NORDSTROM

September 01, 2011

NH Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Delaney:

We are writing to alert your office to information that we have learned about threats from outside of the Nordstrom network to Nordstrom.com customers.

We take very seriously our obligation to safeguard the private information of our customers and know that they place great trust in us. As such, we are writing to every State Attorney General, though this goes beyond what is required legally in some states, to ensure you have full information about this issue. Though we have no evidence of a breach of Nordstrom systems or password files, we wanted to share with you what we've come to learn has happened, actions we've taken to respond and how we've notified the 74 customers in New Hampshire who may have potentially been impacted.

Background on Nordstrom.com

Nordstrom, Inc. is one of the nation's leading fashion specialty retailers, with 213 stores located in 29 states. Nordstrom also serves customers through our online retail presence at Nordstrom.com. We have approximately 9 million customers who have registered with Nordstrom.com. We receive approximately 250,000 calls to our customer call center each month. Our Privacy department receives a notification of every customer call, email or letter to our call center that mentions any type of privacy or security concern. Though we have learned that in most cases, the concern is unrelated to information privacy or security, we have a process to review each matter.

Summary of the Incident

This June, we identified three customers who had experienced unexpected activity in their online accounts, which was later confirmed as fraud. All three customers reported that they found unfamiliar information in their online accounts and two of the three customers reported that orders had been placed using their online accounts without their knowledge. Because of the similarities in these reports, we searched our call records and identified a small number of other accounts with similar patterns. Subsequently, in June and July, we received an additional 13 calls and received one last call in August. Today we have a total of 17 customer accounts that we know have been accessed inappropriately and used for fraud. We don't have any evidence that Nordstrom's networks and systems were breached or that our password files were compromised. We are working closely with each of these customers to understand and resolve their issues.

With regard to the fraud, in 14 cases, the fraudsters added a stolen credit card number to the account, along with new shipping information. In two cases, the fraudsters used the payment card on file to make a purchase (though they could not view the full credit/retail/debit card information associated with the file). In one case, no purchases were made, although the consumer noticed that unfamiliar shipping addresses had been added to the account.

Our Investigation

We conducted a thorough investigation into these incidents and found no evidence that any Nordstrom system was compromised. We did detect certain fraud patterns. For example, we saw that some of the accounts have been accessed from the same Internet Protocol [IP] addresses. Our conversations with the customers also revealed commonalities. For example, our customers told us that they had been using weak passwords and that they used the same passwords on multiple sites. Some customers reported that they had experienced recent account takeover issues with other retailers. The customers also reported receiving prior notifications of breaches of their personal information from other entities, including their email addresses.

We concluded that the customer accounts were compromised independent of Nordstrom. The fraudsters came to Nordstrom.com already knowing the customers' email addresses and passwords. Although we do not know how the passwords were compromised, we understand that there are several possibilities. The passwords could have been exposed in another corporate breach. We know there have been several high profile instances where companies' account databases were breached exposing login credentials and putting individuals who use the same passwords on multiple sites at risk. Alternatively, the customers may have malware on their computers that captured their personal information.

We also engaged Stroz Friedberg (http://www.strozfriedberg.com/), a global digital risk management and investigations firm, to help us conduct more in-depth analyses. We asked Stroz to examine pertinent Nordstrom web activity data as far back as 2004 so that we could understand and identify other accounts that may have been accessed inappropriately. We first identified all customer accounts that had been accessed from the IP addresses associated with the known fraud. While we do not have evidence that these accounts have been misused, we do believe that they may have been accessed without authorization.

Using statistical analysis, we identified other IP addresses that were used to access multiple accounts. In many cases, we believe the access was appropriate, as the IP addresses belong to large companies whose employees are shopping at Nordstrom.com from the corporate network. In other cases, we were not able to determine why the IP address would be used to access multiple accounts. Some of these addresses are associated with US-based Internet Service Providers. Other IP addresses are associated with foreign ISPs. We have flagged accounts accessed from these unknown US and foreign ISPs as suspect. Although we have no information that these accounts were misused, we are treating them all as suspect out of an abundance of caution.

Please note that access to the Nordstrom.com account only exposes limited personal information about the account owner. Although Nordstrom stores customer payment card information, this information is encrypted, and only the last four digits of the card are visible. If an account is accessed inappropriately, the stored number can be used to make purchases, but it cannot be acquired by the fraudster. We have not seen additional complaints about inappropriate charges, and we do not believe that stored account numbers are generally being misused.

