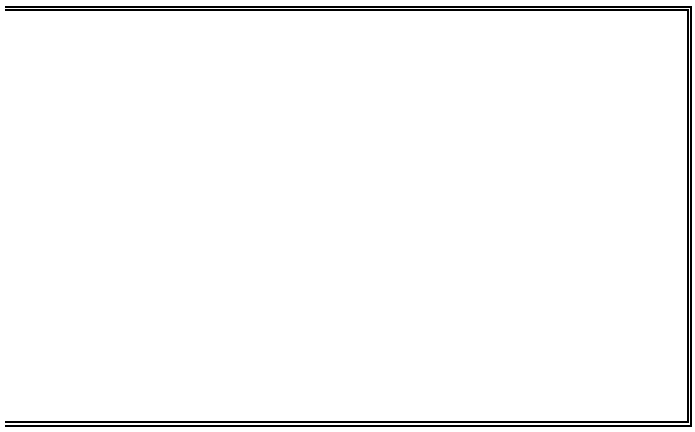


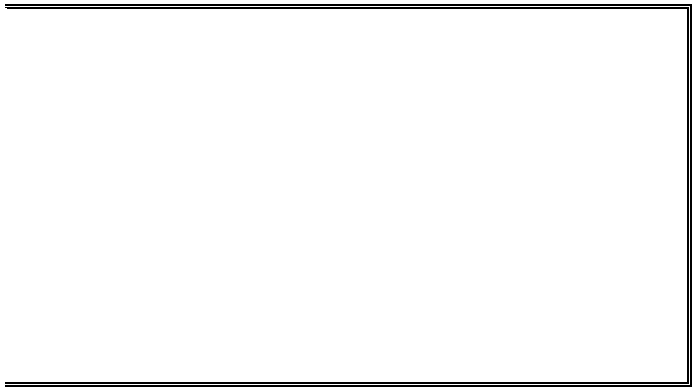
4. This Consent Agreement will not become part of the public record of the proceeding unless and until it is accepted by the Commission. If the Commission accepts this Consent Agreement, it, together with the draft Complaint, will be placed on the public record for 30 days and information about them 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 If this agreement is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to Rule 2.34, the Commission may, without further notice to Settling Respondent: (1) issue its Complaint corresponding in form and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.



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.

be

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-f -0.007 Twctr

accesdadur, i muoy ry rauev(o t)-hJ0.00

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

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;

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

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. Ac0(l02.10(n02 Tc w 3 (r12 d)1 (r (c6,)at 4 35 o(st fe)-1 2p)12 Tc w 3epc6,)ar2 (C)-2st st ferC(mu)c w 3

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 consumer (u)5 (ns)4 5ee Monts am(pr)-2 (.66)1 (e)1 (rn2 (ie)6 (t)3 (e)-1 2(r)-2 (vi)-2d
is Or7eiiisthe Commissionisia wnus6 o[c)1 (o)2 pthne
S(s)1 (4-1 (c)-1 (t)3 (i)-2 ((s)-1 9on a)-1 (n2(u)50 (of)-2 e)1 (rn2 (ie) F(s)1Te)6 ()-2 A(n)2 (s)-1 (t)-2,T

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:

[KEW$

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]