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 various 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 EU-U.S. 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 require member states to enact implementing legislation.

7. To satisfy the EU adequacy standard for certain commercial transfers, Commerce and the European Commission negotiated the EU-U.S. Privacy Shield Framework, which the European Commission determined was adequate by written decision in July 2016, and took effect August 1, 2016. Thus, the EU-U.S. Privacy Shield Framework allows for the transfer of personal data lawfully from the EU to those companies in the United States that participate in Privacy Shield.

8. The EU-U.S. Privacy Shield Framework replaced the U.S.-EU Safe Harbor Framework ("Safe Harbor Framework"), in effect from 2000-2016, as a lawful mechanism under EU law for transferring data from the EU to the United States.

9. To join the EU-U.S. Privacy Shield Framework, a company must self-certify to Commerce that it complies with the Privacy Shield Principles, and to related requirements that have been deemed to meet the EU's adequacy standard. Participating companies must annually recertify their compliance.

10. The EU-U.S. Privacy Shield Framework expressly provides that while decisions by organizations to "enter the Privacy Shield are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles ***must comply fully*** with the Principles." (Emphasis added.)

11. To comply with the Privacy Shield Principles, companies must, among other things, ascertain that any third-party agents to which they transfer data received pursuant to Privacy

Shield are obligated to provide at least the same level of privacy protection as is required by the Principles, as required by Privacy Shield Principle 3, "Accountability for Onward Transfer." One way to meet this requirement is to use an agent that is also a Privacy Shield participant.

12. Companies under the jurisdiction of the FTC are eligible to join the EU-U.S. Privacy Shield Framework. The framework expressly warns companies that claim to have self-certified to the Privacy Shield Principles that failure to comply or otherwise to "fully implement" the Privacy Shield Principles "is enforceable under Section 5 of the Federal Trade Commission Act."

13. The European Commission's adequacy decision expressly notes that, "to ensure the proper application of the EU-U.S. Privacy Shield Framework, interested parties, such as data subjects, data exporters and the national Data Protection Authorities (DPAs), must be able to identify those organisations adhering to the Principles." To that end, Commerce maintains a public website, https://www.privacyshield.gov, where it posts the names of companies that have self-certified to the EU-U.S. Privacy Shield Framework. The listing of companies, available at https://www.privacyshield.gov/list, indicates whether the company's self-certification is current. A U.S. company may only benefit from the EC adequacy decision while it is on the Department of Commerce's Privacy Shield list.

14. Under Article 83 of GDPR, transfers of personal information from the European Economic Area ("EEA") to the United States without the benefit of an authorized mechanism such as Privacy Shield are subject to severe penalties, including administrative fines of up to 20,000,000€ or 4% of the transferor's worldwide annual turnover from the preceding financial year, whichever is greater.

15. RagingWire is under the jurisdiction of the FTC.

RagingWire's Business Practices

16. RagingWire offers colocation services that store customer data at one of three data centers located in the United States. RagingWire customers that collect or process personal information from the EEA and want to transfer that data to RagingWire in the U.S. can comply with GDPR and/or their own Privacy Shield obligations if RagingWire participates in Privacy Shield.

17. RagingWire originally participated in the Safe Harbor Framework, and submitted its final annual recertification for the Safe Harbor Framework on June 16, 2016.

18. RagingWire submitted a Privacy Shield self-certification application in approximately October 2016. It obtained Privacy Shield certification in January 2017.

19. One year later, RagingWire did not complete the steps necessary to renew its Privacy Shield certification, and its Privacy Shield certification lapsed in January 2018.

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 U.S.-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 Tour 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 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 any 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 available on request to the FTC or Department of Transportation, whoever has unfair and deceptive practices jurisdiction over the company.

28. During the 2017-18 period that RagingWire participated in Privacy Shield, RagingWire did not verify, through self-assessment or outside compliance review, that its assertions about its Privacy Shield privacy practices were true and that those privacy practices had been implemented.

29. During the 2017-18 period that RagingWire participated in Privacy Shield, RagingWire also did not complete a verification statement signed by an officer or outside compliance reviewer that the assertions it had made about its Privacy Shield privacy practices during the time it participated in the program were true and that those privacy practices had been implemented.

RagingWire's Failure to Maintain an Independent Recourse Mechanism

30. Principle 7(a)(i) of the Privacy Shield Principles requires, among other things, that organizations participating in Privacy Shield provide "readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles." Supplemental Principle 11(a) specifies that participating organizations may comply with Principle 7(a)(i) by using a qualifying private-sector program.

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 that date. RagingWire did not renew its dispute resolution subscription with TRUSTe until June 2018.

RagingWire's Failure to Properly Withdraw and Affirm Its Ongoing Compliance

35. Supplemental Principle 6(f) of the Privacy Shield Principles requires that any participant that withdraws from Privacy Shield affirm to Commerce that it will either continue to apply the Privacy Shield Principles to any data received pursuant to Privacy Shield or will delete or return all such data. Supplemental Principle 7 requires organizations to respond promptly to inquiries and other requests for information from Commerce relating to the organization's adherence to the Privacy Shield Principles.

36. In February 2018, Commerce informed RagingWire that, because its certification had lapsed, it was required to complete a questionnaire verifying whether the company would re-certify or withdraw from the program and, if the latter, whether RagingWire would return and delete the data it had received under Privacy Shield or would continue to apply the Privacy Shield Principles to that data.

