

Complaint

IN THE MATTER OF

**RESIDUAL PUMPKIN ENTITY, LLC,
AND
PLANETART, LLC**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT

*Docket No. C-4769; File No. 192 3209
Complaint, June 23, 2022 – Decision, June 23, 2022*

This consent order addresses PlanetArt, LLC’s data security and privacy practices. The complaint alleges that Respondents violated Section 5(a) of the FTC Act by: (1) misrepresenting the measures CafePress took to protect Personal Information; (2) misrepresenting the steps CafePress took to secure consumer accounts following security incidents; (3) failing to employ reasonable data security practices; (4) misrepresenting how CafePress would use email addresses; (5) misrepresenting CafePress’ adherence to the Privacy Shield frameworks; (6) misrepresenting whether CafePress would honor deletion requests; and (7) unfairly withholding commissions payable to shopkeepers. The consent order prohibits PlanetArt from misrepresenting: (1) privacy and security measures it takes to prevent unauthorized access to Personal Information; (2) the extent to which PlanetArt is a member of any privacy or security program sponsored by a government, self-regulatory, or standard-setting organization; (3) privacy and security measures to honor users’ privacy choices; (4) information deletion and retention practices; and (5) the extent to which it maintains and protects the privacy, security, availability, confidentiality, or integrity of Personal Information. The order also requires PlanetArt to obtain initial and biennial data security assessments for 20 years.

Participants

For the *Commission*: M. Hasan Aijaz and Matthew Wilshire.

For the *Respondents*: Josh James and Jim Dudukovich, Bryan Cave Leighton Paisner.

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

Complaint

“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**

Complaint

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....

Complaint

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;

Complaint

- 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.

Complaint

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

Complaint

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.

Complaint

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;

Complaint

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

Complaint

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.”

Complaint

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.

Complaint

Email address for order notifications and receipt *

☐ Email me about exclusive CafePress deals and promotions
☐ I agree to use the CafePress.com service in accordance with the [Terms of Service](#) and [Content Usage Policy](#).*

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.

Complaint

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.

Decision and Order

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.

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of Respondent PlanetArt, LLC, named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the

Decision and Order

Commission, the draft Complaint would charge Respondent with violations of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission’s Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondent is PlanetArt, LLC, also doing business as CafePress, a Delaware company with its principal office or place of business at 23801 Calabasas Road, Suite 2005, Calabasas California 91302.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER**Definitions**

For purposes of this Order, the following definitions apply:

- A. **“Covered Incident”** means any instance in which any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization.
- B. **“Personal Information”** means individually identifiable information from or about an individual consumer, including: (1) a first and last name; (2) a physical address; (3) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (4) a telephone number; (5) date of birth; (6) a Social Security number; (7) driver’s license or other government issued identification number; (8) financial institution account number; (9) credit or debit card information; (10) a persistent identifier, such as a customer number held in a

Decision and Order

“cookie,” a static Internet Protocol (“IP”) address, a mobile device ID, or processor serial number; and (11) authentication credentials such as a user ID, password, and security questions and answers. For purposes of this definition, “consumer” includes any individual who is, or seeks to become, an employee, officer, or independent contractor of Respondent.

- C. **“Respondent”** means PlanetArt, LLC, also doing business as CafePress and its successors and assigns.

Provisions**I. Prohibition against Misrepresentations about Privacy and Security**

IT IS ORDERED that Respondent, Respondent’s officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, must not misrepresent in any manner, expressly or by implication:

- A. Respondent’s privacy and security measures to prevent unauthorized access to Personal Information;
- B. The extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization;
- C. Respondent’s privacy and security measures to honor the privacy choices exercised by users;
- D. Respondent’s information deletion and retention practices; and
- E. The extent to which Respondent otherwise protects the privacy, security, availability, confidentiality, or integrity of Personal Information.

