

RECEIVED
NOV 06 2018
CONSUMER PROTECTION

TEL 212 • 309 • 1000
FAX 212 • 309 • 1100

LISA J. SOTTO
DIRECT DIAL: 212 • 309 • 1223
EMAIL: lsotto@HuntonAK.com

FILE NO: 039322.61

November 5, 2018

Via Overnight Delivery

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

To Whom It May Concern:

In accordance with N.H. Rev. Stat. Ann. § 359-C:20, I am writing on behalf of Nordstrom, Inc. (“Nordstrom”) to notify you about a recent data security issue that affected certain Nordstrom employees’ information. The incident did not impact Nordstrom customer information, Nordstrom systems or physical Nordstrom stores.

On October 9, 2018, Nordstrom learned that a contract worker improperly handled certain Nordstrom employee data that day. Employee information that was affected could include names, social security numbers, pay card numbers (for employees who have them), checking account and routing numbers (which appear on the face of checks), insurance provider information, salary information, dates of birth, addresses, and phone numbers. As indicated above, there is no indication that Nordstrom customer data was affected by this issue.

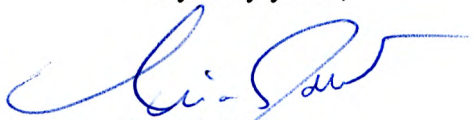
Promptly after learning of the issue, Nordstrom quickly began to investigate the nature and scope of the incident and identify the Nordstrom employees and former employees whose information may have been affected. Nordstrom also notified law enforcement of the issue. Based on the investigation to date, there is no indication that the relevant information has been misused, and the contract worker stated they did not share, misuse or disclose the relevant personal information. Nevertheless, Nordstrom will be providing affected individuals with 24 months of identity protection and credit monitoring services at no cost to them.

There are approximately 43 New Hampshire residents affected by this issue. Enclosed for your reference is a copy of the notification being sent to affected individuals on November 5, 2018.

Office of the New Hampshire Attorney General
November 5, 2018
Page 2

Please do not hesitate to contact me if you have any questions.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Lisa J. Sotto", with a long horizontal flourish extending to the right.

Lisa J. Sotto

Enclosure

NORDSTROM

Processing Center • P.O. BOX 141578 • Austin, TX 78714



JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

November 5, 2018

NOTICE OF DATA BREACH

Dear John Sample:

One of the responsibilities we have as a company is to uphold the privacy of current and former employees' personal information. We are investigating an incident where a contract worker improperly handled some Nordstrom employee data. We want to update you on what happened and what action we're taking to help protect your personal data. We take this situation seriously and on behalf of the Executive Team, we sincerely apologize.

What Happened?

We are investigating an incident where a contract worker improperly handled some Nordstrom employee data. This happened on October 9, 2018. Our Information Security team promptly discovered the incident that day, notified law enforcement and began a comprehensive investigation.

What Information Was Involved?

No customer data was impacted. Employee information that was affected could include name, social security number, pay card number, checking account and routing number, insurance provider information, salary information, date of birth, address and phone number.

What We Are Doing

The contract worker who improperly handled this information no longer has any access to our systems, and we're putting additional measures in place to help prevent this from happening again. We have no evidence data was shared or used inappropriately.

What You Can Do

Out of an abundance of caution, we want to provide you with information and resources to help protect and monitor your information for any potential unauthorized activity.

To provide an added level of assurance and protection, we're offering you free Identity Repair and Fraud Alerts with Credit Monitoring services for 24 months. The Identity Repair services start today. These services are delivered through a company we've selected and worked with called AllClear ID. The attached Reference Guide provides information on these services and registering for AllClear ID's Fraud Alerts with Credit Monitoring services.

Although we have no indication your data was misused, we encourage you to remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your free credit reports. You also are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. The attached Reference Guide includes information about ordering your free credit report and recommendations by the U.S. Federal Trade Commission on the protection of personal information.



01-02-1

For More Information

For questions about this incident and the free Identity Repair and Fraud Alerts with Credit Monitoring Services, please contact AllClear ID. You can reach AllClear ID representatives Monday-Saturday from 6:00 a.m. – 6:00 p.m. Pacific Time at 855-309-1722.

Again, we hope you'll accept our sincere apologies for the concern or difficulty this situation may cause.

Sincerely,

A handwritten signature in black ink, appearing to read "Blake W. Nordstrom". The signature is fluid and cursive, with the first name being the most prominent.

Blake Nordstrom
Co-President, Nordstrom Inc.

Reference Guide

We encourage you to take the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form. Review your credit report carefully, and notify the consumer reporting agencies of any inaccuracies in your information, and of contents you do not understand.

Register for AllClear Identity Repair & Fraud Alerts with Credit Monitoring. We have arranged with AllClear ID to help you protect your identity and your credit information for twenty-four months at no cost to you.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 855-309-1722 and a dedicated investigator will help recover financial losses, and help restore your credit and identity.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. To enroll in the fraud alerts with credit monitoring service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 855-309-1722 and using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's Identity Theft Report (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

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

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-525-6285, www.equifax.com

Experian: P.O. Box 9554, Allen, TX 75013, 1-888-397-3742, www.experian.com

TransUnion: P.O. Box 2000, Chester, PA 19022, 1-800-680-7289, www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.



The consumer reporting agencies may require identification information such as your full name, Social Security number, date of birth, current and prior addresses, government identification card, and proof of your current address, to honor your request.

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street Des Moines, IA 50319, (515) 281-5164 www.iowaattorneygeneral.gov.

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023 (toll-free in Maryland), (410) 576-6300, www.oag.state.md.us.

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina) (919) 716-6400, www.ncdoj.gov.

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392 (toll-free in Oregon), (503) 378-4400, <http://www.doj.state.or.us>.

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, (401)-274-4400, <http://www.riag.ri.gov>.

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze.