1923209

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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 NOS. C-4768 & C-4769

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, "Respondents"), have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Residual Pumpkin Entity, LLC ("Residual Pumpkin"), also 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. Respondent PlanetArt, LLC ("PlanetArt"), also doing business as CafePress, 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 "shopkeepers" on the platform at www.cafepress.com. On September 1, 2020, PlanetArt purchased substantially all of CafePress's assets, including the use of the trade name CafePress, 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.

4. PlanetArt has run the website from the same building, with the same servers, using many of the same vendor accounts, in the same line of business, with many of the same personnel as its predecessor, Residual Pumpkin.

5. The acts and practices of Respondents alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

Data Security

6. Respondents have hosted a platform at the website www.cafepress.com, through which consumers nationwide and internationally can purchase customized merchandise.

7. In selling and promoting products through www.cafepress.com, Respondents routinely have collected information from consumers and shopkeepers—including names, email addresses, telephone numbers, birth dates, gender, photos, social media handles, security questions and answers, passwords, PayPal addresses, the last four digits and expiration dates of credit cards, and Social Security or tax identification numbers of shopkeepers (collectively "Personal Information")—through Respondents' website. Residual Pumpkin stored this Personal Information on their network in clear text, except for passwords, which were encrypted.

Residual Pumpkin's Deceptive Data Security Representations

8. Since at least June 2018 until in or around February 2020, Residual Pumpkin disseminated or caused to be disseminated a privacy policy on the www.cafepress.com website, attached as Exhibit A. This privacy policy contained the following statements regarding the security of the Personal Information it has collected:

> CafePress values the trust you place in us when you use CafePress.com and our affiliated websites, applications or tools (collectively, our "Websites"). Your privacy and trust are important to us and who we are as a company.
>
> * * *
>
> We do our best to provide you with a safe and convenient shopping experience. Our Websites incorporate physical, technical, and administrative safeguards to protect the confidentiality of the information we collect through the Websites, including the use of encryption, firewalls, limited access and other controls where appropriate. **While we use these precautions to safeguard your personal information, we cannot guarantee the security of the networks, systems, servers, devices, and databases we operate or that are operated on our behalf. 100% complete security does not presently exist anywhere online or offline.**

(Emphasis in original.)

9. Since at least 2018 through the date of the breach described below, Respondents have also disseminated or caused to be disseminated the following statements to consumers regarding the security of the Personal Information it collects:

- In standardized email responses to commonly asked questions, Residual Pumpkin claimed: "CafePress.com also pledges to use the best and most accepted methods and technologies to insure [sic] your personal information is safe and secure."

- On Residual Pumpkin's and PlanetArt's checkout pages: "Safe and Secure Shopping. Guaranteed."

10. Since at least August 2018 through the date of the February 2019 breach described below, Residual Pumpkin has disseminated or caused to be disseminated standardized email responses to commonly asked questions from shopkeepers containing the following statements regarding the security of the Personal Information it collects:

- Please keep in mind, your Social Security ID # is sensitive information and it is sent form [sic] an unsecured email. If you have an EIN number, you can use that number in place of the SSN.

  If you do not have an Employer/Employee Identification Number you can file for a EIN. Below is a link to this form. Please note our servers are secure.

- If you do not wish to use your social security number to receive your commission checks, you can file for an EIN. Below is a link to this form.

  http://www.irs.gov/pub/irs-pdf/fss4.pdf

  Please note our servers are secure and your personal information is stored safely in our system.

- To receive your full commission amount, you must provide your tax information. Information collected here will be used solely to fulfill IRS requirements, and will not be used in any other manner. Additionally your information will be secure. The following is a link for more information on our Secure Server….

Respondents' Data Security Practices

11. Since at least January 2018, Respondents have been responsible for a number of practices that failed to provide reasonable security for the Personal Information stored on its network. Among other things:

a. Respondents failed to implement readily-available protections, including many low-cost protections, against well-known and reasonably foreseeable

vulnerabilities, such as "Structured Query Language" ("SQL") injection, Cascading Style Sheets ("CSS") and HTML injection, cross-site scripting ("XSS"), and cross-site request forgery ("CSRF") attacks, that could be exploited to gain unauthorized access to Personal Information on its network;

b. Residual Pumpkin stored Personal Information such as Social Security numbers and security questions and answers in clear, readable text;

c. Residual Pumpkin failed to implement reasonable measures to protect passwords, such as using the SHA-1 hashing algorithm, deprecated by the National Institute of Standards and Technology in 2011, instead of more secure algorithms, and failing to use a "salt"—random data that makes attacks (*e.g.*, brute force, rainbow tables) against cryptographically protected passwords harder;

d. Residual Pumpkin failed to implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics, or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents;

e. Residual Pumpkin failed to implement patch management policies and procedures to ensure the timely remediation of critical security vulnerabilities and used obsolete versions of database and web server software that no longer received patches;

f. Residual Pumpkin failed to establish or enforce rules sufficient to make user credentials (such as user name and password) hard to guess. For example, employees and consumers, including shopkeepers, were not required to use complex passwords. Accordingly, they could select the same word, including common dictionary words, as both the password and user ID, or a close variant of the user ID as the password;

g. Residual Pumpkin created unnecessary risks to Personal Information by storing it indefinitely on its network without a business need;

h. Residual Pumpkin failed to implement reasonable procedures to prevent, detect, or investigate an intrusion. For example, Residual Pumpkin failed to:

   i. log sufficient information to adequately assess cybersecurity events;

   ii. properly configure vulnerability testing and scope penetration testing of the network and web application;

   iii. comply with its own written security policies; and

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;

ii. adequately assess the extent of and remediate malware infections after learning that devices on its network were infected with malware; and

iii. take adequate measures to prevent account takeovers through password resets using data known to have been obtained by hackers.

February 2019 Breach of Consumer Data

12. In or around February 2019, a hacker exploited the failures set forth in Paragraph 11. The hacker found Personal Information stored on Residual Pumpkin's network, including: more than twenty million unencrypted email addresses and encrypted passwords; millions of unencrypted names, physical addresses, and security questions and answers; more than 180,000 unencrypted Social Security numbers; and, for tens of thousands of payment cards, the unencrypted last four digits of the card together with the unencrypted expiration dates. The hacker exported this information over the Internet to outside computers.

13. On March 11, 2019, Residual Pumpkin received notice of a security incident involving an intrusion into its network. An individual stated that he "believe[s] hackers have access to your customer [database]. The data is currently for sale in certain circles." The individual demonstrated the existence of a SQL injection vulnerability that allowed direct access to Residual Pumpkin's database containing consumer information.

14. On March 12, 2019, Residual Pumpkin confirmed that the individual had identified a legitimate vulnerability. On March 13, 2019, Residual Pumpkin issued a patch to remediate the vulnerability.

15. On March 26, 2019, Residual Pumpkin investigated a recent spike in suspected fraudulent orders and concluded the orders were caused by someone "testing ou[t] stolen credit cards."

16. The breach of Respondents' consumers' credentials increased the risk that its website would be used by fraudsters in possession of credit card numbers, individuals sometimes known as "carders." "Carders" are known to target certain websites to place fraudulent orders using stolen credit card numbers.

17. "Carders" often share lists of "cardable" websites, those on which stolen credit cards can easily be used because, for example, Respondents did not use an address verification service to validate the billing addresses of credit cards used for payments. Since at least 2015, carders have listed CafePress on publicly available forums as a cardable website.

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 number of "carders." The letter requested that Residual Pumpkin notify users of compromised accounts to "prevent[] further compromise of accounts owned by users."

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 data in Residual Pumpkin's custody had been obtained by hackers. These posts appeared on 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 from Residual Pumpkin's network.

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 cafepress.com 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 sent breach notification letters and emails to government agencies and affected consumers and posted a notice of the breach via a banner at the top of the CafePress website from September 5, 2019 to October 12, 2019. Residual Pumpkin offered two years of free identity theft insurance and credit monitoring services to consumers whose Social Security numbers or tax identification numbers were exposed.

25. Residual Pumpkin told individuals, law enforcement, and regulators that the April 15, 2019 password reset effectively blocked the passwords from subsequent unauthorized use. However, until at least November 19, 2019, Residual Pumpkin continued to allow passwords to be reset through Residual Pumpkin's website simply by answering a security question associated with an email address—information that was stolen in the breach—without confirming that the individual attempting to change the password controlled that email address. Thus, until November 2019, anyone with access to the breached data could take over another user's account.

26. Even though the passwords were encrypted, as noted above, Residual Pumpkin used a deprecated encryption algorithm and failed to use a salt. Scammers were thus able to recover the passwords and use them in extortion attempts. Scammers sent emails to consumers claiming they had obtained damaging Personal Information by hacking into the consumer's computer and would release it unless paid in bitcoin. To provide credibility to their claims, scammers included the consumer's recovered password to Respondents' website in the extortion message.

27. Residual Pumpkin withheld up to $25 in otherwise payable commissions owed to shopkeepers who closed their account after the breach.

Other Security Breaches

28. The February 2019 breach was not the only incident that Residual Pumpkin experienced as a result of these security failures. Shopkeepers' accounts have been hacked and visitors to those shopkeepers' sites redirected to websites controlled by hackers. Moreover, through at least January 2018, and when Residual Pumpkin identified shopkeeper accounts that it determined had been hacked, Residual Pumpkin not only closed those accounts, but also assessed the shopkeepers a $25 account closure fee.

29. Residual Pumpkin also experienced a number of malware infections. In May 2018, Residual Pumpkin determined that a number of its servers were infected with malware but failed to investigate the cause of infection and instead merely fixed the affected servers.

30. In August 2018, Residual Pumpkin became aware that an employee had been targeted by multiple phishing attempts. A scan showed the employee's computer was infected with malware, including a backdoor bot, a "Trojan" downloader, and a password stealer. Additionally, the employee's email account had been configured for months to forward all incoming email to unknown third-party email addresses.

31. In response to this security incident, Residual Pumpkin replaced the particular computer that was infected, but failed to take reasonable steps to detect, remediate, and prevent similar infections on other devices on its network.

32. Because of Residual Pumpkin's failure to implement reasonable safeguards in response to the discovery of malware-based phishing attacks, other devices on Residual Pumpkin's network remained vulnerable to malware. In fact, the same type of malware that had been found in August 2018 was found on the payroll administrator's computer in February 2019.

33. In April, May, and September 2019, an identity thief or thieves used Personal Information belonging to three Residual Pumpkin employees to try to change the employees' payroll direct deposit information. Only after the third incident did Residual Pumpkin at last begin an investigation.

Injury to Consumers

34. Consumers have likely suffered actual injury as a result of Respondents' data security failures. Breached Personal Information, such as that stored in Respondents' system, is often used to commit identity theft and fraud. For example, as noted above, Personal Information exfiltrated from Respondents' system, 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 Respondents' consumers.

35. Residual Pumpkin's failure to respond adequately to multiple reports of a security breach 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. Residual Pumpkin's insecure password reset procedure further exacerbated the risks to consumers' Personal Information, as those with access to the breached information could take over users' accounts even after Residual Pumpkin had reset their passwords.

36. Consumers had no way of independently knowing about Respondents' security failures and could not reasonably have avoided possible harms from such failures.

Privacy

37. Until in or around February 2020, Residual Pumpkin disseminated or caused to be disseminated a privacy policy (Exhibit A). This privacy policy included the following statements:

> **How we use your information**
> . . . .
> In accordance with your choices when you registered with us, we may use information you give us or information we collect about you to:
> - Provide, maintain, and improve the Websites for internal or other business purposes;
> - Fulfill requests for information;
>
> ***
>
> **Emails, Newsletters, and other Communications:**
> When you create an account through our Websites, you are required to provide us with an accurate e-mail address through which we may contact you. The choices you make during the registration through our Websites or apps constitute your express acknowledgment of whether CafePress may use your e-mail address to communicate with you about product offerings from CafePress, its affiliates, selected third parties, and/or partners.
>
> ***

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 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 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."

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-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."

42. Residual Pumpkin obtained Privacy Shield certification in June 2018 and has had an active certification since then, except from June 12, 2019 through July 23, 2019.

43. The Privacy Shield Principles include the following:

> CHOICE [Principle 2]: (a) An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.
>
> SECURITY [Principle 4]: (a) Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.
>
> ACCESS [Principle 6]: (a) Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the

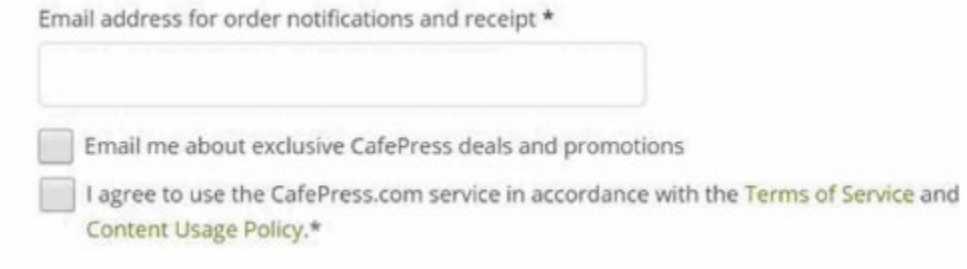
Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

44. Although the European Court of Justice determined on July 16, 2020 that the EU-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 inadequate, those decisions do not change the fact that Residual Pumpkin represented to consumers that it was certified under both Privacy Shield frameworks, and as such, would fully comply with the Principles, including Principles 2, 4, and 6.

Privacy Practices

45. When consumers completed online orders, Respondents have required them to submit their email address as a mandatory input field. Respondents have provided a notice above the field stating, "Email address for order notifications and receipt."