II. Mandated Information Security Program

IT IS FURTHER ORDERED that Respondent, and any business that Respondent controls directly, or indirectly, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Personal Information, must, within sixty (60) days of issuance of this order, establish and implement, and thereafter maintain, a comprehensive information security program (“Information Security Program”) that protects the privacy, security, confidentiality, and integrity of such Personal Information. To satisfy this requirement, Respondent must, at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Information Security Program;

Decision and Order

- B. Provide the written program and any evaluations thereof or updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for Respondent's Information Security Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;
- C. Designate a qualified employee or employees to coordinate and be responsible for the Information Security Program;
- D. Assess and document, at least once every twelve (12) months and promptly (not to exceed forty-five (45) days) following a Covered Incident, internal and external risks to the privacy, security, confidentiality, or integrity of Personal Information that could result in the (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Personal Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information;
- E. Design, implement, maintain, and document safeguards that control for the internal and external risks Respondent identifies to the privacy, security, confidentiality, or integrity of Personal Information identified in response to sub-Provision II.D. Each safeguard must be based on the volume and sensitivity of the Personal Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Personal Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information. Such safeguards must also include:
 - 1. Technical measures to monitor all of Respondent's networks and all systems and assets within those networks to identify data security events, including unauthorized attempts to exfiltrate Personal Information from those networks;
 - 2. Policies and procedures to ensure that all code for web applications is reviewed for the existence of common vulnerabilities;
 - 3. Policies and procedures to minimize data collection, storage, and retention, including data deletion or retention policies and procedures;
 - 4. Encryption of all Social Security numbers on Respondent's computer networks;
 - 5. Data access controls for all databases storing Personal Information, including by, at a minimum, (a) restricting inbound connections to approved IP addresses, (b) requiring authentication to access them, and (c) limiting employee access to what is needed to perform that employee's job function;
 - 6. Policies and procedures to ensure that all devices on Respondent's network with access to Personal Information are securely installed and inventoried

Decision and Order

- at least once every twelve (12) months, including policies and procedures to timely remediate critical and high-risk security vulnerabilities and apply up-to-date security patches;
7. Replacing, and not adopting in the future, authentication measures based on the use of security questions and answers to access accounts with multi-factor authentication methods that use a secure authentication protocol, such as cryptographic software or devices or mobile authenticator applications; and
 8. Training of all of Respondent's employees, at least once every twelve (12) months, on how to safeguard Personal Information.
- F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, confidentiality, or integrity of Personal Information, and modify the Information Security Program based on the results;
- G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed 30 days) following a Covered Incident, and modify the Information Security Program based on the results. Such testing and monitoring must include vulnerability testing of Respondent's network(s) once every four months and promptly (not to exceed 30 days) after a Covered Incident, and penetration testing of Respondent's network(s) at least once every twelve (12) months and promptly (not to exceed 30 days) after a Covered Incident;
- H. Select and retain service providers capable of safeguarding Personal Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy, security, confidentiality, or integrity of Personal Information;
- I. Consult with, and seek appropriate guidance from, independent, third-party experts on data protection and privacy in the course of establishing, implementing, maintaining, and updating the Information Security Program; and
- J. Evaluate and adjust the Information Security Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision II.D of this Order, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Information Security Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program based on the results.

III. Independent Program Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision II of this Order titled Mandated Information Security Program, Respondent and any business that Respondent controls directly, or indirectly, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Personal Information must obtain initial and biennial assessments (“Assessments”):

- A. The Assessments must be obtained from one or more qualified, objective, independent third-party professionals (“Assessors”), who: (1) use procedures and standards generally accepted in the profession; (2) conduct an independent review of the Information Security Program; (3) retain all documents relevant to each Assessment for five (5) years after completion of such Assessment, and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents relating to the Respondent’s compliance with the Order may be withheld from the Commission by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim. Respondent may obtain separate assessments for (1) privacy and (2) information security from multiple Assessors, so long as each of the Assessors meet the qualifications set forth above.
- B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion.
- C. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment; and (2) each 2-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments.
- D. Each Assessment must, for the entire assessment period: (1) determine whether Respondent has implemented and maintained the Information Security Program required by Provision II of this Order, titled Mandated Information Security Program; (2) assess the effectiveness of Respondent’s implementation and maintenance of sub-Provisions II.A-J; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and (5) identify specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise of Respondent’s size, complexity, and risk profile; and (b)

