SHUTTERFLY INC

February 24, 2022

CONFIDENTIAL TREATMENT REQUESTED

BY U.S. MAIL

Office of the Attorney General
Consumer Protection Bureau
33 Capitol St.
Concord, NH 03301

To Whom It May Concern:

We are resending this notice, originally sent on February 18, 2022, as we believe the sample individual letter may not have been enclosed.

On behalf of Shutterfly, LLC, and pursuant to N.H. Rev. Stat. § 359-C:20(I)(B), this letter provides notice of a cybersecurity incident.

On or about December 13, 2021, Shutterfly learned that it was the victim of a ransomware attack when the company found that files on computers in various parts of its corporate network had been encrypted. The attack involved some limited disruption to corporate systems and also the theft of certain data. With the support of outside cybersecurity experts, we took steps to find the facts, to ensure the ongoing security of our systems, and to mitigate the risk of further unauthorized access. We have reported the incident to law enforcement and are cooperating with them.

We believe that the threat actor activity began on or about on December 3, 2021, and that the attack was carried out by the Conti ransomware group. Affected systems are now operational. Our investigation is continuing with a priority of determining what data was accessed or exfiltrated by Conti.

We learned that an individual in New Hampshire was affected on January 18, 2022. To date, Shutterfly has identified 1 New Hampshire resident whose personal information may have been affected. Shutterfly anticipates sending this individual formal notice on February 18, 2022 via letter. A sample of the notification letter is enclosed. The affected data included the following: name, address, Social Security Number, date of birth,

financial account number, and routing number. In addition, due to the nature of the documents accessed, other employment related information may have been taken, such as salary and compensation information, or information related to FMLA leave or workers' compensation claims. We are not aware of any resulting identity theft, fraud, or financial loss to individuals.

As stated in the attached sample notice, Shutterfly is offering to provide individuals 24 months of free identity theft and credit monitoring services through Equifax. We have established a call center to respond to individuals' questions.

Efforts to further secure our systems are ongoing. Shutterfly promptly undertook a number of measures to enhance its security and improve its capabilities to detect cyber threats and avoid unauthorized activity, including: 1) resetting passwords and enhancing password controls, 2) improving monitoring and multi-factor authentication ("MFA") controls, and 3) adding additional hardening measures.

If our ongoing investigation leads to any material updates, we will be in touch with your office again. Shutterfly takes the protection of personal information seriously and is committed to answering any questions that your office may have. Please do not hesitate to contact me at sharon.segev@shutterfly.com or (650) 610-5115.

***

In accordance with N.H. Rev. Stat. § 91-A:5(IV), (XI) and/or other applicable laws and regulations, Shutterfly requests that confidential treatment be provided to this letter and to any notes, memoranda, or other records created by or at the direction of the Office of the Attorney General, its officers, or staff members that reflect, refer to, or relate to this letter (the "Confidential Materials"). Shutterfly also requests that Confidential Materials be kept in a non-public file and that only staff of your Office have access to them. Should your Office receive any request for the Confidential Materials pursuant to the New Hampshire Right to Know Law or otherwise, Shutterfly requests that the undersigned be immediately notified of such request and be furnished a copy of all written materials pertaining to such request.

Respectfully yours,

Sharon Segev
Chief Legal & People Officer

Enclosures

SHUTTERFLY INC

Shutterfly Inc.
<Address 1>
<Address 2>
<City> <State> <ZIP>

<Date>

<First Name> <Last Name>
<Address 1>
<Address 2>
<City> <State> <ZIP>

Dear <First Name> <Last Name>:

We are writing to inform you of a data security incident at Shutterfly that may involve some of your personal information.

What Happened?

An unauthorized third party gained access to our network. This was what is known as a "ransomware" attack. The attacker both locked up some of our systems and accessed some of the data on those systems. This included access to personal information of certain people, including you. We believe the access occurred on or about December 3, 2021. We discovered the incident on December 13, 2021.

What Information Was Involved?

Some of your personal data was among the data affected. This included: <Exposure>. In addition, due to the nature of the documents accessed, other employment related information may have been taken, such as salary and compensation information, or information related to FMLA leave or workers' compensation claims.

What We Are Doing

We quickly took steps to restore and secure our systems. We brought in outside cybersecurity experts. We are continuing to investigate, with their help. We continue to focus on improving our security based on what we learn. We have notified law enforcement.

We are offering you two years of credit monitoring for free from Equifax. To take advantage of this offer see the included instructions.

What You Can Do

We strongly encourage you to contact Equifax and take advantage of the two years of free service. Carefully review your accounts for any suspicious activity and remain vigilant. You may wish to change the password and security questions associated with your online accounts. If you see suspicious activity, notify the organization where you hold the account. Also notify any relevant government agency, such as the IRS, the Social Security Administration, or state DMV.

Attached to this letter are helpful resources on how to protect your personal information.

For More Information

Keeping your personal data secure is important to us, and we regret the understandable concern this incident has created. If you have any questions, call **1-866-389-3602**.

Sincerely,

The Shutterfly Team

EQUIFAX®

<First Name> <Last Name>
Enter your Activation Code: **<Activation Code>**
Enrollment Deadline: **May 31, 2022**

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of **<Activation Code>** then click "Submit"

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. You can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com , calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at www.annualcreditreport.com/manualRequestForm.action Credit reporting agency contact details are provided below.

Equifax:	**Experian:**	**TransUnion:**
equifax.com	experian.com	transunion.com
equifax.com/personal/credit-report-services	experian.com/help	transunion.com/credit-help
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
866-349-5191	888-397-3742	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado and Illinois residents: You may obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Georgia, Maryland, New Jersey, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For New York residents: You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12224-0341, www.ag.ny.gov/home.html 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, www.dos.ny.gov/consumerprotection 1-800-697-1220.

For Rhode Island residents: You may obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes. You may also contact the Rhode Island Office of the Attorney General, 150 South Main Street Providence, Rhode Island 02903, www.riag.ri.gov (401) 274-4400.