Someone accessing an account inappropriately would be able to see the customer's name, addresses on file, email address, telephone number, order history, day and month of birth, and Wishlist (favorite items) information. In each case, customers chose what information to store in their accounts, so not all accounts have all of these fields populated. Because we do not track when customers make changes to their accounts, we do not know what information might have been present in their online account when it was accessed.

Although we cannot be certain, we believe that the online accounts have been accessed to validate that the customer has a Nordstrom.com account. It is possible that this knowledge is being used to perpetrate other consumer fraud, such as phishing. However, we are not aware of any targeted phishing attacks directed at Nordstrom customers.

We have shared our investigation details with law enforcement agencies. We will work with law enforcement as needed to support their efforts to address these and related cybercrimes.

What We Are Doing

Though we don't have any evidence that Nordstrom's networks and systems were breached or that our password files were compromised, we have taken the following actions to ensure that our customers are aware of this issue and taking actions to protect their personal information:

- We have posted a fraud alert so that all Nordstrom.com visitors see information on computer security.
- We are sending a notification letter to the mailing address we have on file for every customer whose account may have been accessed by a computer associated with a suspicious IP address. A copy of our customer letter is attached for reference.
- We are also requiring each of the potentially impacted customers to change their passwords and requiring them to use stronger passwords. Because we know that customer email addresses have been compromised in other breaches, we have reprogrammed our systems so that they will not generate an email notification to reset the account passwords. Customers will be instructed to change their passwords in the notification letter and given guidance on password and online security.
- We are also providing customers with a year of complimentary credit monitoring. Although we have *not* exposed any sensitive consumer information, we want our customers to have access to the fraud resolution

services that the credit monitoring product offers. Providing this service to our customers without charge is consistent with our Nordstrom values.

- To be able to respond to any specific customer questions related to this issue, we have a dedicated toll free number with a dedicated team of employees available at Nordstrom.com. The number is 1-800-285-5800.
- We are working with Stroz Friedberg to determine additional controls that we may be able to implement to detect unauthorized account access. We have already blocked certain foreign IP addresses entirely. We are working to determine additional ways to evaluate access attempts and to authenticate shoppers.

We very much want to help protect our customers and to preserve their confidence in online shopping and would welcome additional conversations with you and your team about how to take future action in this regard.

We are happy to answer any other questions that you may have about this matter. We've provided three individuals here for you to contact. (Blake wants to ensure it's easy to get a hold of someone at Nordstrom so he suggests Kim plus two other well-versed individuals names/contact info gets inserted)

Sincerely,

Kim Dawson

Kim Dawson
Privacy Director

Susan Hastings
Privacy Manager

Julie Blume
Senior Privacy Compliance Specialist

September 3, 2011

Dear J

We value the trust you as our customer put in Nordstrom and appreciate the goodwill you extend to us when you choose to shop with us. We work hard every day to continue to earn your trust and your business. We realize you hold Nordstrom to a high standard and you expect that we will provide you with a great online shopping experience. We also know that you expect your personal information at Nordstrom.com is secure and protected and we take our responsibility in this regard very seriously. That is why we are writing to you. We want to let you know about an important issue that impacted a small number of Nordstrom.com online accounts, including potentially yours.

We have learned that your login information (email and password) may be known to people who attempted to use it to access your online account without your authorization. While we do not have evidence of a breach of Nordstrom systems or password files, we wanted to let you know what we've learned so you can take appropriate actions to protect your online accounts at Nordstrom.com and other websites.

Recently we confirmed that 17 customers had their Nordstrom.com online accounts accessed from outside the Nordstrom network by unauthorized individuals and in some cases their accounts were used to make fraudulent transactions. When we learned about these cases and realized there were similarities between them, we quickly pulled together our internal team and added the capabilities of outside expert investigators to launch a full investigation of this issue to understand its full potential impact to our online customers.

In reviewing the 17 reported cases, we believe those customers' email addresses and passwords were used by unauthorized individuals to log in to their Nordstrom.com accounts, but we do not know how the email addresses and passwords were obtained. We don't have any evidence that Nordstrom networks and systems were breached or that our password files were compromised. The common practice many people have of using the same email address and password across multiple websites may have made our customers' online accounts vulnerable. Through our analysis, we also detected certain fraud patterns that suggested potential unauthorized access of other Nordstrom.com online accounts as well. While we do not have information that your Nordstrom.com account was used for fraudulent transactions we wanted to let you know about this issue so you can take precautions to ensure that your personal information is secure.