Decision and Order

sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Respondent's management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent that Respondent revises, updates, or adds one or more safeguards required under Provision II of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

- E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit an unredacted copy of the initial Assessment and a proposed redacted copy suitable for public disclosure of the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re CafePress, FTC File No. 1923209." Respondent must retain an unredacted copy of each subsequent biennial Assessment as well as a proposed redacted copy of each subsequent biennial Assessment suitable for public disclosure until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

IV. Cooperation with Third Party Information Security Assessor

IT IS FURTHER ORDERED that Respondent, whether acting directly or indirectly, in connection with any Assessment required by Provision III of this Order titled Independent Program Assessments by a Third Party, must:

- A. Provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege.
- B. Provide or otherwise make available to the Assessor information about Respondent's network(s) and all of Respondent's IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network(s) and IT assets deemed in scope; and
- C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Information Security Program required by Provision II of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and

Decision and Order

maintenance of sub-Provisions II.A-J; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program.

V. Annual Certification

IT IS FURTHER ORDERED that Respondent must:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for Respondent's Information Security Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.
- B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re CafePress, FTC File No. 1923209."

VI. Covered Incident Reports

IT IS FURTHER ORDERED that Respondent, within thirty (30) days after Respondent's discovery of a Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;
- C. A description of each type of information that triggered any notification obligation to the U.S. federal, state, or local government entity;
- D. The number of consumers whose information triggered any notification obligation to the U.S. federal, state, or local government entity;

Decision and Order

- E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
- F. A representative copy of any materially different notice sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, “In re CafePress, FTC File No. 1923209.”

VII. Notice to Users

IT IS FURTHER ORDERED that, on or before fourteen (14) days after the date of the filing of this Order, Respondent must email an exact copy of the notice attached hereto as Exhibit A (“Notice”) to all consumers whose Personal Information was in the data breached from the website www.cafepress.com in 2019. Respondent shall not include with the Notice any other information, documents, or attachments.

VIII. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For 10 years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives with managerial or professional responsibilities for conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reports and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

Decision and Order

IX. Compliance Reports and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

- A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which:
 - 1. Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.
- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in: (a) any designated point of contact; or (b) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within 14 days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal

Decision and Order

Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, “In re CafePress, LLC, FTC File No. 1923209.”

X. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years. Specifically, Respondent, in connection with any conduct related to the subject matter of the Order, must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold;
- B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person’s: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. Copies or records of all consumer complaints and refund requests that relate to the privacy, security, and confidentiality of any Personal Information, whether received directly or indirectly, such as through a third party, and any response;
- D. A copy of each unique advertisement or other marketing material making a representation subject to this Order;
- E. A copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, security and confidentiality of any Personal Information, including any representation concerning a change in any website or other service controlled by Respondent that relates to the privacy, security, and confidentiality of Personal Information.
- F. For 5 years after the date of preparation of each Assessment required by this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent’s compliance with related Provisions of this Order, for the compliance period covered by such Assessment.
- G. For 5 years from the date received, copies of all subpoenas and other communications with law enforcement, if such subpoena or other communication relate to Respondent’s compliance with this Order.
- H. For 5 years from the date created or received, all records, whether prepared by or on behalf of Respondent, that demonstrate non-compliance OR tend to show any lack of compliance by Respondent with this Order.

Decision and Order

- I. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission.

XI. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within 10 days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XII. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Provision in this Order that terminates in less than 20 years;
- B. This Order's application to any Respondent that is not named as a defendant in such complaint; and
- C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had

Decision and Order

never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Attachment A

Subject line: Notice of FTC Settlement, 2019 Data Breach

Dear [Customer]:

We are contacting you about the 2019 breach of your information collected by the prior owners of CafePress. This notice is about that breach, which you may have already been notified of. We recently reached a settlement with the Federal Trade Commission, the nation's consumer protection agency, to resolve issues related to the 2019 data breach, and to make sure CafePress keeps your information safe.

What happened?