46. In certain markets, Residual Pumpkin included an additional checkbox to obtain consumer consent to receive marketing emails.



47. However, users would receive marketing emails when they provided their email during checkout, even though the input box only explained that Residual Pumpkin would use the email address "for order notifications and receipt." Similarly, where Residual Pumpkin provided an additional checkbox to seek consumers' opt-in consent to receive marketing emails, as shown in Paragraph 46 above, consumers would receive marketing emails even if they left the checkbox unchecked. Residual Pumpkin was aware that its practices were inconsistent with its stated practices since at least August 2018.

48. Residual Pumpkin has also failed to honor its commitments related to deleting information. Since June 19, 2018, Residual Pumpkin claimed it would delete information upon request from residents of the EEA and Switzerland. In fact, until November 2019 Residual Pumpkin only deactivated user accounts when it received such requests but did not delete the associated account information. Because of this failure to honor deletion requests, information from many consumers who had requested before the February 2019 breach that Residual Pumpkin delete their information was exposed in the breach.

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 implemented reasonable measures to protect Personal Information against unauthorized access.

51. In fact, as set forth in Paragraph 11, Respondents did not implement reasonable measures to protect Personal Information against unauthorized access. Therefore, the representation set forth in Paragraph 50 is false or misleading.

Count II
Response to Data Security Incident Misrepresentations

52. As described in Paragraphs 19 and 24-25, Respondents have represented, directly or indirectly, expressly or by implication, that they took appropriate steps to secure consumer account information following security incidents.

53. In fact, as set forth in Paragraph 25, Respondents had not taken appropriate steps to secure access to consumer accounts following security incidents. Consumer accounts remained at risk even after the passwords had been reset. Therefore, the representation set forth in Paragraph 52 is false or misleading.

Count III
Unfair Data Security Practices

54. As described in Paragraph 11, Respondents' failure to employ reasonable data security measures to protect Personal Information caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice.

Count IV
Data Collection and Use Misrepresentation

55. As described in Paragraphs 37, 45, and 46, Respondents have represented, directly or indirectly, expressly or by implication, that they would use email addresses only for order notification and receipt.

56. In fact, as described in Paragraph 47, Respondents did not use email addresses only for order notification and receipt. Respondents sent marketing emails to consumers irrespective of whether they consented to receive such emails. Therefore, the representation set forth in Paragraph 55 is false or misleading.

Count V
Misrepresentation Relating to Privacy Shield Frameworks

57. As described in Paragraph 37, Respondents have represented, directly or indirectly, expressly or by implication, that they adhered to the EU-U.S. and the Swiss-U.S. Privacy Shield frameworks, including the principles of Choice, Security, and Access.

58. In fact, as described in Paragraphs 11 and 43-49, Respondents did not adhere to the Privacy Shield Principles of Choice, Security, and Access. Therefore, the representation set forth in Paragraph 57 is false or misleading.

Count VI
Misrepresentation Relating to Deletion of Consumer Data

59. As described in Paragraph 37, Respondents have represented, directly or indirectly, expressly or by implication, that they honored requests from residents of the EEA and Switzerland to erase data and restrict the use of personal data for direct marketing.

60. In fact, as described in Paragraph 48, Respondents did not honor requests from residents of the EEA and Switzerland to erase data and restrict the use of personal data for direct marketing. Therefore, the representation set forth in Paragraph 59 is false or misleading.

Count VII
Unfair Withholding of Payable Commissions After Security Breach

61. As described in Paragraphs 27 and 28, Respondents withheld payable commissions owed to shopkeepers whose accounts were closed after a security breach.

62. Withholding payable commissions owed to shopkeepers whose accounts were closed after a security breach is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice.

Violations of Section 5

63. The acts and practices of Respondents as alleged in this complaint constitute unfair or 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 23rd day of June, 2022, has issued this complaint against Respondents.

By the Commission.

April J. Tabor
Secretary

SEAL:

Exhibit A

You may not use false or misleading Content to market and promote your shops and products. Some examples of false and misleading information are:

- Making claims that the proceeds from sales will go to a charity without first obtaining permission from such charity to use their name in connection with product sales, and complying with all applicable laws relating to charity fundraising;
- Using a third party trademark to market your content (e.g. using "Gucci"® in your product descriptions, titles, tags or other SEO text on your CafePress shop); and
- Spamming or attempting to deliberately subvert the results of the CafePress directory or search engine with false, misleading, or unnecessarily repetitive information (e.g., tag spamming or artificially increasing your CafePress search results rankings).

Back To Top

CafePress Privacy Statement

Effective: June 19, 2018

CafePress values the trust you place in us when you use CafePress.com and our affiliated websites, applications or tools (collectively, our "Websites"). Your privacy and trust are important to us and who we are as a company. This Privacy Statement (the "Privacy Statement" or the "Statement") describes how we collect, use, disclose, retain, and protect your information when you interact with our Websites

For individuals residing in the EEA or Switzerland, please click here to find out more information.

When this Privacy Statement applies

This Privacy Statement applies to any Website that links to it, as well as information we collect when you interact with us through social media or other websites and online services. It does not apply to non-CafePress websites and mobile applications that may link to the Websites or be linked to or from the

Websites; please review the privacy policies on those websites and applications directly to understand their privacy practices.

BY USING OUR SERVICES AND MAKING THE CHOICES YOU MADE WHEN REGISTERING WITH US, YOU ARE ACCEPTING THE TERMS OF THIS PRIVACY STATEMENT AND OUR USER AGREEMENT, AND YOU ARE CONSENTING TO OUR COLLECTION, USE, DISCLOSURE, RETENTION, AND PROTECTION OF YOUR PERSONAL INFORMATION AS DESCRIBED IN THIS PRIVACY STATEMENT. IF YOU DO NOT PROVIDE THE INFORMATION WE REQUIRE, WE MAY NOT BE ABLE TO PROVIDE ALL OF OUR SERVICES TO YOU.

We may make changes to this Statement from time to time. We will post any changes, and such changes will become effective when they are posted. Your continued use of our Websites following the posting of any changes will mean you accept those changes.

Information we collect about you

We collect, process, and retain information from you and any devices (including mobile devices) you may use when you use our Websites or Services, register for an account with us, provide us information on a web form, update or add information to your account, participate in community discussions, chats, or dispute resolution, or when you otherwise correspond with us. Below we describe the different types of information we collect from you and the devices you use when you interact with our Websites.

Information You Give Us: Some of the Websites may include features or services that permit you to enter contact information and other information about you. We collect and store any information you enter on our Websites. This may include your name, mailing address, ZIP code, phone number, email address, and/or payment information.

Information About Your Interaction With Our Websites: We collect information about your interactions with our Websites, such as the purchases you make or the advertisements you view.

Information Collected Automatically: When you interact with our Websites, certain information about your use of our Websites is automatically collected. This information includes computer and connection information such as statistics on your page views, traffic to and from our Websites, referral URL, ad data, your IP address, and device identifiers; this information may also include your browsing history, transaction history, and your web log information.

Most of this information is collected through "cookies," web beacons, tagging and other tracking technologies, as well as through your web browser or device (e.g., IP address, MAC address, browser version, etc.), to help enable you to shop on our Websites, and enable us to enhance or personalize your online browsing and shopping experience. Most web browsers automatically accept cookies but, if you prefer, you can usually modify your browser setting to disable or reject cookies. If you delete your cookies or if you set your browser to decline cookies, some features of the Websites may not be available, work, or work as designed.

We use Google Analytics, a web analytics service provided by Google, Inc., on our Websites. Google Analytics uses cookies or other tracking technologies to help us analyze how users interact with and use the Websites, compile reports on the Websites' activity, and provide other services related to our Websites' activity and usage. The technologies used by Google may collect information such as your IP address, time of visit, whether you are a return visitor, and any referring website. The Websites do not use Google Analytics to gather information that personally identifies you. The information generated by Google

Analytics will be transmitted to and stored by Google and will be subject to Google's privacy policies. To learn more about Google's partner services and to learn how to opt out of tracking of analytics by Google, click here

Information From Social Media and Other Websites: When you interact with us or the Websites by a social media platform, (such as by clicking on a social media icon linked from our Websites), we may collect the personal information that you make available to us on that page, including your account ID or username and other information included in your posts. If you choose to log in to your CafePress account with or through a social networking service, CafePress and that service may share certain information about you and your activities.

How we use your information

We use your information to help us personalize and continually improve your experience on the Websites, including fulfilling your orders and requests for information, analyzing and compiling trends and statistics, and communicating with you.

In accordance with your choices when you registered with us, we may use information you give us or information we collect about you to:

- Provide, maintain, and improve the Websites for internal or other business purposes;
- Fulfill requests for information;
- Provide, produce, and ship the products that you order or the services you request;
- Provide customer support;
- Track and evaluate the use of the Websites;
- Communicate with you about your Customer Account, Content Owner Account, profile or transactions with us, or changes to our policies or terms;
- Send you information about features and enhancements on or to our Websites;
- Send you newsletters or other materials;
- Send you offers or other communications about our products and services, such as special or promotional events, including services, products, or events for which we collaborate or co-offer with a third party;
- Administer contests, sweepstakes, promotions, and surveys;
- Detect, investigate, and prevent activities that may violate our policies or be fraudulent or illegal;
- Optimize or improve our products, services and operations; and
- Perform statistical, demographic, and marketing analyses of users of the Websites and their viewing patterns.

