**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**<br><br>**RagingWire Data Centers, Inc., a corporation,**<br><br>**Respondent.** | **DOCKET NO. 9386** |

## ORDER DENYING RESPONDENT'S MOTION TO DISMISS

By Commissioner Christine S. Wilson, for the Commission:

On November 5, 2019, the Commission issued an administrative complaint against RagingWire Data Centers, Inc. ("RagingWire" or "Respondent"), alleging that the company engaged in deceptive acts or practices in violation of Section 5 of the Federal Trade Commission Act ("FTC Act") by making false or misleading representations regarding its participation in the EU-U.S. Privacy Shield Framework and/or the Safe Harbor Framework, and its compliance with Privacy Shield Principles. Respondent has moved to dismiss the Complaint for failure to state a claim. Respondent's motion rests on its assertion that the Complaint fails to plead materiality adequately, a required element for showing that an act or practice is deceptive. We find the Complaint, construed in a light most favorable to Complaint Counsel—as required in the context of a motion to dismiss—adequately pleads that RagingWire's alleged misrepresentations were material. We therefore deny Respondent's motion to dismiss.

## I. COMPLAINT ALLEGATIONS AND PROCEDURAL BACKGROUND

We summarize the Complaint's allegations below:

Since 1995, European Union ("EU") law has prohibited (or required EU Member States to prohibit) 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 that such personal data are protected *(i.e.*, meet the EU's "adequacy" standard). Compl. ¶¶ 5–6. To satisfy this standard for certain commercial transfers, the U.S. Department of Commerce ("Commerce") and the European Commission negotiated the EU-U.S. Privacy Shield

Framework ("Privacy Shield"). *Id.* ¶ 7. Privacy Shield provides a mechanism for companies to transfer personal data from the EU to the United States in a manner consistent with the requirements of EU law on data protection. *Id.* ¶¶ 5, 7. Accordingly, personal data from the EU may lawfully be transferred to companies in the United States that participate in Privacy Shield. *Id.* ¶ 7. Privacy Shield took effect on August 1, 2016, replacing the U.S.-EU Safe Harbor Framework, a mechanism for personal data transfer that was in effect for a number of years before that. *Id.* ¶¶ 7–8. Under the EU's General Data Protection Regulation ("GDPR"), which took effect on May 25, 2018, transfers of personal information from the European Economic Area 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. *Id.* ¶¶ 6, 14.

To join Privacy Shield, a company must self-certify to Commerce that it complies with the Privacy Shield Principles and related requirements that have been deemed to meet the EU's standards. *Id.* ¶ 9. Participating companies must annually recertify their compliance. *Id.* As part of recertification, those companies must verify, through self-assessment or outside compliance review, that the assertions about their Privacy Shield privacy practices are true and that those practices have been implemented. *Id.* ¶ 26. They must also prepare a statement, signed by a corporate officer or outside reviewer, that a self-assessment or outside compliance review has been completed. *Id.* ¶ 27. Although the decision to participate in Privacy Shield is entirely voluntary, once a company self-certifies to Commerce and publicly declares its commitment to adhere to the Privacy Shield Principles, it must comply fully with them. *Id.* ¶ 10.

In some circumstances, Privacy Shield participants must ensure that third parties with which they do business provide comparable privacy protections. Under Privacy Shield Principle 3, "Accountability for Onward Transfer," participants must 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 Privacy Shield Principles. *Id.* ¶ 11. One way to meet this requirement is to use an agent that is also a Privacy Shield participant. *Id.*

Respondent RagingWire is a Nevada corporation that provides data colocation services at its specialized storage facilities, or "data centers," located in the United States. Compl. ¶¶ 2, 16. These data centers are designed to house and protect servers owned and operated by other businesses. *Id.* ¶ 2. In addition to storing customer data, RagingWire provides various complementary services, including on-site technical support, network connectivity, and physical security. *Id.* ¶¶ 2, 16. RagingWire customers that collect or process personal information from the European Economic Area and want to transfer that data to RagingWire in the United States can comply with the GDPR and/or their own Privacy Shield obligations if RagingWire participates in Privacy Shield. *Id.* ¶ 16.