Before November 2019, CafePress didn't have reasonable practices to keep your information safe. When the company had a security breach, the following information about you may have been stolen: your email address, password, name, address, phone number, [Social Security number or Tax Identification number], answers to your security questions, and the expiration date and last four digits of your credit card.

What you can do to protect yourself

Here are some steps to reduce the risk of identity theft and protect your information online:

1. **Use different passwords for different accounts.** That way, if one account is hacked or has a data breach, your other accounts will be safer. And if you've reused your CafePress password or security questions on other websites, be sure to change them right away.
2. **Consider a password manager.** These are apps that store and manage strong, unique passwords and security questions for all the sites you use. Search independent review sites to find a free or paid password manager that works for you.
3. **Use multi-factor authentication** when it's an option. Multi-factor authentication can help secure your account by requiring two or more ways to verify it's you before granting access

Analysis to Aid Public Comment

to your account. This security feature makes it much harder for people to take advantage of stolen passwords or answers to security questions.

4. **Learn more** from the Federal Trade Commission at <https://www.ftc.gov/data-breach-resources> or at <https://www.IdentityTheft.gov>.

If you have any questions or concerns, please contact us at support@CafePress.com, at 1.844.988.0030 or reply to this email. Learn more about the settlement at [insert link].

Sincerely,

[Name of actual person]

[Title]

ANALYSIS OF CONSENT ORDERS TO AID PUBLIC COMMENT

The Federal Trade Commission (“Commission”) has accepted, subject to final approval, agreements containing consent orders from Residual Pumpkin Entity, LLC (“Residual Pumpkin”) and PlanetArt, LLC (“PlanetArt”) (collectively, “Respondents”).

The proposed consent orders (“Proposed Orders”) have been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreements and the comments received and will decide whether it should withdraw from the agreements and take appropriate action or make final the Proposed Orders.

This matter involves Respondents’ data security and privacy practices. Respondent Residual Pumpkin owned CafePress until September 2020, when Residual Pumpkin sold CafePress to Respondent PlanetArt. The CafePress website allows users, known as shopkeepers, to earn commissions from sales of merchandise offered to consumers. CafePress collected information such as names, email addresses, telephone numbers and—from shopkeepers—Social Security numbers (“Personal Information”). CafePress claimed to keep this information safe, but in fact failed to provide reasonable security. For example, CafePress failed to: guard against well-known and reasonably foreseeable threats, such as SQL injection and cross-site scripting attacks; encrypt Social Security numbers; and implement a process for receiving and addressing third-party security vulnerability reports. CafePress also claimed to adhere to principles set forth in the EU-U.S. and Swiss U.S. Privacy Shield frameworks, specifically that it would honor user requests to delete data and user choices about how email addresses would be used. Instead, CafePress failed to delete Personal Information when it was requested to do so and sent marketing emails to nearly all its consumers, even those who had not opted in to receive such messages. As a result of

Analysis to Aid Public Comment

CafePress' data security practices, consumers' Personal Information was stolen and sold on the dark web. CafePress learned of the breach but failed to notify affected consumers. After some shopkeepers learned of the breach and closed their accounts, CafePress withheld up to \$25 in payable commissions from each of those shopkeepers.

The complaint alleges that Respondents violated Section 5(a) of the FTC Act by: (1) misrepresenting the measures CafePress took to protect Personal Information; (2) misrepresenting the steps CafePress took to secure consumer accounts following security incidents; (3) failing to employ reasonable data security practices; (4) misrepresenting how CafePress would use email addresses; (5) misrepresenting CafePress' adherence to the Privacy Shield frameworks; (6) misrepresenting whether CafePress would honor deletion requests; and (7) unfairly withholding commissions payable to shopkeepers.

The Proposed Orders contain provisions designed to prevent Respondents from engaging in the same or similar acts or practices in the future.

Summary of Proposed Order with PlanetArt

Part I prohibits PlanetArt from misrepresenting: (1) privacy and security measures it takes to prevent unauthorized access to Personal Information; (2) the extent to which PlanetArt is a member of any privacy or security program sponsored by a government, self-regulatory, or standard-setting organization; (3) privacy and security measures to honor users' privacy choices; (4) information deletion and retention practices; and (5) the extent to which it maintains and protects the privacy, security, availability, confidentiality, or integrity of Personal Information.

