its participation in the EU-U.S. Privacy Shield Framework.

23. RagingWire did not remove its Privacy Shield Statements until October 2018, after RagingWire was contacted by the FTC.

24. In June 2019, RagingWire again applied for and obtained Privacy Shield certification.

RagingWire's Privacy Shield Non-Compliance

25. At least during the January 2017-18 period that RagingWire was a Privacy Shield participant, RagingWire failed to comply with the Privacy Shield Principles.

RagingWire's Failure to Verify Compliance

26. Supplemental Principle 7 of the Privacy Shield Principles requires a company that participates in Privacy Shield to annually verify, through self-assessment or outside compliance review, that the assertions it makes about its Privacy Shield privacy practices are true and that those privacy practices have been implemented.

27. Participants must also prepare a statement, signed by a corporate officer or outside reviewer, that such assessment or outside compliance review has been completed. Participants must make their annual verification statements

31. TRUSTe LLC ("TRUSTe"), a subsidiary of TrustArc Inc., offers a qualifying Privacy Shield dispute resolution mechanism. Privacy Shield participants may satisfy the requirements of Principle 7(a)(i) and Supplemental Principle 11(a) by participating in TRUSTe's dispute resolution program.

32. RagingWire contracted with TRUSTe to provide dispute resolution services.

33. Under the heading "Dispute Resolution," RagingWire's Privacy Shield Statements included a hyperlink to the private sector program developed by TRUSTe LLC. RagingWire's Privacy Shield Statements directed consumers to use that link to submit "unresolved privacy or data use concern[s]" to RagingWire's "U.S.-based third party dispute resolution provider."

34. However, RagingWire's subscription with TRUSTe was terminated as of October 1, 2017, and TRUSTe ceased providing dispute resolution services to RagingWire as of tisol or 0 Tc 0 Tw 2 (.

NOTICE

You are notified that on the seventh day of July, 2020, at 10:00 a.m., at the Federal Trade Commission Headquarters Building, 600 Pennsylvania Avenue, NW, Room 532-H, Washington, DC 20580, an Administrative Law Judge of the Federal Trade Commission, will hold a hearing on the charges set forth in this Complaint. At that time and place, you will have the right under the Federal Trade Commission Act to appear and show cause why an order should not be entered requiring you to cease and desist from the violations of law charged in this Complaint.

You are notified that you are afforded the opportunity to file with the Federal Trade Commission ("Commission") an answer to this Complaint on or before the 14th day after service of the Complaint upon you. An answer in which the allegations of the Complaint are contested must contain a concise statement of the facts constituting each ground of defense; and specific admission, denial, or explanation of each fact alleged in the Complaint or, if you are without knowledge thereof, a statement to that effect. Allegations of the Complaint not thus answered will be deemed to have been admitted.

If you elect not to contest the allegations of fact set forth in the Complaint, the answer should consist of a statement that you admit

The following is the form of the order which the Commission has reason to believe should issue if the facts are found to be as alleged in the Complaint. If, however, the Commission concludes from record facts developed in any adjudicative proceedings in this matter that the proposed order provisions as to Respondent might be inadequate to fully protect the consuming public, the Commission may order such other relief as it finds necessary and appropriate.

2. Protect the information by another means authorized under EU (for the EU-U.S. Privacy Shield Framework) or Swiss (for the Swiss-U.S. Privacy Shield Framework) law, including by using a binding corporate rule or a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the European Commission; or

3.

each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; or (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (14) days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E.

representation subject to this Order, and all materials that it relied upon in making the representation.

VI. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within ten (10) r ,(nt)]TJ -0.003 Tc 0. 31.69 0 Tat5.9 (m2 (n u03 Tc t())Tj 13 (T.48(d)-4 (a)-10 t)-2

upheld on appeal, then the order will terminate according to this Provision as though the complaint had never been made.