Prior to June 2016, RagingWire participated in the Safe Harbor Framework. *Id.* ¶ 17. In January 2017, it obtained a Privacy Shield certification. *Id.* ¶ 18. One year later, however, RagingWire did not complete the steps necessary to renew its Privacy Shield certification, and its Privacy Shield certification lapsed in January 2018. *Id.* ¶ 19. Despite this lapse, RagingWire continued to represent in its online privacy policy that it participated in and complied with

Privacy Shield and that it adhered to the Privacy Shield Principles. *Id.* ¶ 20. It also 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 either framework. *Id.* ¶ 21. Further, RagingWire continued to represent that it was committed to resolving complaints regarding privacy and data collection or use in compliance with Privacy Shield, and it directed users to contact its third-party dispute resolution provider TRUSTe LLC in case of any unresolved privacy or data concerns. *Id.* ¶¶ 20, 33. In fact, however, RagingWire's subscription with TRUSTe LLC had been terminated as of October 1, 2017, and was not renewed until June 2018. Id. ¶ 34. Accordingly, during this time, RagingWire was not in compliance with the Privacy Shield requirement to maintain a readily available independent recourse mechanism for dispute resolution. *Id.* ¶¶ 30, 43.

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. *Id.* ¶ 22. RagingWire did not remove its online Privacy Shield statements until October 2018, after RagingWire was contacted by the FTC. *Id.* ¶ 23. In June 2019, RagingWire again obtained Privacy Shield certification. *Id.* ¶ 24.

The Commission's Complaint against RagingWire alleges four counts of misrepresentation. In the first count, the Complaint asserts that RagingWire misrepresented that it was a current participant in Privacy Shield and/or the Safe Harbor Framework for a period of ten months after its certifications had lapsed. *Id.* ¶¶ 38–39; *see also id.* ¶¶ 22–23 (describing RagingWire's failure until October 2018 to take down the claim that it participated in Privacy Shield, despite the lapse of its certification in January 2018). The other three counts allege that RagingWire represented that it complied with Privacy Shield Principles when in fact it did not comply with those Principles by (1) failing to meet the compliance-verification requirements, (2) failing to maintain a readily available independent recourse mechanism, and (3) letting its certification lapse without affirming or verifying to Commerce that it either would 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. *Id.* ¶¶ 40–45. The Complaint alleges that the identified acts and practices "constitute deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act." *Id.* ¶ 46.

The Respondent filed an Answer on November 25, 2019. On December 2, 2019, Respondent moved to dismiss the Complaint for failure to state a claim.

## II. STANDARD OF REVIEW

We review RagingWire's Motion to Dismiss Administrative Complaint ("Motion") using the standards applied by federal courts under Rule 12(b)(6) of the Federal Rules of Civil Procedure. *LabMD, Inc.*, 2014 WL 253518, at *2 (F.T.C. Jan. 16, 2014); *S.C. State Bd. of Dentistry*, 138 F.T.C. 229, 232–33 (2004). "Our task is to determine whether the Complaint contains sufficient factual matter to state a claim to relief that is plausible on its face." *LabMD*, 2014 WL 253518, at *2 (quoting *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2012)) (internal quotation marks, ellipsis, and brackets omitted). We must "accept the allegations in the

complaint as true and construe them in the light most favorable to Complaint Counsel." *LabMD*, 2014 WL 253518, at *2 (quoting *Am. Dental Ass'n v. Cigna Corp.*, 605 F.3d 1283, 1288 (11th Cir. 2010)) (internal quotation marks and brackets omitted); *S.C. State Bd. of Dentistry*, 138 F.T.C. at 232–33.

## III. ANALYSIS

The Complaint alleges that RagingWire engaged in deceptive acts or practices in violation of Section 5 of the FTC Act. An act or practice is deceptive if (1) there is a representation, omission, or practice (2) that is likely to mislead consumers acting reasonably under the circumstances and (3) the representation, omission, or practice is material. *FTC v. Gill*, 265 F.3d 944, 950 (9th Cir. 2001); *FTC Policy Statement on Deception*, appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 175–76 (1984) ("*Deception Statement*"); *Cliffdale Assocs.*, 103 F.T.C. at 164–65. Respondent urges us to dismiss the Complaint for failure to allege materiality.

A representation is considered material if it "involves information that is important to consumers and, hence, likely to affect their choice of, or conduct regarding, a product." *FTC v. Cyberspace.Com LLC*, 453 F.3d 1196, 1201 (9th Cir. 2006) (quoting *Cliffdale Assocs.*, 103 F.T.C. at 165); *FTC v. QT, Inc.*, 448 F. Supp. 2d 908, 960 (N.D. Ill. 2006) (quoting *Kraft, Inc. v. FTC*, 970 F.2d 311, 322 (7th Cir. 1992)), *aff'd*, 512 F.3d 858 (7th Cir. 2008); *Cambridge Analytica, LLC*, 2019 WL 6724446, at *10 (F.T.C. Nov. 25, 2019). Respondent argues that the Complaint fails to allege materiality because it does not directly state that Privacy Shield compliance is important to RagingWire customers or that Privacy Shield certification affected any customer's purchasing decisions. Motion at 4. Such allegations, however, are not required.