Part II requires PlanetArt to establish and implement, and thereafter maintain, a comprehensive information security program that protects the privacy, security, confidentiality, and integrity of Personal Information.

Part III requires PlanetArt to obtain initial and biennial data security assessments for 20 years.

Part IV requires PlanetArt to disclose all material facts to the assessor and prohibits PlanetArt from misrepresenting any fact material to the assessment required by Part II.

Part V requires PlanetArt to submit an annual certification from a senior corporate manager (or senior officer responsible for its Security Program) that PlanetArt has implemented the requirements of the order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Part VI requires PlanetArt to notify the Commission of a "Covered Incident" within thirty days of discovering such incident.

Parts VII requires PlanetArt to provide notice to consumers to inform them of the breach and the settlement with the FTC.

Analysis to Aid Public Comment

Part VIII requires PlanetArt to submit an acknowledgement of receipt of the order, including all officers or directors and employees having managerial responsibilities for conduct related to the subject matter of the order, and to obtain acknowledgements from each individual or entity to which a PlanetArt has delivered a copy of the order.

Part IX requires PlanetArt to file compliance reports with the Commission and to notify the Commission of bankruptcy filings or changes in corporate structure that might affect compliance obligations.

Part X contains recordkeeping requirements for accounting records, personnel records, consumer correspondence, advertising and marketing materials, and claim substantiation, as well as all records necessary to demonstrate compliance with the order.

Part XI contains other requirements related to the Commission's monitoring of PlanetArt's order compliance.

Part XII provides the effective dates of the order, including that, with exceptions, the order will terminate in 20 years.

The purpose of this analysis is to facilitate public comment on the Proposed Orders, and it is not intended to constitute an official interpretation of the complaint or Proposed Orders, or to modify the Proposed Orders' terms in any way.

Complaint

IN THE MATTER OF

**HEALTH RESEARCH LABORATORIES, LLC,
WHOLE BODY SUPPLEMENTS, LLC,
AND
KRAMER DUHON**

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT

*Docket No. 9397; File No. X180007
Complaint, November 13, 2020 – Decision, June 24, 2022*

This consent order addresses Health Research Laboratories, LLC and Whole Body Supplements, LLC's advertising for Black Garlic Botanicals, BG18, The Ultimate Heart Formula, and Neupathic. The complaint alleges that Respondents violated Sections 5(a) and 12 of the FTC Act by disseminating false and unsubstantiated advertisements claiming that: (1) Black Garlic Botanicals, BG18, and The Ultimate Heart Formula will prevent, reduce the risk of, cure, mitigate, or treat cardiovascular disease, atherosclerosis, and/or hypertension; and (2) Neupathic will cure, treat, or mitigate diabetic neuropathy. The consent order bans Respondents from advertising, marketing, promoting, or offering for sale any dietary supplements and from making any disease prevention, reduction of risk, cure, mitigation, or treatment claim when advertising, marketing, promoting, or offering for sale any product.

Participants

For the *Commission*: Elizabeth J. Averill and Philip Z. Brown.

For the *Respondents*: Joel W. Reese and Joshua Russ, Reese Marketos LLP.

COMPLAINT

The Federal Trade Commission, having reason to believe that Health Research Laboratories ("HRL"), a limited liability company, Whole Body Supplements ("WBS"), a limited liability company, and Kramer Duhon, individually and as an owner and officer of HRL and WBS (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 HRL is a Nevada limited liability company with its principal office or place of business at 16250 Knoll Trail Drive, Dallas, TX 75248.
2. Respondent WBS is a Nevada limited liability company with its principal office or place of business at 16250 Knoll Trail Drive, Dallas, TX 75248.
3. Respondent Kramer Duhon is the Chief Operating Officer and managing member of HRL and the Chief Operating Officer and managing member of WBS. Individually or in concert with others, he controlled or had the authority to control the acts and practices of HRL and WBS, including the acts and practices alleged in this complaint. His principal office or place of business is 16250 Knoll Trail Drive, Dallas, TX 75248.