

**UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION**

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

**In the Matter of**

**RESIDUAL PUMPKIN ENTITY, LLC,  
a limited liability company,  
formerly d/b/a CAFEPRESS, and**

**PLANETART, LLC, a limited liability company,  
d/b/a CAFEPRESS.**

**DOCKET NO.**

**COMPLAINT**

The Federal Trade Commission, having reason to believe that Residual Pumpkin Entity, LLC, a limited liability company, and PlanetArt, LLC, a limited liability company (collectively, “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](http://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](http://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](http://www.cafepress.com), through which consumers nationwide and internationally can purchase customized merchandise.

7. In selling and promoting products through [www.cafepress.com](http://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](http://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](mailto: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](mailto: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

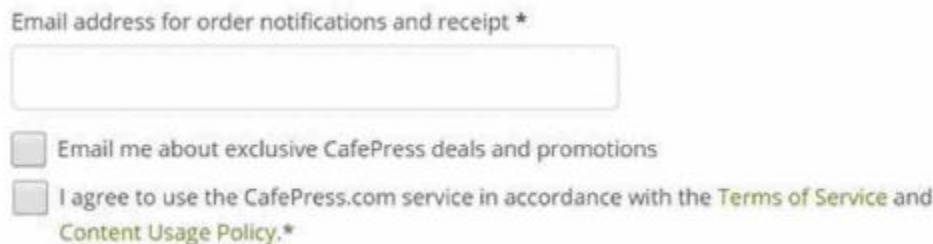
Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

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.



The screenshot shows a web form with the following elements:

- A label: "Email address for order notifications and receipt \*"
- An empty text input field.
- A checkbox with the text: "Email me about exclusive CafePress deals and promotions"
- A checkbox with the text: "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.

**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 \_\_\_\_\_ day of \_\_\_\_\_, 2021, has issued this complaint against Respondents.

By the Commission.

April J. Tabor  
Secretary

SEAL: