1923209

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Lina M. Khan, Chair
Noah Joshua Phillips
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of RESIDUAL PUMPKIN ENTITY, LLC, a limited liability company, formerly d/b/a CAFEPRESS, and PLANETART, LLC, a limited liability company, d/b/a CAFEPRESS.	DOCKET NO.

COMPLAINT

The Federal Trade Commission, having reason to believe that Residual Pumpkin Entity, LLC, a limited liability company, and PlanetArt, LLC, a limited liability company (collectively, ³5HVSRQGHQWV´ KDYH YLRODWHG WKH SURYLVLRQV RI WK
appearing to the Commission that this proceeding is in the public interest, alleges:

1. 5HVSRQGHQW 5HVLGXDO 3XPSNLQ (QWLW\ //& ³5HVLGXDO 3XPSNLQ´ formerly doing business as CafePress, is a Delaware limited liability company with its principal office or place of business at 11909 Shelbyville Road, Louisville, Kentucky 40243.

2. 5HVSRQGHQW 3ODQHW$UW //& ³3ODQHW$UW´ is a Delaware limited liability company with its principal office or place of business at 23801 Calabasas Road, Suite 2005, Calabasas, California 91302.

3. Residual Pumpkin developed and operated a platform that allows consumers to purchase customized merchandise such as t-shirts and coffee mugs from other consumers or
y=X µ%Ôä€<<

and began operating the website www.cafepress.com. As part of the September 1, 2020 transaction, CafePress changed its name to Residual Pumpkin Entity. This complaint uses the name Residual Pumpkin to refer to activity conducted by that entity before its September 1, 2020 name change.

i. Residual Pumpkin failed to reasonably respond to security incidents. For example, Residual Pumpkin failed to:

   i. timely disclose security incidents to relevant parties, preventing them from taking readily available low-cost measures to avoid or mitigate reasonably foreseeable harm;3 (n)]TJ ET Q q 0 0 612 792 re W n ë• ï À &äp îî g’¾í>¦®ïìZîZÒ¤î¢«N

18. On April 10, 2019, Residual Pumpkin received an email from a foreign government with an attached letter stating that a hacker had illegally obtained access to CafePress user account information from January 2014 to January 2019. The email included an attachment with CafePress account logins and passwords and said the hacker had sold the information to a large QXPEHU RI GHUV ´ 7KH OHWWHU UHTXHVWHG FRPSDQ\ 5HVLGXDO accounts WR ³SURYH QRWLILFDWLRQ DFFRXQWV RZQHG E\ XVHUV

19. On April 15, 2019, Residual Pumpkin required all users who logged into the service to reset their passwords, telling consumers only that the company had updated its password policy.

20. Publicly available internet posts began appearing on July 13, 2019, stating that consumer GDWD LQ 5HVLGXDO 3XPSNLQ¶V FXVWRPHU DFFRXQW GDWDEDVH KDG EHHQ EUHDFKHG Twitter.com, Reddit.com, and other discussion boards. By July 19, 2019, posters began to request assistance with decrypting the passwords, and by August 3, 2019, posts appeared purporting to show recovered passwords from the breach.

21. On July 26, 2019, Residual Pumpkin became aware of a post on Facebook stating that the poster had received notice from a monitoring service that her information had been breached IURP 5HVLGXDO 3XPSNLQ¶V QHWZRUN

22. From July 26, 2019, through August 5, 2019, Residual Pumpkin received additional reports from consumers stating that they received third-party notifications that their data had been hacked. On August 5, 2019, a post on the haveibeenpwned.com website indicated that the website had been breached. The next day, Residual Pumpkin internally confirmed that its customer records were available for sale on the dark web.

23. After third parties publicized the breach, Residual Pumpkin reviewed the data it had received in the April 10, 2019 email and confirmed that it appeared to contain CafePress account names and passwords.

