



DLA Piper LLP (US)
701 Fifth Avenue Suite 6900
Seattle, Washington 98104-7029
www.dlapiper.com

Kate Lucente
kate.lucente@us.dlapiper.com
T 206 839 4854
F 206 494 1809

May 18, 2023

Via EMAIL: IDTHEFT@OAG.STATE.MD.US

The Honorable Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Security Incident Notification

Dear Attorney General Frosh:

We are providing notice on behalf of Levi Strauss & Co. ("LS&Co.") pursuant to Md. Code Ann., Com. Law § 14-3504, about an incident involving 15 Maryland residents.

LS&Co. detected a number of unusual log in attempts for accounts at Levi.com between April 24th and April 27th. Upon discovering this incident, LS&Co. immediately de-activated account credentials for any user accounts that were accessed during this period. LS&Co. also began an investigation into the suspicious activity.

LS&Co.'s investigation determined that an unauthorized person gained access to certain accounts between April 24th and April 27th. The investigation further revealed the unauthorized person likely arrived at Levi.com with account log in credentials already in hand. The unauthorized person likely obtained compromised account credentials from another source, likely a third-party data breach or through malware present on a device that was used by the account owner to log in to Levi.com. The unauthorized person used these credentials in their possession to access some LS&Co. customer accounts.

This unauthorized person could have viewed all information contained in the account profile information, including order history, name, email, user ID, stored addresses, and partial information for any saved payment methods, such as last 4 digits of card number, card type and expiration. It does not appear that any fraudulent purchases were initiated using the information, and LS&Co.'s systems do not allow saved payment methods to be used for purchases without a secondary means of authentication.

Please know that protecting personal information is something that LS&Co. takes very seriously. LS&Co.'s security detection tools functioned properly in this instance, and LS&Co. was able to promptly identify and block the suspicious activity. LS&Co. conducted a diligent investigation to confirm the nature and scope of the incident. LS&Co. also took steps in partnership with its monitoring provider to prevent similar attacks in the future, and LS&Co. continually makes improvements that strengthen its cybersecurity protections.

On or around May 22, 2023, LS&Co. will notify affected Maryland residents, A sample notification letter is enclosed.

Should you have any questions regarding this matter or if we can be of any further assistance to the Maryland residents affected by this incident, please contact me at (206) 839- 4854 or Kate.Lucente@us.dlapiper.com.

Respectfully submitted,

DLA Piper LLP (US)

Kate Lucente

Counsel for Levi Strauss & Co.

Enclosure

[LS&Co. Logo]

Levi Strauss and Co.
1155 Battery St.
San Francisco, CA 94111

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Security Incident

Dear <<Name 1>>:

We are writing to inform you of some suspicious login activity detected for your account at Levi Strauss & Co. ("LS&Co."). Out of an abundance of caution, we are providing you with this notice so that you are aware of the activity, know what we are doing and can take steps to protect your information should you feel it is appropriate to do so. LS&Co. takes risks to our consumers' information very seriously and we sincerely regret any inconvenience or concern this communication may cause.

What Happened?

Our defense monitoring tools detected a number of unusual log in attempts for accounts between April 24th and April 27th. Our immediate response was to de-activate account credentials for any user accounts that were accessed during this period and we began an investigation into the suspicious activity. If you logged into your Levi.com account during this period, your legitimate access may have still triggered a password reset, and we apologize for any inconvenience having to re-set your password may cause. If you did not attempt to access your Levi.com account during this period, your account may have been accessed by an unauthorized person. This unauthorized person could have viewed all information contained in your account profile information, including your order history, as well as your name, email, user ID, stored addresses, and partial information for any saved payment methods (last 4 digits of card number, card type and expiration).

It does not appear that any fraudulent purchases were initiated using your information and our systems do not allow saved payment methods to be used for purchases without a secondary means of authentication.

If you have not already verified your account and reset your account credentials, you will need to do so, in order to access your LS&Co. account. Upon accessing your account, we recommend that you verify any saved payment information and delete any information that you do not recognize.

How did this Happen?

Because the bad actor(s) behavior indicates that they arrived at Levi.com with account log in credentials in hand, it appears that they obtained compromised account credentials from another source, likely a third-party data breach or through malware present on a device that was used by the account owner to log in to Levi.com. They used these credentials in their possession to access some LS&Co. customer accounts, including yours. This form of cyber attack is known as “credential stuffing.” Since individuals often use the same account credentials (email and password combinations) for multiple online accounts, an unauthorized person may be able to obtain stolen login credentials from one website and use those same stolen credentials to gain unauthorized access to online accounts on other websites. Please review below for more information about steps you can take to protect yourself and your accounts.

What We Are Doing.

Please know that protecting your personal information is something that LS&Co. takes very seriously. Our security detection tools functioned properly in this instance, and we were able to promptly identify and block the suspicious activity. We conducted a diligent investigation to confirm the nature and scope of the incident. We also took steps in partnership with our monitoring provider to prevent similar attacks in the future, and we continually make improvements that strengthen our cybersecurity protections.

What Steps Should I Take?

If you have not already done so, please follow the steps to verify your account and reset your password. You may contact LS&Co. Customer Support as set forth below for help and additional instructions on completing these steps.

We also suggest that you change the passwords for your other online accounts. **You should use a strong password that is unique to each of your online accounts.** This is the best defense you can take for credential stuffing threats. For more information about password security, you can consult the Federal Trade Commission’s guidance on secure password practices for consumers, available at <https://consumer.ftc.gov/articles/password-checklist>. We also encourage you to install and maintain malware and virus protection software on your devices that is designed to identify and remove harmful content, including key stroke logging malware.

For More Information

We have included some additional information below regarding other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report.

If you have any further questions regarding this incident, please contact us at [ENTER CONTACT INFORMATION]

We sincerely regret any concern this incident may cause.

Sincerely,

[Signature]

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

	Experian	Equifax	TransUnion
Phone	1-888-397-3742.	1-800-525-6285 or 1-888-766-0008	1-800-680-7289
Address	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	Equifax Consumer Fraud Division PO Box 740256 Atlanta, GA 30374	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Credit Report Fraud Alert Form	https://www.experian.com/fraud/center.html	https://www.equifax.com/personal/credit-report-services/	https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift or remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

	Experian	Equifax	TransUnion
Address	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	https://www.experian.com/freeze/center.html	https://www.equifax.com/personal/credit-report-services	https://www.transunion.com/credit-freeze

To request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail.:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of Birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, your state Attorney General, or the Federal Trade Commission. This notice has not been delayed by law enforcement.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above.

District of Columbia Residents: You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
441 4th Street NW
Suite 1100 South
Washington, D.C. 20001
(202) 727-3400
<https://oag.dc.gov/>

Maryland Residents: You may obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
Telephone: 1-888-743-0023.
www.oag.state.md.us/Consumer

New York Residents: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General
Consumer Frauds & Protection
Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, NY 12231
(800) 697-1220
www.dos.ny.gov

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: 1-919-716-6400
www.ncdoj.gov

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.