Some of these uses of your information may be in connection with our legitimate interests in providing the Services.

We may combine information gathered from multiple portions of the Websites into a single record. We may also use or combine information that we obtain from our business records. Additionally, information

collected from a particular browser or device may be used with another computer or device that is linked to the browser or device on which such information was collected.

How we share your information with others

We do not share your personal information with third parties, except as set forth below. We may disclose information that does not specifically identify you, such as aggregate information, device identifiers or other unique identifiers, to third parties in any manner we deem appropriate. For information about how to manage your information and the choices you have, see how to limit the use of your information below.

Third-Party Service Providers: We may share the information collected via our Websites with service providers that perform functions on our behalf to help us provide and support the Websites and our products and Services, including, but not limited to: hosting, content syndication, content management, technical integration, marketing, analytics, customer service, and fraud protection. For example, we use third parties to process payments made to us and assist with product fulfillment and other operations. These third parties may have access to your personal information when needed to perform their functions. We require these service providers to maintain the confidentiality and security of all information we provide and use it only for the purpose of providing the services for which they have been engaged.

Business Partners and Other Third Parties: Based on the choices you made when registering, we may engage in activities that include sharing your information with unaffiliated third parties, such as business partners who provide products and services that we think you may be interested in. Before we share such information, we obtain your consent.

Sale, Assignment or Change of Control: We may change our ownership or corporate organization while providing the Websites. We may transfer to another entity or its affiliates or service providers some or all information about you in connection with, or during negotiations of, any merger, acquisition, sale of assets or any line of business, other change of ownership or control, or financial transaction. Under such circumstances, we would request the acquiring party to follow the practices described in this Privacy Statement. Nevertheless, we cannot promise that an acquiring party or the merged entity will have the same privacy practices or treat your information the same as described in this Privacy Statement.

Law Enforcement, Legal Process, and Emergency Situations: We may also use or disclose your information if required to do so by law or on the good-faith belief that such sharing is necessary to (a) conform to applicable law or comply with legal process served on us or our Websites; (b) protect and defend our rights or property, the Websites or our users; or (c) act to protect the personal safety of us, our employees and agents, other users of the Websites, or the public. In particular, if you are a Content Owner (as defined by our **User Agreement**), we may disclose your information to a third party that alleges that you have infringed their intellectual property rights through the products sold through our Websites. Similarly, if you allege that a Content Owner is infringing upon your intellectual property rights, we may disclose your information to that Content Owner.

Interest-based advertising

Like many websites, we use tracking technologies such as cookies, web beacons and similar technologies to record your preferences, track the use of our Websites and exposure to our online advertisements. We may also use these technologies to monitor traffic, improve the Websites, and make it easier to use and more relevant.

We partner with third party advertising companies who also use these tracking tools to provide advertisements on our Websites, as well as on other websites and applications about our products and Services that may be of interest to you. In accordance with your choices when registering with us, the advertisements you see may be based on information collected through cookies, web beacons and other tracking technologies from our Websites and on other third party websites you visit and mobile applications you use that participate in our advertising networks. They may also use persistent identifiers to track your Internet usage across other websites and mobile applications in their networks beyond the Websites. They may use this information to provide you with interest-based advertising or other targeted content. While we do not share information that personally identifies you with unaffiliated third parties for their own uses, such third parties may, with sufficient data from other sources, be able to personally identify you, unknown to us. To learn more about the third party collection and use of your information, please visit the Network Advertising Initiative and/or the Digital Advertising Alliance. Similarly, for information about how to manage your mobile app tracking settings, see How to limit the use of your information below.

Some content or applications, including advertisements, on the Websites may be served by unaffiliated third parties. We do not control these third parties' tracking technologies or how they may be used. If you have any questions about an advertisement, you should contact the responsible advertiser directly. We are not responsible for the content or privacy practices on any website not operated by CafePress to which our Websites link or that link to our Websites.

Your browser or device may include "Do Not Track" functionality. At this time, CafePress does not respond to browser "Do Not Track" signals.

How to access and modify your information

We take steps to ensure that the personal information we collect is accurate and up to date, and that you have the ability to access and make corrections to it. This includes:

1. Giving you the ability to see, review, and change your personal information by signing in to your account at CafePress.com.
2. Honoring any legal right, you might have to access, modify or erase your personal information. To request access and to find out whether any fees may apply, if permitted by applicable state, federal, or national law (outside of the United States), please contact privacy@cafepress.com.