24. In September 2019, Residual Pumpkin

Injury to Consumers

34. &RQVXPHUV KDYH OLNHO\ VXIIHUHG DFWXDO LQMXU\ DV
IDLOXUHV %UHDFKHG 3HUVRQDO ,QIRUPDWLRQ RIWHQ LV XVHG
used to commit identity theft and fraud. For example, as noted above, Personal Information
H[IILOWUDWHG IURP 5HVSRQGHQW¶V GDWD systems, including login credentials and Social Security numbers,
was known to be in the hands of criminals on the dark web including credit card fraudsters and
scammers who, among other things, used recovered passwords in extortion attempts of
5HVSRQGHQWV¶ FRQVXPHUV

35. 5HVLGXDO 3DUW\ 5HVSRQGHQW¶V IDLOXUH WR UHVSRQG DGHTXDWHO\ WR PXOWLSOH
led to an unreasonable delay in notifying consumers that their information was exposed and
increased the likelihood that those consumers would become victims of identity theft and fraud.
5HVLGXDO 3DUW\ 5HVSRQGHQW¶V SDVVZRUG UHVHW SURFHGXUH IXUWKHU
FRQVXPHUV¶ 3HUVRQDO ,QIRUPDWLRQ DV

Users in the European Union (EEA) and Switzerland
If you are a resident of the EEA [European Economic Area] or Switzerland, the following information applies.

Purposes of processing and legal basis for processing: As explained above, we process personal data in various ways depending upon your use of our Websites. We process personal data on the following legal bases: (1) with your consent; (2) as necessary to perform our agreement to provide Services; and (3) as necessary for our legitimate interests in providing the Websites where those interests do not override your fundamental rights and freedom related to data privacy.

***

Individual Rights: If you are a resident of the EEA or Switzerland, you are entitled to the following rights.
. . . .
The right to request data erasure: You have the right to have your data erased from our Websites if the data is no longer necessary for the purpose for which it was collected, you withdraw consent and no other legal basis for processing exists, or you believe your fundamental rights to data privacy and protection outweigh our legitimate interest in continuing the processing.

***

Privacy Shield Frameworks
CafePress Inc. complies with the EU-US Privacy Shield Framework and the Swiss-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 and Switzerland transferred to the United States pursuant to Privacy Shield. CafePress has certified that it adheres to the Privacy Shield Principles with respect to such data. If there is any conflict between the policies in this privacy policy and data subject rights under 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/
. . . .
EU and Swiss individuals have the right to obtain our confirmation of whether we maintain personal information relating to you. Upon request, we will provide you with access to the personal information that we hold about you. You also may correct, amend, or delete the personal information we hold about you. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data, should direct their query to GDPR@cafepress.com. If requested to remove data, we will respond within a reasonable timeframe.
. . . .
We will provide an individual opt-out or opt-in choice before we share your data with third parties other than our agents, or before we use it for a purpose other than which it was originally collected or subsequently authorized.

To limit the use and disclosure of your personal information, please submit a written request to GDPR@cafepress.com.

38. The 'Department of Commerce' ('Commerce') and the European Commission have negotiated the Privacy Shield to provide a mechanism for companies to transfer personal data from the European Union to the United States in a manner consistent with the requirements of European Union law on data protection. The Swiss-U.S. Privacy Shield framework is identical to the EU-U.S. Privacy Shield framework.

39. 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'.

40. To join the EU-U.S. and/or Swiss-U.S. Privacy Shield framework, a company must certify to Commerce that it complies with the Privacy Shield Principles. Participating companies must annually re-certify their compliance.

41. Companies under the jurisdiction of the FTC are eligible to join the EU-U.S. and/or Swiss-U.S. Privacy Shield framework. Both frameworks warn companies that claim to have self

Principles, except where the burden or expense of providing access would be G L V S U R S R U W L R Q D W H W R W K H U L V N V W R W K H L Q G L where the rights of persons other than the individual would be violated.

44. Although the European Court of Justice determined on July 16, 2020 that the E.U.-U.S. Privacy Shield framework was not adequate for allowing the lawful transfer of personal data from the European Union and the Swiss Data Protection and Information Commissioner determined on September 8, 2020 that the Swiss-U.S. Privacy Shield framework was similarly

49. The acts and practices of Respondents alleged in this complaint involve material conduct occurring within the United States.

Count I
Data Security Misrepresentations

50. As described in Paragraphs 8-10, Respondents have represented, directly or indirectly, expressly or by implication, that they

Count V
Misrepresentation Relating to Privacy Shield Frameworks

55. As described in Paragraph 57