Because we realize you may have many questions about this situation, we've provided additional information on the following pages. We have also pulled together a team of some of our best Nordstrom employees who are well-versed in this matter and can help answer your individual questions through a dedicated toll-free number at Nordstrom.com. Please contact us at 1-800-285-5800 with questions you may have.

Nordstrom takes these issues very seriously and we are continuing to take steps where we can to prevent these types of incidents from happening. Again, please do not hesitate to contact our dedicated team who can handle any specific questions or concerns related to this letter. We sincerely apologize for any inconvenience this situation may have caused you.

Sincerely,

Kim Dawson
Privacy Director, Nordstrom, Inc.

Blake Nordstrom
President, Nordstrom, Inc.

NORDSTROM

PO Box 21986 Seattle, WA 98111-3986 206-303-2340

What happened?

We recently confirmed that 17 of our customers had their Nordstrom.com online accounts accessed from outside the Nordstrom network by unauthorized individuals using the customers' email addresses and passwords. While we do not know exactly how the customer email addresses and passwords were obtained, we have no evidence that Nordstrom's networks and systems were breached or that our password files were compromised. Customers became aware of this issue by finding orders placed through their online account that they did not make or unfamiliar information in their online accounts such as a billing or shipping address that wasn't theirs. The fraudulent transactions were often attempted using other peoples' stolen credit cards or, on a few occasions, the card that was on file in the customer's online account was used. **The unauthorized individuals were not able to view or obtain the full credit, debit or retail card number on file in the online account.**

Why did you receive this letter?

As part of our investigation into the 17 customer reports, we reviewed our web history information. Like all websites, we record the Internet Protocol (IP) address of every computer that accesses our site and during our reviews we found that certain IP addresses tried to access a number of accounts. We flagged those IP addresses as suspicious and then identified any customer accounts that those IP addresses may have attempted to access. Your account is one of a small number of our nearly 9 million online accounts that we've identified. We do not have evidence that your account was fraudulently used but wanted you to be aware of this issue so you can ensure that your personal information is secure.

How did this happen?

We believe that in the 17 cases, our customers' email address and passwords were used to log in to their online accounts. While we do not know exactly how the customer email addresses and passwords were obtained, we have no evidence that Nordstrom's networks and systems were breached or that our password files were compromised. As we mentioned above, while discussing this issue with customers who reported the 17 cases, we found that most had used common emails and passwords across many websites, which may have made their online accounts vulnerable. We also found other similarities – in some of the cases our customers' online account passwords were not complex and were easy to guess; in other cases our customers may have had malware on their personal computers, which could enable unauthorized access.

Once they were accessed, in some cases the unauthorized individuals attempted to make a fraudulent transaction. Of the customers we have spoken with, some found orders placed that they did not make while others had unfamiliar information such as a billing or shipping address that wasn't theirs.

What information could they see?

Your email address and password may have been used to access your online account. The unauthorized individuals may have also been able to see your name, billing and shipping addresses, phone number, month and day of birth (not the year), online order history, Wishlist information, and the last four digits of the credit card on file in the online account. The fraudulent transactions were often completed using someone else's stolen credit cards or, on a few occasions, the card that was on file in the customer's online account was used. **Your full credit, debit or retail card information could not be viewed.**

What should you do?

1. Please review your account statements carefully and report any unexpected activity to us and your credit card company immediately. Call our team dedicated to you and this issue at 1-800-285-5800 if you find any suspicious activity or unfamiliar information associated with your online account, as we are continuing to investigate this matter.
2. You may have already noticed that we implemented a mandatory password reset. This reset also removed any encrypted account number you may have had on file until you re-enter it. Please take a moment to reset your password and review the accuracy of the information associated with your online account (addresses, etc.).
3. We also encourage you to review your account statements from other online companies. We've found in some cases, the customers who have been impacted also reported experiencing compromises of their online accounts at other websites. We strongly recommend that you also use different passwords for each website you visit and on any email accounts you use. We've also provided a list of resources below.

What should you do? (continued)

4. To help you further protect personal information, we are also offering a complimentary one-year membership to Experian's ProtectMyID product. Once your ProtectMyID membership is activated, your credit report will be monitored daily for indicators of identity theft. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. For more information about this product, including enrollment instructions, please see the attached page.

What is Nordstrom doing to protect you?

Since learning about this issue, we are working with a security firm and other experts to assist us with our investigation. We have implemented additional precautionary security measures. We have also notified law enforcement and every state Attorney General about this issue. We hope our investigation can help law enforcement identify and prosecute individuals engaged in online account fraud.

What should you do in the future to protect yourself?

We encourage you to immediately take measures to protect personal information in your online accounts, including the following steps:

- Install the latest security updates and anti-virus software on your computer's operating system to help prevent malware and viruses
- Reset your email account password
- Use complex passwords (a minimum of 7 alpha/numeric cAsE sEnsitive characters)
- Do not use the same password on more than one website
- Do not share your password with others
- Sign out/log off website sessions so that your session is closed and cannot be accessed by another user on the same computer, especially when using a public computer or terminal
- Visit these additional resources:
    - http://www.us-cert.gov/cas/tips/
    - http://www.microsoft.com/security/pc-security/protect-pc.aspx
    - http://www.clarkhoward.com/news/clark-howard/technology/clark-howards-virus-spyware-and-malware-protection/nFZJ/

How will you know in the future if the emails or requests you get from Nordstrom are safe?

Please know that Nordstrom will never send you a message requesting your passwords or other sensitive information such as your account number or Social Security number. You will never receive a link requesting a password reset from Nordstrom that you did not request.

As always, we encourage you to carefully review your account when placing an order and report anything unexpected or out of the ordinary.

What can you do if you have more questions?

We have a team of Nordstrom employees who can help answer your individual questions through a dedicated toll-free number at Nordstrom.com. Please contact us at 1-800-285-5800 with any questions you may have.

NORDSTROM

Additional Information for Our Customers

You will have access to your Experian credit report as part of the credit monitoring product. We recommend that you check your other consumer reports annually. You may obtain a free copy of your credit report once every 12 months from each of the nationwide consumer reporting agencies by visiting http://www.annualcreditreport.com or by contacting the consumer reporting agencies at:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790
www.equifax.com	www.experian.com	www.transunion.com

You may wish to place a fraud alert on your credit report. The fraud alert is a consumer statement that alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a 90 day fraud alert on your Experian credit file, visit https://www.experian.com/fraud/center.html or call 1-888-EXPERIAN (1-888-397-3742) and follow the simple prompts. Once the fraud alert has been placed with Experian, a notification will be sent to the other two credit reporting agencies, Exquifax and Trans Union, on your behalf.

We also recommend that you carefully review all your account statements during the next 24 months to make certain there have been no unauthorized transactions made or new accounts opened in your name. Contact your financial institutions immediately if there is unauthorized activity or if an unauthorized account has been opened in your name.

To learn more about identity theft, visit the Federal Trade Commission's website at www.ftc.gov/bcp/edu/microsites/idtheft/. You can call the Commission at 1-877-ID-THEFT (877-438-4338) or send mail to the Federal Trade Commission - Consumer Response Center at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Maryland residents may contact the state Attorney General's Office for more information about identity theft:

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

North Carolina residents may contact the state Attorney General's Office for more information about identity theft:

North Carolina Office of the Attorney General - Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001
1-877-566-7226 - www.ncdoj.com

Residents of West Virginia and Massachusetts have the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a security freeze may delay your ability to obtain credit. You may request that a freeze be placed on your consumer report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below.

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834-6790

The following information should be included when requesting a security freeze: full name, with middle initial and any suffixes; Social Security number; full date of birth, current address and previous addresses for the past two years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request also should include a copy of a government issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

The consumer reporting agency may charge a reasonable fee of up to $5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the consumer reporting company.

Experian ProtectMyID™ Credit Monitoring Product

To help you protect your identity, Nordstrom is offering you a free one-year membership in Experian's ProtectMyID™ Alert product. Enrollment in ProtectMyID may help detect possible misuse of your personal information and provides you with superior identity theft prevention services focused on immediate identification and resolution of identity theft.

Free ProtectMyID Membership Enrollment Instructions

Visit: protectmyid.com/redeem or call 877-371-7902

Provide the following Activation Code: <xxxxxxxxx>

Please note that to receive the free credit monitoring protection service, you must enroll before December 31, 2011.

ProtectMyID provides you with powerful identity protection that will help detect, protect and resolve potential identity theft. In the case that identity theft is detected, ProtectMyID will assign a dedicated U.S.-based Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish for seamless service.

Your complimentary 12-month ProtectMyID membership includes:

- **Credit Report:** A free copy of your Experian credit report.
- **Daily Credit Monitoring:** Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections.
- **Identity Theft Resolution:** If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.
- **$1 Million Identity Theft Insurance*:** As a ProtectMyID member, you are immediately covered by a $1 Million insurance policy that can help you cover certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-371-7902.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis, Inc. 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.

NORDSTROM