FENWICK & WEST LLP

555 CALIFORNIA STREET, 12TH FLOOR SAN FRANCISCO, CA 94104

TEL 415.875.2300 FAX 415.281.1350 WWW.FENWICK.COM

March 28, 2018

TYLER G. NEWBY

EMAIL TNEWBY@FENWICK.COM
Direct Dial (415) 875-2495

Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Unauthorized Access to Shutterfly, Inc. Employee Personal Information

To Whom It May Concern,

Pursuant to New Hampshire Revised Statute Section 359-C:20, I am writing to notify you that Shutterfly, Inc. recently discovered a security incident involving unauthorized access to a Workday database in which employee personal information was stored. Unauthorized access to this database was obtained through a fraudulent account log-in. Although Shutterfly has not yet determined when the unauthorized access to the system first occurred, evidence indicates that the system was accessed without authorization on January 11, 2018. The personal information of 6 New Hampshire residents may have been accessed without authorization as a result of this incident.

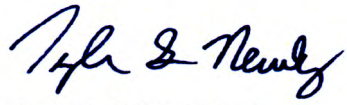
Promptly after discovering the issue on March 20, 2018, Shutterfly conducted an investigation and took steps to secure our employees' personal information. Shutterfly determined that unauthorized parties may have accessed a test employee information database using legitimate log-in credentials obtained by unknown means. The accessed database included the personal information of current and former Shutterfly employees, dependents and beneficiaries, including name, Social Security number, address, date of birth, bank account numbers and salary information. No customer data was impacted by this incident. Shutterfly has notified law enforcement and continue to work closely with them on their investigation.

One of our top priorities is to help ensure the privacy and security of our employees' personal information. Toward that end, Shutterfly is offering identity protection and credit monitoring services to the affected employees free of charge for one year. Attached for your reference is a sample of the notice to the affected individuals, which Shutterfly has sent by email to current employees and by first class mail to others.

If you have any questions, please contact me by email at tnewby@fenwick.com, or by phone at (415) 875-2495.

Sincerely,

FENWICK & WEST LLP



TYLER G. NEWBY

SHUTTERFLY INC

2800 Bridge Parkway
Redwood City, CA 94065

[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

Dear [EMPLOYEE / FORMER EMPLOYEE/ ADULT DEPENDENT OR BENEFICIARY]:

I'm writing today to notify you that we have learned of potential unauthorized access to your confidential, personal data in Workday. Although we do not have evidence that personal data was stolen, as is consistent with our culture of transparency, I wanted you to hear about this directly from me as quickly as possible. While our investigations are ongoing, the purpose of this message is to share what we know at this point and tell you what actions you can take. You can expect to hear from us again if there are further developments to share.

What happened?
On March 20, 2018, we learned that a Shutterfly employee's credentials were used without authorization to access our Workday test environment on January 11, 2018. We do not yet know if unauthorized access occurred at other times. This test environment is used by a limited number of employees to develop, test and preview Workday functionality before it goes live. As soon as we were made aware, our security team promptly implemented additional security measures. We do not believe that the security of the Workday service was compromised.

What information was involved?
Shutterfly has used Workday to house employee records for current and former employees since June 2013. As such, potentially exposed data may have included items such as your name, social security number, date of birth, and work email; any passport number, state ID (including driver's license), bank account and routing numbers, pay stub information, or personal email that was on file in Workday; and the names, dates of birth, and social security numbers of any beneficiaries and/or dependents that were on file in Workday. To be clear, no customer or vendor data was impacted.

Our investigations are continuing, but at this time we have not found evidence of confidential data being stolen. If we learn anything to the contrary, we will let you know.

What is Shutterfly doing?
In addition to our own internal investigations, we are working with an outside forensic investigation firm to assist in our ongoing efforts. We have also notified law enforcement.

We also want to make sure that you have resources to protect your personal data, in case it was stolen. Therefore, Shutterfly has contracted with Experian to provide a free one-year membership in Identity Works Premium, Experian's best identity protection solution. This product helps detect possible misuse of your personal data and provides you with identity protection services focused on immediate identification and resolution of identity theft.

What you can do.
You can sign up with Experian by following the instructions and using the enrollment code provided on the following page of this letter. You will be able to access this offer at no cost by signing up no later than June 30, 2018. We've also provided more information on measures you may want to take to protect your privacy in the included document.

How can I get more information?
We have established a hotline to answer any further questions you may have: 1-855-229-1597 or WDHelp@Shutterfly.com.

On behalf of Shutterfly's Leadership Team, I want to apologize for the inconvenience and the concern this incident may cause. The safety and security of your confidential data is of paramount importance. You have our commitment that we will use the learnings from this incident to take the strongest possible measures to prevent future incidents. As we continue to investigate, you can expect to hear from us again if there are any new developments to share.

Thanks,

[insert signature]

Christopher North
President and Chief Executive Officer
Shutterfly, Inc.

HOW TO ACCESS YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: June 30, 2018 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [URL]
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [customer service number] by **[enrollment end date].** Be prepared to provide engagement number **[engagement #]** as proof of eligibility for the identity restoration services by Experian.

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [customer service number]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions

PROTECTIVE MEASURES YOU CAN TAKE

The following resources are available to help you protect your personal information and monitor your accounts for suspicious activity.