We may not be able to delete your personal information without also deleting your user account. You will not be permitted to examine the personal information of any other person or entity. In order to verify your identity, you may be required to provide us with personal information prior to accessing any records containing information about you. We may not accommodate a request to change or delete personal information if we believe doing so would violate any law or legal requirement or cause the information to be incorrect.

How to limit the use of your information

In many instances, you have choices about the information you provide and limiting how we use your information. These choices, and any related consequences, are described in detail below.

Personal Information: You may choose not to provide your personal information, such as your name, mailing address, ZIP code, phone number, email address, or payment information, but then you might not be able to take advantage of many features of our Websites and/or checkout.

Emails, Newsletters, and other Communications: When you create an account through our Websites, you are required to provide us with an accurate e-mail address through which we may contact you. The choices you make during the registration through our Websites or apps constitute your express acknowledgment of whether CafePress may use your e-mail address to communicate with you about product offerings from CafePress, its affiliates, selected third parties, and/or partners. While you cannot opt-out of receiving notifications and other communications regarding your account or your transactions, you can opt-out of receiving newsletters and promotional emails and other marketing communications from us by using the "unsubscribe" feature in our marketing e-mails or contacting Customer Service.

Location Tracking: Most mobile devices allow you to control or disable the use of location services by any application on your mobile device through the device's settings' menu.

Online Tracking and Interest-Based Advertising: You also have choices to limit some tracking mechanisms that collect information when you use the Websites. Many web browsers automatically accept cookies, but you can usually modify your browser's setting to decline cookies if you prefer. If you choose to decline cookies, certain features of our Websites, including the Websites themselves, may not function properly or remain accessible to you. In addition, you may also render some web beacons unusable by rejecting or removing their associated cookies. Note that if you choose to remove cookies, you may remove opt-out cookies that affect your advertising preferences.

You may opt out of tracking of analytics data by Google Analytics, one of our customer usage analytics providers, by clicking here.

Many of the third-party advertisers that place tracking tools on our Websites are members of programs that offer you additional choices regarding the collection and use of your information. You can learn more about the options available to limit these third parties' collection and use of your information by visiting the websites for the Network Advertising Initiative and the Digital Advertising Alliance, as well as the webpages for Facebook's ad preferences tool and privacy policy.

Similarly, you can learn about your options to opt-out of mobile app tracking by certain advertising networks through your device settings. For more information about how to change these settings for Apple, Android or Windows devices, see:

Apple: http://support.apple.com/kb/HT4228

Android: http://www.google.com/policies/technologies/ads/

Windows: http://choice.microsoft.com/en-US/opt-out

Please note that opting-out of advertising networks services does not mean that you will not receive advertising while using our Websites or on other websites, nor will it prevent the receipt of interest-based advertising from third parties that do not participate in these programs. It will, however, exclude you from interest-based advertising conducted through participating networks, as provided by their policies and choice mechanisms.

Updating your information

To discover whether we have information about you and to update that information, please contact us at privacy@cafepress.com.

How we secure your information

We do our best to provide you with a safe and convenient shopping experience. Our Websites incorporate physical, technical, and administrative safeguards to protect the confidentiality of the information we collect through the Websites, including the use of encryption, firewalls, limited access and other controls where appropriate. **While we use these precautions to safeguard your personal information, we cannot guarantee the security of the networks, systems, servers, devices, and databases we operate or that are operated on our behalf. 100% complete security does not presently exist anywhere online or offline.**

You can help protect the privacy of your own information by using encryption and other techniques to prevent unauthorized interception of your personal information. You are responsible for the security of your information when using unencrypted, public or otherwise unsecured networks.

Users outside the U.S.

If you use our Websites outside of the United States, you understand that we may collect, process, and store your personal information in the United States and other countries. The laws in the U.S. regarding personal information may be different from the laws of your state or country. Any such transfers will comply with safeguards as required by relevant law. If applicable, you may have a right to claim compensation for damages caused by a breach of relevant data protection laws.

Users in the European Union (EEA) and Switzerland

If you are a resident of the EEA 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.

Transfers: Personal data we collect may be transferred to, and stored and processed in, the United States or any other country in which we or our affiliates or subcontractors maintain facilities. We will ensure that transfers of personal data to a third country or an international organization are subject to appropriate safeguards. For more information regarding data received or transferred pursuant to the Privacy Shield Frameworks, see our **Privacy Shield Frameworks** section below.

Individual Rights: If you are a resident of the EEA or Switzerland, you are entitled to the following rights. **Please note:** In order to verify your identity, we may require you to provide us with personal information prior to accessing any records containing information about you.

