UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

June 23, 2022

Anonymous

RE: *In the Matter of CafePress, LLC*
File No. 1923209

Dear Anonymous:

We would like to thank you for commenting on the Federal Trade Commission's ("Commission" or "FTC") proposed consent orders in the above-referenced proceeding. The Commission has placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of the agency's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission is committed to protecting consumers from deceptive, unfair, and other unlawful practices, and we appreciate your feedback on this matter.

According to our complaint against Residual Pumpkin Entity, LLC, and PlanetArt, LLC, the companies violated the FTC Act by engaging in deceptive and unfair practices relating to the data security and privacy of the personal information of their consumers.

The Proposed Orders, among other things, prohibit the companies from making misrepresentations about privacy and security of information they collect, mandate the creation of an Information Security Program, require third-party program assessments, and require the submission of a report to the FTC after any Covered Incident. In addition, affected consumers will receive a notice that their data was compromised and steps they can take to protect their personal information. Consumers that used CafePress to sell merchandise, had commissions wrongfully withheld, and faced an increased risk of identity theft will receive monetary redress.

In your comment, you first asked whether two years was too late to notify consumers of a data breach and what would allow the FTC to notify consumers within 30 days of another breach. The FTC investigated the companies' business practices and the breach itself. The Proposed Order with PlanetArt, LLC, requires the company to provide a notice to consumers that gives them information about what happened and details specific steps they can take to protect their personal information. The Proposed Orders also require the companies to take action in the event of a "Covered Incident," which is defined as an incident requiring the companies to provide notice to a government entity if an individual consumer's information was, or is reasonably believed to have been, accessed or acquired without authorization. In such an event, the Proposed Respondents must submit a report about the Covered Incident within 30 days of when the Proposed Respondent discovers the Covered Incident.

Second, you recommended that the companies should be required to "maintain [compliance with] an industry standard," such as the AICPA-developed SOC 2 standard. The Proposed Orders require the companies to implement and maintain a rigorous information security program. They further require the companies to obtain independent assessments of their compliance with that program, whose results must be made available to the Commission.

Third, you wanted to know whether the company was Payment Card Industry Data Security Standard ("PCI") compliant. The complaint does not contain allegations regarding PCI-DSS compliance, but the proposed consent orders prohibit misrepresentations about compliance with third-party security programs. The consent orders also include financial information in the definition of Personal Information, which is covered under the Information Security Program.

Fourth, you inquired whether the company broke the Controlling the Assault ofNon-Solicited Pornography and Marketing Act of2003 ("CAN-SPAM Act"), 15 U.S.C. § 7701 et seq., by failing to comply with requests to opt out of email marketing. The CAN-SP AM Act requires opt-out methods to be included in electronic mail messages and prohibits sending electronic messages to recipients who used the opt-out method included in such electronic messages. See 15 U.S.C. § 7704(3), (4). We do not allege that Proposed Respondents failed to honor the opt-out mechanisms included in their electronic mail. You further ask how the FTC will audit which consumers will opt in or opt out and whether CafePress will sync those choices among pieces of the companies' technological infrastructure. The Proposed Orders prohibit any misrepresentation about any "measures to honor the privacy choices exercised by users," and require the companies to establish, implement, and maintain an Information Security Program that covers, among other things, internal risks to the unauthorized use of Personal Information.

Fifth, you proposed the FTC require that the companies create or participate in a bug bounty program with a safe harbor. The Proposed Orders require the companies to consult with and seek guidance from third-party experts in relation to their Information Security Program and obtain third-party program assessments.

Sixth, you recommended that the FTC could mandate the company get an independent review of all code before it is used in a production environment. A code review is included in the Information Security Program, which requires the policies and procedures that "ensure that all code for web applications is reviewed for the existence of common vulnerabilities."

Seventh, you suggested CafePress should post a notice on their home page about the breach. Consumers who were affected by the breach will receive a notice giving them details about what happened to their data and what steps they can take to protect their personal information.

Eighth, you inquired whether the Proposed Order's $500,000 in monetary relief covers both monies earned through misconduct and the FTC's cost of bringing this enforcement action. We expect the money to be sufficient to provide redress to consumers who used CafePress to sell merchandise, had commissions wrongfully withheld, and faced an increased risk of identity theft. Monetary relief from Commission enforcement actions are not used to pay FTC costs.

Having considered all the facts of this case and the comments submitted in response to the Proposed Orders, the Commission has now determined that the public interest would best be served by issuing the Complaint and the Decisions and Orders in final form without any modifications. The final Decisions and Orders and other relevant materials are available from the Commission's website at http://www.ftc.gov. The Commission thanks you again for your comment.

By direction of the Commission.