Free Credit Report

You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling 877-322-8228 or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. When you receive your credit report(s), please review them carefully. Look for any accounts you did not open, requests for your credit report from anyone that you did not apply for credit with, or inaccuracies regarding your personal identifying information, such as your home address or social security number. If you see anything you do not understand or that is incorrect, contact the appropriate credit reporting agency using the contact information on the credit report or listed below and ask them to have information relating to fraudulent transactions deleted:

Experian P.O. Box 9554 Allen, TX 75013 www.experian.com 888-397-3742	Equifax P.O. Box 740256 Atlanta, GA 30374 www.equifax.com 800-525-6285	TransUnion P.O. Box 6790 Fullerton, CA 92834 www.transunion.com 800-680-7289

Additionally, you can obtain information from the Federal Trade Commission about taking steps to avoid identity theft at: http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Flagging Your Credit Report

To further protect you from the possibility of identity theft, each of the national credit reporting agencies provides the ability to place a fraud alert or security freeze on your credit files. A fraud alert notifies any creditors that access your credit report that you may be the victim of fraud and encourages them to take additional steps to protect you from fraud. Placing a fraud alert is as simple as calling the numbers above for each or any of the credit reporting agencies and requesting that a fraud alert be placed on your credit file.

Whether or not you find any signs of fraud on your credit reports, we recommend that you closely monitor your banking and credit account statements for suspicious activity on your existing accounts. You should also remain vigilant over the next two years by attentively monitoring your credit reports and account statements for indications of fraud and/or theft, including identity theft.

SHUTTERFLY INC

2800 Bridge Parkway
Redwood City, CA 94065

[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

Dear [PARENT OF MINOR DEPENDENT/BENEFICIARY]:

I'm writing today to notify you that we have learned of potential unauthorized access to confidential, personal data in a system containing employee data. Although we do not have evidence that personal data was stolen, as is consistent with Shutterfly's culture of transparency, I wanted you to hear about this directly from me as quickly as possible. Because your child or children were listed as dependents or beneficiaries of a Shutterfly, Inc. employee between June 2013 and today, it's possible this personal information was exposed. While our investigations are ongoing, the purpose of this message is to share what we know at this point and tell you what actions you can take. You can expect to hear from us again if there are further developments to share.

What happened?
On March 20, 2018, we learned that a Shutterfly employee's credentials were used without authorization to access our Workday test environment on January 11, 2018. We do not yet know if unauthorized access occurred at other times. This test environment is used by a limited number of employees to develop, test and preview Workday functionality before it goes live. As soon as we were made aware, our security team promptly implemented additional security measures. We do not believe that the security of the Workday service was compromised.

What information was involved?
Shutterfly has used Workday to house employee records for current and former employees since June 2013. As such, potentially exposed data may have included the names, dates of birth, and social security numbers of any employee dependents and/or beneficiaries that were on file in Workday. To be clear, no customer or vendor data was impacted.

Our investigations are continuing, but at this time we have not found evidence of confidential data being stolen. If we learn anything to the contrary, we will let you know.

What is Shutterfly doing?
In addition to our own internal investigations, we are working with an outside forensic investigation firm to assist in our ongoing efforts. We have also notified law enforcement.

We also want to make sure that you have resources to protect the personal data of your dependents and beneficiaries, in case it was stolen. Therefore, Shutterfly has contracted with Experian to provide a free one-year membership in Identity Works Premium, Experian's best identity protection solution. This product helps detect possible misuse of personal data and provides you with identity protection services focused on immediate identification and resolution of identity theft.

What you can do.
You can sign your dependents or beneficiaries up with Experian by following the instructions and using the enrollment code provided on the following page of this letter. You will be able to access this offer at no cost by signing up no later than June 30, 2018. We've also provided more information on measures you may want to take to protect your privacy in the included document.

How can I get more information?
We have established a hotline to answer any further questions you may have: 1-855-229-1597 or WDHelp@Shutterfly.com.

On behalf of Shutterfly Inc.'s Leadership Team, I want to apologize for the inconvenience and the concern this incident may cause. The safety and security of your confidential data is of paramount importance. You have our commitment that we will use the learnings from this incident to take the strongest possible measures to prevent future incidents. As we continue to investigate, you can expect to hear from us again if there are any new developments to share.

Thanks,

[insert signature]

Christopher North
President and Chief Executive Officer
Shutterfly, Inc.

HOW TO ACCESS YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: June 30, 2018 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [URL]
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [customer service number] by **[enrollment end date].** Be prepared to provide engagement number **[engagement #]** as proof of eligibility for the identity restoration services by Experian.

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [customer service number]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions

PROTECTIVE MEASURES YOU CAN TAKE

The following resources are available to help you protect your personal information and monitor your accounts for suspicious activity.

Free Credit Report

You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling 877-322-8228 or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. When you receive your credit report(s), please review them carefully. Look for any accounts you did not open, requests for your credit report from anyone that you did not apply for credit with, or inaccuracies regarding your personal identifying information, such as your home address or social security number. If you see anything you do not understand or that is incorrect, contact the appropriate credit reporting agency using the contact information on the credit report or listed below and ask them to have information relating to fraudulent transactions deleted:

Experian P.O. Box 9554 Allen, TX 75013 www.experian.com 888-397-3742	Equifax P.O. Box 740256 Atlanta, GA 30374 www.equifax.com 800-525-6285	TransUnion P.O. Box 6790 Fullerton, CA 92834 www.transunion.com 800-680-7289

Additionally, you can obtain information from the Federal Trade Commission about taking steps to avoid identity theft at: http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Flagging Your Credit Report

To further protect you from the possibility of identity theft, each of the national credit reporting agencies provides the ability to place a fraud alert or security freeze on your credit files. A fraud alert notifies any creditors that access your credit report that you may be the victim of fraud and encourages them to take additional steps to protect you from fraud. Placing a fraud alert is as simple as calling the numbers above for each or any of the credit reporting agencies and requesting that a fraud alert be placed on your credit file.

Whether or not you find any signs of fraud on your credit reports, we recommend that you closely monitor your banking and credit account statements for suspicious activity on your existing accounts. You should also remain vigilant over the next two years by attentively monitoring your credit reports and account statements for indications of fraud and/or theft, including identity theft.