The Complaint alleges that RagingWire represented that it participated in Privacy Shield and complied with Privacy Shield Principles. Compl. ¶ 20. Its online privacy policy expressly asserted that "RagingWire complies with the EU-US Privacy Shield Framework" and directed users to "view our certification page." *Id.* It also stated that "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." *Id.* In addition, RagingWire's online privacy policy stated that "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" and expressly invited clients with "an unresolved privacy or data use concern that we have not addressed satisfactorily" to "contact our U.S.-based third party dispute resolution provider" at a URL for TRUSTe. *Id.* Further, RagingWire "disseminated or caused to be disseminated sales materials containing representations that RagingWire was a participant in Privacy Shield and/or the Safe Harbor Framework." *Id.* ¶ 21.

"In most cases, the very existence of an express claim is sufficient to demonstrate that the claim is material." *ECM Biofilms, Inc.*, 2015 WL 6384951, at *53 (F.T.C. Oct. 19, 2015), *pet. for review denied*, 851 F.3d 599, 604 (6th Cir. 2017). Thus, express statements are presumed to be material. *Id.*; *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1095–96 (9th Cir. 1994); *Jerk, LLC*, 159 F.T.C. 885, 906 (2015), *aff'd in relevant part*, *Fanning v. FTC*, 821 F.3d 164, 172–73 (1st Cir.

2016); *POM Wonderful LLC*, 155 F.T.C. 1, 62 (2013) (citing *Novartis Corp.*, 127 F.T.C. 580, 686 (1999) (citing *Deception Statement*, 103 F.T.C. at 182)), *aff'd*, 777 F.3d 478 (D.C. Cir. 2015). Express claims encompass not only the explicit statements in the representation but also necessary implications derived from the statements. *FTC v. Bronson Partners, LLC*, 564 F. Supp. 2d 119, 126 n.4 (D. Conn. 2008).

We recently applied the presumption of materiality to similar representations regarding Privacy Shield in *Cambridge Analytica*. In that case, as in this one, the respondent represented on its website that it participated in and complied with Privacy Shield, even though its certification had lapsed. *Cambridge Analytica*, 2019 WL 6724446, at *8 (F.T.C. Nov. 25, 2019). The Commission found that the representations were express and that therefore the presumption of materiality applied. *Id.* at *12. Similarly, because the representations cited in the Complaint here were express, they are presumptively material. That presumption, along with the Complaint's allegations of false and misleading representations, Compl. ¶¶ 38–45, constitutes sufficient basis to state a deception claim that is plausible on its face. Respondent may seek to rebut the presumption with contrary evidence, but that raises issues for trial, not for a motion to dismiss.

Respondent asserts that the presumption should not apply because the Complaint does not specifically plead the presumption. RagingWire Data Centers, Inc.'s Reply in Support of Motion to Dismiss Administrative Complaint and Request for Stay and Referral ("Reply") at 4. But a complaint "need not . . . plead law or match facts to every element of a legal theory." *Rhodes v. Super. Ct. of D.C.*, 303 F. Supp. 3d 1, 3 (D.D.C. 2018) (quoting *Krieger v. Fadely*, 211 F.3d 134, 136 (D.C. Cir. 2000)) (internal quotation marks omitted). As the Supreme Court explained, a complaint need only provide the factual basis for a claim for relief and should not be dismissed "for imperfect statement of the legal theory supporting the claim asserted." *Johnson v. City of Shelby*, 574 U.S. 10, 11–12 (2014).[1]

Even without a presumption, the Complaint pleads sufficient facts to support a reasonable inference of materiality. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (a claim survives a motion to dismiss "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged."). We can reasonably infer materiality from RagingWire's own actions and from the legal obligations to which its customers that collect personal data from the EU are subject.