Sincerely,

April J. Tabor
Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

June 23, 2022

Chris Cronin

RE: *In the Matter of CafePress, LLC*
File No. 1923209

Dear Mr. Cronin:

We would like to thank you for commenting on the Federal Trade Commission's ("Commission" or "FTC") proposed consent orders in the above-referenced proceeding. The Commission has placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of the agency's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission is committed to protecting consumers from deceptive, unfair, and other unlawful practices, and we appreciate your feedback on this matter.

According to our complaint against Residual Pumpkin Entity, LLC, and PlanetArt, LLC, the companies violated the FTC Act by engaging in deceptive and unfair practices relating to the data security and privacy of the personal information of their consumers.

The Proposed Orders, among other things, prohibit the companies from making misrepresentations about privacy and security of information they collect, mandate the creation of an Information Security Program, require third-party program assessments, and require the submission of a report to the FTC after any Covered Incident. In addition, affected consumers will receive a notice that their data was compromised and steps they can take to protect their personal information. Consumers that used CafePress to sell merchandise, had commissions wrongfully withheld, and faced an increased risk of identity theft will receive monetary redress.

Section II of the Proposed Orders require that the Proposed Respondents maintain the security of consumer information. First, they specifically require the creation, implementation, and maintenance of an Information Security Program that "protects the privacy, security, confidentiality, and integrity of" of Personal Information. The Proposed Orders define Personal Information as individually identifiable information about an individual consumer and give several examples including name, address, telephone number, persistent identifiers, and authentication credentials. Second, provision II.D requires that the "internal and external risks to the privacy, security, confidentiality, or integrity of Personal Information" be assessed and documented at least once a year and within 30 days of any "Covered Incident." A Covered Incident is defined as any incident where the Proposed Respondents would be required to give notice to a government entity that an individual consumer's information "was, or is reasonably believed to have been, accessed or acquired without authorization." Finally, provision II.E

requires Proposed Respondents to "[d]esign, implement, maintain, and document safeguards that control" for any risks to the "privacy, security, confidentiality, or integrity of Personal Information" that the II.D assessment identifies.

Your letter states the FTC could adopt a risk analysis framework articulated by the Sedona Conference to avoid "[s]elf-interested risk analysis" that ignores impacts to consumers. However, the provisions described above, and others in the Proposed Orders, require Proposed Respondents to assess risks of potential harm to consumers and to take action when such risks are identified.

Having considered all the facts of this case and the comments submitted in response to the Proposed Orders, the Commission has now determined that the public interest would best be served by issuing the Complaint and the Decisions and Orders in final form without any modifications. The final Decisions and Orders and other relevant materials are available from the Commission's website at http://www.ftc.gov. The Commission thanks you again for your comment.

By direction of the Commission.

Sincerely,

April J. Tabor
Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

June 23, 2022

John Davisson, Director of Litigation & Senior Counsel
Sara Geoghegan, Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

RE: *In the Matter of CafePress, LLC*
File No. 1923209

Dear Mr. Davisson and Ms. Geoghegan:

We would like to thank you for commenting on the Federal Trade Commission's ("Commission" or "FTC") proposed consent orders in the above-referenced proceeding. The Commission has placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of the agency's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission is committed to protecting consumers from deceptive, unfair, and other unlawful practices, and we appreciate your feedback on this matter.

According to our complaint against Residual Pumpkin Entity, LLC, and PlanetArt, LLC, the companies violated the FTC Act by engaging in deceptive and unfair practices relating to the data security and privacy of the personal information of their consumers.

The Proposed Orders, among other things, prohibit the companies from making misrepresentations about privacy and security of information they collect, mandate the creation of an Information Security Program, require third-party program assessments, and require the submission of a report to the FTC after any Covered Incident. In addition, affected consumers will receive a notice that their data was compromised and steps they can take to protect their personal information. Consumers that used CafePress to sell merchandise, had commissions wrongfully withheld, and faced an increased risk of identity theft will receive monetary redress.

In your comment, EPIC notes that it supports the proposed consent agreements, highlights the importance of the prompt disclosure of data breaches and the monetary relief, and recommends that the Commission use its trade regulation rulemaking authority to enact a data minimization rule and define and prohibit privacy harms. We note that the monetary relief will help redress affected consumers and is not a penalty. We appreciate EPIC's support of the proposed consent agreements and note that the Commission is considering whether to initiate rulemaking.

Having considered all the facts of this case and the comments submitted in response to the Proposed Orders, the Commission has now determined that the public interest would best be served by issuing the Complaint and the Decisions and Orders in final form without any modifications. The final Decisions and Orders and other relevant materials are available from the Commission's website at http://www.ftc.gov. The Commission thanks you again for your comment.

By direction of the Commission.

Sincerely,

April J. Tabor
Secretary