- The right to access and rectify your data: You have the right to obtain information about our processing of personal data and a copy of your personal data that we store. You have the right to request that we update your personal data if it is inaccurate or incomplete.
- 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.
- The right to restrict or object to our processing: You have the right to restrict or object to our processing if we are processing your data based on legitimate interests or the performance of a task in the public interest as an exercise of official authority (including profiling); using your data for direct marketing (including profiling); or processing your data for purposes of scientific or historical research and statistics.

For questions and/or to opt-out and remove your personal information in our database please contact GDPR@cafepress.com.

You may have the right to make a GDPR complaint to the relevant Supervisory Authority. A list of Supervisory Authorities is available here: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm. If you need further assistance regarding your rights, please contact us using the contact information provided below and we will consider your request in accordance with applicable law. In some cases, our ability to uphold these rights for you may depend upon our obligations to process personal information for security, safety, fraud prevention reasons, compliance with regulatory or legal requirements, or because processing is necessary to deliver the services you have requested. Where this is the case, we will inform you of specific details in response to your request.

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/.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, CafePress is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission.

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.

Your right to access your personal data may be restricted in exceptional circumstances, including, but not limited to, when the burden or expense of providing this access would be disproportionate to the risks to your privacy in the case in question, or when the rights of persons other than you would be violated by the

provision of such access. If we determine that your access should be restricted in a particular instance, we will provide you with an explanation of our determination and respond to any inquiries you may have.

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.

In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

CafePress' accountability for personal data that it receives under the Privacy Shield and subsequently transfers to a third party is described in the Privacy Shield Principles. In particular, CafePress remains responsible and liable under the Privacy Shield Principles if third-party agents that it engages to process the personal data on its behalf do so in a manner inconsistent with the Principles, unless CafePress proves that it is not responsible for the event giving rise to the damage.

In compliance with the Privacy Shield Principles, CafePress commits to resolve complaints about your privacy and our collection or use of your personal information transferred to the United States pursuant to Privacy Shield. European Union and Swiss individuals with Privacy Shield inquiries or complaints should first contact CafePress at GDPR@cafepress.com.

CafePress has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbb.org/EU-privacy-shield/for-eu-consumers for more information and to file a complaint. This service is provided free of charge to you.

If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

Other important information

Users Under Thirteen: Our Services are intended for users ages 13 and older only. Accordingly, we will not knowingly collect or use any personal information from children that we know to be under the age of 13. In addition, we will delete any information in our database that we know originates from a child under the age of 13.

Users Thirteen to Seventeen: Prospective users between the ages of 13 and 17 can only use our Services under their parents or legal guardian's supervision. If you are between the ages of 13 and 17, you, your parent, or your legal guardian may request that we deactivate any of your personal information in our database and/or opt-out from receiving communications from us. If you wish to do so, please contact us at privacy@cafepress.com.

Notice to California Residents: If you are a California resident, California Civil Code Section 1798.83 permits you to request certain information regarding the disclosure of your personal information by

CafePress and its related companies to third parties for the third parties direct marketing purposes. To make such a request, please send your request, by mail, to:

CafePress Inc.
Attn: Legal - CA Privacy
11909 Shelbyville Road
Louisville, KY 40243

Questions or report a problem

For questions about our Privacy Statement, to make choices about receiving promotional communications, to update your personal information, or to place an order, you can contact CafePress Inc. by email, telephone or postal mail:

CafePress Customer Service
6901 A Riverport Drive
Louisville, KY 40258
(877) 809-1659
Email: Customer Service

Back To Top

Report an Alleged Infringement

CafePress Inc. ("CafePress") is an internet service provider ("ISP") providing an automated, Internet-based service for the design, marketing and sale of customized merchandise by users of our service. Our users are contractually prohibited from using the service in a manner that infringes the intellectual property rights of others.

We respect the intellectual property rights of others, and do NOT welcome infringing content. We encourage you to contact us if you believe that a user of our service has infringed your rights. We promptly evaluate all claims of infringement, and terminate the accounts of repeat infringers.

If you believe that a user of our service has infringed your intellectual property rights, please notify our Intellectual Property Rights Agent and provide all of the following:

1. A physical or electronic signature, and a statement that you are authorized to act on behalf of the owner of the copyright or other rights that have been allegedly infringed;
2. Identification of the copyright, trademark or other rights that have been allegedly infringed;
3. The URL or product number(s) used in connection with the sale of the allegedly infringing merchandise; ***Note: Simply including www.cafepress.com is not sufficient to identify what you are objecting to; you must provide the product number or store id part of the URL to identify the user.***
4. Your name, address, telephone number and email address;