37. RagingWire did not complete the questionnaire.

Count 1-Privacy Shield Participation Misrepresentation

38. As described in Paragraphs 20-21, RagingWire has represented, directly or indirectly, expressly or by implication, that it was a current participant in the EU-U.S Privacy Shield Framework and/or the Safe Harbor Framework from at least January 2017 until at least October 2018.

39. In fact, as described in Paragraphs 17 and 19, RagingWire's Privacy Shield and Safe Harbor Framework certifications had lapsed and it was not a current participant in the EU-U.S. Privacy Shield Framework or the Safe Harbor Framework from at least January 2018 until

approximately June 2019. Therefore, the representations set forth in Paragraphs 38 were false or misleading.

Count 2-Misrepresentation Regarding Verification

40. As described in Paragraphs 20-21, RagingWire has represented, directly or indirectly, expressly or by implication, that it complies with the Privacy Shield Principles.

41. In fact, as described in Paragraphs 26-29, RagingWire failed to comply with the verification requirements during the time it participated in Privacy Shield. Therefore, the representations set forth in Paragraph 40 were false or misleading.

Count 3-Misrepresentation Regarding Dispute Resolution

42. As described in Paragraphs 20-21, RagingWire has represented, directly or indirectly, expressly or by implication, that it complies with the Privacy Shield Principles.

43. In fact, as described in Paragraphs 30-34, RagingWire failed to comply with the Privacy Shield Principles' requirement that it maintain a readily available independent recourse mechanism for the period from approximately October 1, 2017 through June 19, 2018. Therefore, the representations set forth in Paragraph 42 were false or misleading.

Count 4-Misrepresentation Regarding Continuing Obligations

44. As described in Paragraphs 20-21, RagingWire has represented, directly or indirectly, expressly or by implication, that it complies with the Privacy Shield Principles.

45. In fact, as described in Paragraphs 35-37, RagingWire let its certification lapse and did not affirm or verify to Commerce that it would either delete or return personal information that it received during the time it participated in the program or would continue to apply the principles to such information. Therefore, the representations set forth in Paragraph 44 were false or misleading.

Violations of Section 5 of the FTC Act

46. The acts and practices of RagingWire 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.

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 all of the material facts to be true. Such an answer will constitute a waiver of hearings as to the facts alleged in the Complaint and, together with the Complaint, will provide a record basis on which the Commission may issue a final decision containing appropriate findings and conclusions and a final order disposing of the proceeding. In such answer, you may, however, reserve the right to submit proposed findings of fact and conclusions of law under FTC Rule § 3.46.

Failure to answer timely will be deemed to constitute a waiver of your right to appear and contest the allegations of the Complaint. It will also authorize the Commission, without further notice to you, to find the facts to be as alleged in the Complaint and to enter a final decision containing appropriate findings and conclusions and a final order disposing of the proceeding.

The Administrative Law Judge will hold an initial prehearing scheduling conference to be held not later than 10 days after the answer is filed by the Respondent. Unless otherwise directed by the Administrative Law Judge, the scheduling conference and further proceedings will take place at the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Room 532-H, Washington, DC 20580. Rule 3.21(a) requires a meeting of the parties' counsel as early as practicable before the prehearing scheduling conference, but in any event no later than five (5) days after the answer is filed by the Respondent. Rule 3.31(b) obligates counsel for each party, within five (5) days of receiving a Respondent's answer, to make certain initial disclosures without awaiting a formal discovery request.

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.

ORDER

Definitions

For purposes of this Order, the following definition applies:

1. "Respondent" means RagingWire Data Centers, Inc., a corporation, and its successors and assigns.

Provisions

I. Prohibition against Misrepresentations about Participation in or Compliance with Privacy Programs

IT IS ORDERED that Respondent and its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service must not misrepresent in any manner, expressly or by implication, the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework and the APEC Cross-Border Privacy Rules.

II. Requirement to Meet Continuing Obligations Under Privacy Shield

IT IS ORDERED that Respondent and its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, must affirm to the Department of Commerce, within thirty (30) days after any withdrawal or lapse in its certification to the EU-U.S. Privacy Shield Framework or the Swiss-U.S. Privacy Shield Framework, and on an annual basis thereafter for as long as it retains such information, that it will:

1. Continue to apply the EU-U.S. Privacy Shield Framework Principles to the personal information it received while it participated in the Privacy Shield; or

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. Return or delete the information.

III. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order.

B. For twenty (20) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

IV. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

A. Sixty (60) days after the effective date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order; and (e) provide a copy of

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. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. The subject line must begin: In re *RagingWire Data Centers, Inc*., FTC Docket No. 9386.

V. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order, and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

A. accounting records showing the revenues from all goods or services sold;

B. personnel records showing, for each person providing services, whether as an employee or otherwise, that person's name, addresses, telephone numbers, job title or position, dates of service, and (if applicable) the reason for termination;

C. all records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission; and

D. a copy of each widely disseminated representation by Respondent making any

representation subject to this Order, and all materials that were 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) days of receipt of a written request from a representative of the Commission, Respondent must submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

VII. Order Effective Dates

IT IS FURTHER ORDERED that the final and effective date of this Order is the 60th day after this Order is served. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) 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 Provision in this Order that terminates in less 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 Provision.

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 will terminate according to this Provision 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.

THEREFORE, the Federal Trade Commission, this fifth day of November, 2019, has issued this Complaint against Respondent.

By the Commission.

April J. Tabor
Acting Secretary

SEAL: