Neiman Marcus | Group

Tracy M. Preston
Senior Vice President
General Counsel



April 14, 2107

The Honorable Joseph Foster
Attorney General of New Hampshire
New Hampshire Department of Justice
33 Capitol St.
Concord, NH 03301

Dear Attorney General Foster:

On behalf of the Neiman Marcus Group ("NMG"), I wish to provide notice to your office under New Hampshire's data breach law. The security incidents may have affected the usernames and passwords of New Hampshire residents.

Unauthorized individuals began attempting to access NMG customers' online accounts on or about December 26, 2015 with respect to Neiman Marcus, Bergdorf Goodman, Last Call, CUSP, and Horchow websites (collectively the "NMG websites") by trying various login and password combinations using automated attacks. At the time, the outside forensic experts NMG engaged to investigate this matter determined that the online intruders were able to view customers' names, basic contact information, email addresses, purchase history, and only the last four digits of the payment cards associated with the online account. Unfortunately, it has become clear that the intruders also had access to full payment card numbers and card expiration dates.

As with any suspected fraud purchase, no NMG customer will be required to pay for any unauthorized purchase as a result of this incident. Customers have been directed to contact NMG if they believe they have been subjected to any fraudulent purchases as a result of this attack or otherwise.

NMG estimates that approximately 17 New Hampshire residents were affected by this incident and that approximately 6,494 customers in total were affected by this incident. On April 14, 2017, NMG began notifying the New Hampshire residents by mail. As a precautionary measure, NMG also is providing one year of free credit monitoring and identity theft protection services to potentially affected individuals, as described in the attached sample notice letter sent to potentially affected residents and enclosed with this letter. Please note that there may be some variation among the type of letters provided to consumers. NMG also has notified its payment processor to ensure that it addresses issues related to potentially compromised cards.

NMG has required all known affected customers to change their password. NMG also has encouraged its customers to change their user name and password on all NMG websites, and every other site where the customer has used the same user name and password combination.

NMG takes this incident very seriously and has notified federal law enforcement. If you have any questions or need further information regarding this incident, please do not hesitate to contact me.

Respectfully submitted,

Tracy M. Preston
SVP and General Counsel
The Neiman Marcus Group

Neiman Marcus Group
C/O ID Experts
PO Box 6336
Portland, OR 97228-6336



<<Mail ID>>
<<Name>>
<<Address1>>
<<Address2>>
<<City>>, <<ST>> <<ZIP>>

<<Date>>

**Notice of Data Breach**

Dear Loyal Customer:

We are writing to share important information with you about a security incident regarding your Neiman Marcus online account username and password, as well as steps we have taken in response to the incident and recommended actions you may wish to take.

**What Happened?**

Unauthorized individuals began attempting to access Neiman Marcus Group customers' online accounts on or about December 26, 2015 with respect to our Neiman Marcus, Bergdorf Goodman, Last Call, CUSP, and Horchow websites (collectively the "NMG websites") by trying various login and password combinations using automated attacks. At the time, the outside forensic experts we engaged to investigate this matter determined that the online intruders were able to view customers' names, basic contact information, email addresses, purchase history, and only the last four digits of the payment cards associated with the online account. Unfortunately, it has become clear that the intruders also had access to full payment card numbers and card expiration dates.

**What Information Was Involved?**

We are notifying you that online intruders may have accessed your name, basic contact information, email address, purchase history, and full payment card number and expiration date.

**What We Are Doing.**

We have notified the companies that process payment cards for the Neiman Marcus Group to ensure that any issues related to potentially compromised cards can be addressed. In 2016, we required all known affected customers to change their password.

As with any suspected fraud purchase, no Neiman Marcus Group customer will be required to pay for any unauthorized purchase as a result of this incident. If you believe that you have been subjected to any fraudulent purchases as a result of this attack or otherwise, please contact us at 1-800-711-7289.

We do not believe that exposure of your payment card number could result in identity theft. Nevertheless, as a precaution, we are providing you with one year of MyIDCare™ through ID Experts. MyIDCare services include: Credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, exclusive educational materials and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. You can sign up for these services by visiting www.myidcare.com/enrollneiman, and following the online instructions to activate your MyIDCare package. Also, you will need to reference the following enrollment code below when calling or enrolling on the website, so please do not discard this letter. Please note the deadline to enroll is July 12, 2017.

**Your Enrollment Code: <<Enrollment Code>>**

You may call 844-309-7049 at any time if you have questions.

**What You Can Do.**

We have protected your online account by requiring a password reset before your NMG website account can be used again. Therefore, if you have not logged on to your account already, you will be required to reset your password the next time you logon. We recommend you change your password on every other site where you used the same user name and password combination. The most secure passwords are those that are difficult to guess and are used at only one website.

We encourage you to regularly review your accounts with NMG websites, other financial accounts and credit reports, and report any suspicious or unrecognized activity immediately. You should remember to be vigilant and report any suspected incidents of fraud to us or the relevant financial institution.

Never confirm or provide personal information such as passwords or account information to anyone contacting you. The Neiman Marcus Group will never send you any unsolicited emails asking for your account number, password, or other private information.

We also have included an attachment listing additional steps you may wish to consider taking at any time if you ever suspect that you may have been the victim of identity theft. We offer this out of an abundance of caution so that you have information that may be helpful to you, even though loss of a payment card can only lead to fraudulent charges, and you will not have liability for those charges.

We take the security of your information very seriously. We truly regret any inconvenience this incident may cause you. If you have any questions and concerns, please do not hesitate to call us at 1-800-711-7289.

Thank you for your patience and understanding.

Sincerely,

Lindy Rawlinson

Lindy Rawlinson
SVP, Customer Experience & eCommerce
The Neiman Marcus Group

## Important Identity Theft Information: Additional Steps You Can Take to Protect Your Identity

The following are additional steps you may wish to take to protect your identity.

### Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies.

You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

- **Equifax**, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com
- **Experian**, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742. www.experian.com
- **TransUnion**, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. www.transunion.com

### Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

| | | |
|---|---|---|
| Equifax: | Report Fraud: | 1.800.766.0008 |
| Experian: | Report Fraud: | 1.888.397.3742 |
| TransUnion: | Report Fraud: | 1.800.680.7289 |

### Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00, (or in certain states such as Massachusetts, no more than $5.00), each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the following addresses:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348
- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013
- TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- 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
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Don't send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five 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.

To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include (1) proper identification (name, address, and Social Security number), (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze all together, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the security freeze.

Suggestions if You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.
- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Take Steps to Avoid Identity Theft

Further information can be obtained from the FTC about steps to take to avoid identity theft through the following paths: http://www.ftc.gov/idtheft; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at http://www.oag.state.md.us/idtheft/index.htm, calling the Identity Theft Unit at 410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, calling 919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at http://www.atg.state.vt.us.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $5 to place a security freeze on your account, and 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. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.