As to its actions, RagingWire elected to join Privacy Shield and the Safe Harbor Framework and to publicize its participation on its website and in its marketing materials. Compl. ¶¶ 17–18, 20–21. Indeed, RagingWire went to considerable lengths to inform its clients that it was committed to resolve their complaints about privacy and data collection and use "[i]n compliance with the EU-U.S. Privacy Shield Principles." *Id.* ¶ 20. Further, after letting its certification lapse, and then removing its representations about Privacy Shield adherence from its website in October 2018, *id.* ¶ 23, RagingWire renewed its Privacy Shield certification in 2019,

[1] Similarly, as Respondent itself acknowledges, the Complaint's omission of the words "material" and "materiality" does not warrant dismissal. *See* Reply at 2–3.

*id.* ¶ 24. These allegations support a reasonable inference that RagingWire appears to have understood its Privacy Shield participation and its compliance with Privacy Shield principles were important to its customers, which supports a reasonable inference that such claims are likely to affect their conduct and are thus material.

The Complaint's allegations regarding customers' legal obligations also support a reasonable inference that RagingWire's participation in Privacy Shield is important to its customers. Companies that transfer data from the EU to the United States must do so through an authorized mechanism such as Privacy Shield or risk significant fines. *Id.* ¶ 14 (citing GDPR, Art. 83). Privacy Shield, in turn, requires these companies to ensure that third-party agents to which they transfer data provide at least the same level of privacy as required by Privacy Shield Principles. *Id.* ¶ 11. One way these companies may establish compliance is to ensure that any company to which they transfer data is also part of Privacy Shield. *Id.* It is therefore reasonable to infer that companies (including customers or potential customers of Raging Wire) that receive personal data pursuant to Privacy Shield and then transfer that data from the EU to the United States would find it important that the company that stores this data is a Privacy Shield participant. *See id.* ¶ 16 (alleging that RagingWire stores customer data at its U.S. centers).

Respondent urges us to dismiss the Complaint because it "does not allege that there are, in fact, customers that want to or do transfer protected data to RagingWire." Motion at 4–5. Further, Respondent asserts that there is no reason to believe that such customers even exist, "[i]n light of the nature of RagingWire's business." *Id.* at 5. Respondent admits, however, that some of its customers have locations in Europe, Answer at 4, though even its U.S.-based customers could be collecting data from the EU. To the extent that Respondent contends that its customers do not care about whether it complies with Privacy Shield because they do not actually "transfer" data to RagingWire, Respondent is free to make this argument in rebuttal to the presumption of materiality, but it is not an argument we can properly assess on a motion to dismiss. The argument raises factual issues regarding the nature of RagingWire's services—including the "technical support" and "network connectivity" alleged in Paragraph 2 of the Complaint—and the needs and concerns of its customers, so it cannot form a basis for dismissal. *See S.C. State Bd. of Dentistry*, 138 F.T.C. at 233 ("[T]he Commission should not dismiss the complaint if the motion, or Complaint Counsel's opposition to the same, raises disputed issues of material fact.").

Respondent also takes issue with the Complaint's failure to identify customers who actually viewed the Privacy Shield statements and relied on them in making their decisions. Reply at 5. The Complaint need not, however, identify customers who relied on the express claims. *See FTC v. Ideal Fin. Sols., Inc.*, 2014 WL 2565688, at *6 (D. Nev. June 5, 2014) ("Express claims are presumed material, and the FTC does not have to prove actual reliance by consumers."); *Deception Statement,* 103 F.T.C. at 183 (Commission will not generally require extrinsic evidence concerning the materiality of a challenged claim). The materiality standard requires only that a representation is "likely" to affect consumer choice, not that it actually did. *See, e.g., Cliffdale Assocs.*, 103 F.T.C. at 165–66; *see also FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1203 (10th Cir. 2005) ("Neither proof of consumer reliance nor consumer injury is necessary to establish a § 5 violation. Otherwise, the law would preclude the FTC from taking

preemptive action against those responsible for deceptive acts or practices, contrary to § 5's prophylactic purpose.") (citation omitted).

As noted above, Respondent may marshal evidence to rebut the presumption of materiality. Indeed, belying Respondent's claim that the Complaint fails to put it on notice regarding the basis for asserting materiality, Reply at 7–8, Respondent has already indicated that it is poised to offer rebuttal, Answer at 3–4. At this stage in the proceedings, however, Complaint Counsel have alleged sufficient facts to state a plausible claim to relief. The Complaint adequately alleges that RagingWire's misrepresentations about its participation in and compliance with Privacy Shield are material and hence deceptive.

Accordingly,

**IT IS ORDERED THAT** Respondent RagingWire's Motion to Dismiss Administrative Complaint is **DENIED.**

By the Commission.

April J. Tabor
Acting Secretary

SEAL:
ISSUED: February 3, 2020