From: [Levi Customer Support]

Notice of Security Incident

Dear [Name]

We are contacting you about some recent actions that may affect you.

- We recently issued a forced password reset after detecting suspicious activity on our website.
- Bad actors have attempted to log into some accounts using email and password combinations obtained elsewhere. If you re-use your passwords across websites, it is possible they were able to log into your account.
- You should reset your password on Levi.com and any other websites for which you share common passwords. Use only unique, complex passwords to keep your information safe.
- We continue to invest in our website cybersecurity to combat these, and other similar, kinds of attacks.

Read on for important information about this incident.

Levi Strauss & Co. ("LS&Co" or "we") recently detected suspicious activity that we may have impacted your account. After an investigation, we determined that unknown parties launched an automated cyberattack to attempt to access accounts.

To protect your account, we are issuing a forced password reset that will require you to create a new password to access your account (click here to get started).

What Happened?

On June 13th we identified an unusual spike in activity on our website. Our investigation showed characteristics associated with a "credential stuffing" attack where bad actor(s) who have obtained compromised account credentials from another source (such as a third-party data breach) then use a bot attack to test these credentials against another website – in this case www.levis.com. LS&Co was not the source of the compromised login credentials.

Users often assign the same email and password combination across multiple online accounts allowing an unauthorized person to gain access more easily using stolen login credentials from another source.

In an abundance of caution, we responded to the attack by promptly de-activating account credentials for all user accounts that were accessed during the relevant time period. If you logged into your Levi.com account during this time, your legitimate access may have triggered a password reset.

What Information Was Involved?

Anyone that accessed your account would be able to view information contained there such as your order history, name, email, stored addresses, and, *if you have saved a payment method*, partial information that includes the last 4 digits of card number, card type and expiration date.

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

What We Are Doing

Protecting your personal information is something we take seriously. Our security detection tools functioned properly in this instance, and we were able to promptly identify and block the attack. We conducted a diligent investigation to confirm the nature and scope of the incident. We continually evaluate and identify improvements to strengthen our website cybersecurity.

What You Can Do

If you have not already done so, please reset your password. Upon accessing your account, verify the accuracy of your personal information. If you detect anything unusual, please contact LS&Co. Customer Support for help and additional instructions. We suggest that you change the passwords – using a strong and unique password - for your other online accounts. This is an important defense against 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 regarding other 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, 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.