UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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.**	**FILE NO. 1923209** **AGREEMENT CONTAINING CONSENT ORDER**

The Federal Trade Commission ("Commission") has conducted an investigation of certain acts and practices of Residual Pumpkin Entity, LLC and PlanetArt, LLC (collectively "Proposed Respondents"). The Commission's Bureau of Consumer Protection ("BCP") has prepared a draft of an administrative Complaint ("draft Complaint"). BCP and PlanetArt, LLC ("Settling Respondent") through its duly authorized officer enter into this Agreement Containing Consent Order ("Consent Agreement") to resolve the allegations in the attached draft Complaint through a proposed Decision and Order to present to the Commission, which is also attached and made a part of this Consent Agreement.

IT IS HEREBY AGREED by and between Settling Respondent and BCP, that:

1. The Settling Respondent is PlanetArt, LLC, also doing business as CafePress, a Delaware limited liability company with its principal office or place of business at 23801 Calabasas Road, Suite 2005, Calabasas California 91302.

2. Settling Respondent neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Settling Respondent admits the facts necessary to establish jurisdiction.

3. Settling Respondent waives:

   a. Any further procedural steps;

   b. The requirement that the Commission's Decision contain a statement of findings of fact and conclusions of law; and

   c. All rights to seek judicial review or otherwise to challenge or contest the validity of the Decision and Order issued pursuant to this Consent Agreement.

4. This Consent Agreement will not become part of the public record of the proceeding unless and until it is accepted by the Commission. If the Commission accepts this Consent Agreement, it, together with the draft Complaint, will be placed on the public record for 30 days and information about them publicly released. Acceptance does not constitute final approval, but it serves as the basis for further actions leading to final disposition of the matter. Thereafter, the Commission may either withdraw its acceptance of this Consent Agreement and so notify Settling Respondent, in which event the Commission will take such action as it may consider appropriate, or issue and serve its Complaint (in such form as the circumstances may require) and decision in disposition of the proceeding, which may include an Order. *See* Section 2.34 of the Commission's Rules, 16 C.F.R. § 2.34 ("Rule 2.34").

5. If this agreement is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to Rule 2.34, the Commission may, without further notice to Settling Respondent: (1) issue its Complaint corresponding in form and substance with the attached draft Complaint and its Decision and Order; and (2) make information about them public. Settling Respondent agrees that service of the Order may be effected by its publication on the Commission's website (ftc.gov), at which time the Order will become final. *See* Rule 2.32(d). Settling Respondent waives any rights it may have to any other manner of service. *See* Rule 4.4.

6. When final, the Decision and Order will have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other Commission orders.

7. The Complaint may be used in construing the terms of the Decision and Order. No agreement, understanding, representation, or interpretation not contained in the Decision and Order or in this Consent Agreement may be used to vary or contradict the terms of the Decision and Order.

8. Settling Respondent agrees to comply with the terms of the proposed Decision and Order. Settling Respondent understands that it may be liable for civil penalties and other relief for each violation of the Decision and Order after it becomes final.

PLANETART, LLC

By:_____
Roger Bloxberg
Chief Executive Officer, PlanetArt, LLC
Date:_____

_____
Joshua A. James
James A. Dudukovich
Bryan Cave Leighton Paisner
Attorneys for PlanetArt, LLC
Date:_____

FEDERAL TRADE COMMISSION

By:_____
M. Hasan Aijaz
Matthew J. Wilshire
Attorneys, Bureau of Consumer Protection

APPROVED:

_____
Matthew Wernz
Director
Southwest Region

_____
Samuel Levine
Acting Director
Bureau of Consumer Protection

Date:_____

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	**DECISION AND ORDER**
RESIDUAL PUMPKIN ENTITY, LLC, a limited liability company, formerly d/b/a CAFEPRESS, and	**DOCKET NO. C-**
PLANETART, LLC, a limited liability company, d/b/a CAFEPRESS.	

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 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:

1. "**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.

2. "**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 "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.

3. "**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;

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 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) 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 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;

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 wwww.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.

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 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.

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 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.

April J. Tabor
Secretary

SEAL:
ISSUED:

Exhibit 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 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]