

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)
)
TDARX, Inc.,) DOCKET NO.
A corporation.)
)
)
)

COMPLAINT

The Federal Trade Commission (“FTC”), having reason to believe that TDARX, 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 TDARX, Inc. is a Delaware corporation with its principal office or place of business at 4000 Brownsboro Rd, Winston Salem, North Carolina 27106.
2. Respondent provides IT management and security services through the websites <https://www.tdarx.com> and <http://www.nocdoc.com>.
3. The acts and practices of Respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act.
4. Respondent had set forth on its website, http://www.nocdoc.com/pdf/privacy_policy.pdf, privacy policies and statements about its practices, including statements related to its participation in the EU-U.S. Privacy Shield framework agreed upon by the U.S. government and the European Commission.

Privacy Shield

5. The EU-U.S. Privacy Shield framework (“Privacy Shield”) was designed by the U.S. Department of Commerce (“Commerce”) and the European Commission to provide a mechanism for U.S. companies to transfer personal data outside of the EU that is consistent with the requirements of the European Union data protection legislation. The EU General

Data Protection Regulation, passed in May 2016 and enforced since May 2018 (replacing the 1995 EU Data Protection Directive), sets forth EU requirements for privacy and the protection of personal data. Among other things, it requires 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. Any company that voluntarily withdraws or lets its self-certification lapse must take steps to affirm to Commerce that it is continuing to protect the personal information it received while it participated in the program.

6. To satisfy the EU adequacy standard for certain commercial transfers, Commerce and the European Commission negotiated the EU-U.S. Privacy Shield framework, which went into effect in July 2016. The EU-U.S. Privacy Shield framework allows companies to transfer personal data lawfully from the EU to the United States. 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 related requirements that have been deemed to meet the EU's adequacy standard. Any company that participates in Privacy Shield must verify, at least once a year, 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.
7. Companies under the jurisdiction of the FTC, as well as the U.S. Department of Transportation, are eligible to join the EU-U.S. Privacy Shield framework. A company under the FTC's jurisdiction that claims it has self-certified to the Privacy Shield Principles, but failed to self-certify to Commerce or failed to comply with the Privacy Shield Principles, may be subject to an enforcement action based on the FTC's deception authority under Section 5 of the FTC Act.
8. Commerce maintains a public website, <https://www.privacyshield.gov/welcome>, where it posts the names of companies that have self-certified to the EU-U.S. Privacy Shield framework. The listing of companies, <https://www.privacyshield.gov/list>, indicates whether the company's self-certification is current.
9. Respondent has disseminated or caused to be disseminated privacy policies and statements on the http://www.nocdoc.com/pdf/privacy_policy.pdf website, including, but not limited to, the following statements:

Recourse Mechanism for Privacy Shield Complaints

In compliance with the Privacy Shield Principles, NOCDOC commits to resolve complaints about our collection or use of your personal information. EU individuals with inquiries or complaints regarding our Private Shield policy should first contact NOCDOC at: CustomerCare@nocdoc.com or fill out a form at <http://www.nocdoc.com/contact.aspx>

NOCDOC has further committed to cooperate with EU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning human resources data transferred from the EU in the context of the employment relationship.

10. Although Respondent obtained Privacy Shield certification in 2017, that certification lapsed one year later, in 2018.
11. Commerce warned the company 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. Respondent did not do so timely, nor did it withdraw and affirm its commitment to protect any personal information it had acquired while in the program.
12. After its certification lapsed, Respondent continued to claim, as indicated in paragraph 9, that it participated in the EU-U.S. Privacy Shield framework.
13. The Privacy Shield Principles include Supplemental Principle 7, which requires any company that participates in Privacy Shield to verify, at least once a year, 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. The verification statement must be signed by a corporate officer or the outside reviewer and is required to be made available on request to the FTC or Department of Transportation, whoever has unfair and deceptive practices jurisdiction over the company.
14. Respondent is under the jurisdiction of the FTC. During the 2017-18 period that Respondent was certified to participate in Privacy Shield, Respondent failed to comply with the requirement to obtain, through self-assessment or outside compliance review, an attested verification statement 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.

Count 1-Privacy Misrepresentation

15. As described in Paragraph 9, Respondent represented, directly or indirectly, expressly or by implication, that it was a current participant in the EU-U.S Privacy Shield framework.
16. In fact, as described in Paragraphs 10-12, after its certification lapsed, Respondent was not a current participant in the EU-U.S. Privacy Shield framework. Therefore, the representation set forth in Paragraph 15 is false or misleading.

Count 2-Misrepresentation Regarding Verification

17. As described in Paragraph 9, Respondent represented that it complied with the EU-U.S. Privacy Shield principles.
18. In fact, as described in Paragraphs 13-14, Respondent failed to comply with the verification requirement during the time it participated in the program. Therefore, the representation set forth in Paragraph 17 is false or misleading.

Count 3-Misrepresentation Regarding Continuing Obligations

19. As described in Paragraph 9, Respondent represented that it complied with the EU-U.S. Privacy Shield framework principles. These principles include a requirement that if it ceased to participate in the EU-U.S. Privacy Shield framework, it must affirm to Commerce that it will continue to apply the principles to personal information that it received during the time it participated in the program.
20. In fact, as described in Paragraph 10, Respondent did not affirm to Commerce that it will continue to apply the principles to personal information that it received during the time it participated in the program. Therefore, the representation set forth in Paragraph 19 is false or misleading.

Violations of Section 5 of the FTC Act

21. The acts and practices of Respondent 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.

THEREFORE, the Federal Trade Commission this ___ day of ____ 2019, has issued this complaint against Respondent.

By the Commission.

April J. Tabor
Acting Secretary

SEAL
ISSUED: