Neiman Marcus | Group

January 25, 2014

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

Dear General Foster:

I write to inform you that Neiman Marcus Group discovered that a criminal cyber-security intrusion had occurred on its systems which may have affected New Hampshire residents.[1]

In mid-December, the Neiman Marcus Group's merchant processor informed the Neiman Marcus Group of potentially unauthorized payment card activity that occurred following customer purchases at Neiman Marcus Group stores. The Neiman Marcus Group informed federal law enforcement agencies and began working actively with the U.S. Secret Service, the payment brands, its merchant processor, a leading investigation, intelligence and risk management firm, and a leading payment brand approved forensics firm to investigate the situation. As a result of the investigation we initiated, using two of the leading computer forensic investigative firms, we learned for the first time on January 1, 2014 (preliminarily), and then more concretely on January 2 and 3, that sophisticated, self-concealing malware that can "scrape" (copy from temporary memory during execution of payment) payment card information ("the scraping malware") had been clandestinely inserted into our system. We later learned that this malware had been inserted in our system as early as July 2013. Separate, related malware that allows this scraping malware to function appears to have been clandestinely inserted earlier in 2013. Neiman Marcus was not aware of any of this hidden malware until it was discovered this month by our investigative experts. Based on current information, the possibly compromised personal information included name and other Track One payment card data, but, to Neiman Marcus Group's knowledge, did not include other sensitive personal information such as Social Security numbers or dates of birth. The Neiman Marcus Group does not use PIN pads in our stores.

To date, the information provided to the Neiman Marcus Group by its merchant processor and the credit card companies state that about 2,400 unique credit or debit cards used at Neiman Marcus stores were subsequently used for fraudulent transactions. The credit card companies

[1] The Neiman Marcus Group reserves and preserves all of its rights, including that the submission of this report does not constitute a waiver of personal jurisdiction in those states where it does not operate retail locations.

informed us that these cards were all previously used at Neiman Marcus stores. However, for the vast majority of these cards, we have not been provided information about whether these cards were also used at other retailers that may have been subjected to a cyber attack. Therefore, we cannot confirm whether Neiman Marcus or another merchant was the source of information for the fraudulent cards. We have postal addresses for about 71% of these cardholders. The addresses that the Neiman Marcus Group possess indicate that 2 of these individuals are residents of New Hampshire.

On January 10, the Neiman Marcus Group sent emails to those cardholders in this group of approximately 2,400 for whom we had email addresses. We also issued a public statement that we had suffered a data security incident. For those account holders for whom we had postal addresses, we began preparing letters, which were mailed the next business day.

Based on information received at this point in the investigation, which is ongoing, it appears that the scraping malware was active between July 16, 2013 and October 30, 2013, and therefore may have been obtaining payment-card information during this time. At this point in the investigation, it appears that scraping malware was not operating at all Neiman Marcus Group stores and was probably not operating each day during this period. Thus, we cannot state definitively which payment cards may have been impacted by the scraping malware.

The number of unique payment cards used at all Neiman Marcus Group stores during the July 16, 2013 to October 30, 2013, period was approximately 1.1 million. The Neiman Marcus Group does not possess postal address information for approximately 31% of these individuals, and so we have placed a public notice on our website explaining the data security incident, and we are distributing notice to major media outlets.

The addresses that the Neiman Marcus Group does possess indicate that 822 New Hampshire residents used a payment card at Neiman Marcus during the July 16, 2013 to October 30, 2013 period, although the Neiman Marcus Group has more than one address for some customers, and so certain residents may be counted in two states. This information is preliminary, and we expect the information to become more definite as the investigation continues.

On January 16, our CEO Karen Katz issued a public letter, posted on our website with a clear and prominent link from our home page, and explained that we had been the victim of a data security incident. As part of our commitment to our customers, we are offering one free year of credit monitoring and identity theft protection to all customers who shopped with us at any Neiman Marcus Group store or online between January 2013 and January 22, 2014. The notifications and FAQs can be accessed at this link: http://www.neimanmarcus.com/infosecurity. On January 22, we issued individual notifications by email and letter to all customers who used a payment card for any Neiman Marcus Group transaction, in any store or online, any time in the past year for whom we have contact information. Like our website notice, this notification will provide information about the data security incident and the free credit monitoring and identity-theft insurance we are providing.

Notably, these notices are being sent not only to the group of cardholders whose information appears to have been potentially exposed during the period the scraping malware was

operating – based on the information at this point in the investigation – but also to a much larger group. We are taking these broader notification steps in an abundance of caution in light of the uncertainty at this stage of the investigation. Fundamentally, our goal is to communicate to all our customers that taking care of them is and has always been our top concern.

As a precaution, the Neiman Marcus Group is offering complimentary credit monitoring services to all customers who shopped with us at any Neiman Marcus Group store or online, any time between January 2013 and January 22, 2014, and it has provided other precautionary information and measures customers can take to safeguard their identities. For your convenience, a copy of the notice template sent to possibly affected New Hampshire residents is enclosed with this letter.

In response to this incident, the Neiman Marcus Group has taken and is taking a number of steps to contain the situation to help prevent an unlawful intrusion like this from happening again. Among them, the Neiman Marcus Group is:

- Contacting and working directly with federal law enforcement agencies
- Conducting a full review of all of its payment card information systems and vulnerability assessment with the payment brands, its merchant processor, a leading investigations, intelligence and risk management firm, and a leading payment brand approved forensics firm
- Reviewing its intrusion detection systems and firewalls
- Reinforcing its security tools
- Reviewing and hardening its systems
- Modifying its software and security credentials
- Searching for and removing all malware it discovers in the course of its investigation.

If you have any questions or need further information regarding this incident, please do not hesitate to contact David Hoffman at Sidley Austin LLP or Anthony Jannotta at Dentons. Their contact information is listed below.

Sincerely,

Tracy M. Preston
Senior Vice President, General Counsel
Neiman Marcus Group

Contact information:

David H. Hoffman, Sidley Austin LLP
Phone: 312-853-2174
Email: david.hoffman@sidley.com

Anthony Jannotta, Dentons
Phone: 212-768-6870
Email: anthony.jannotta@dentons.com

Neiman Marcus | Group

Karen Katz
President and Chief Executive Officer

We deeply regret and are very sorry that some of our customers' payment cards were used fraudulently after making purchases at our stores. We have taken steps to notify those affected customers for whom we have contact information. We aim to protect your personal and financial information. We want you always to feel confident shopping at Neiman Marcus and your trust in us is our absolute priority. As best we know today, social security numbers and birth dates were not compromised. Customers that shopped online do not appear at this time to have been impacted by the criminal cyber-security intrusion. Your PIN was never at risk because we do not use PIN pads in our stores.

We have taken and are continuing to take a number of steps to contain the situation, and to help prevent an unlawful intrusion like this from happening again. Actions we have taken include working with federal law enforcement, disabling the malware we have found, enhancing our security tools, and assessing and reinforcing our related payment card systems in light of this new threat.

In mid-December, we were informed of potentially unauthorized payment card activity that occurred following customer purchases at our stores. We quickly began our investigation and hired a forensic investigator. Our forensic investigator discovered evidence on January 1st that a criminal cyber-security intrusion had occurred. The forensic and criminal investigations continue.

If you are concerned about fraudulent activity, you can take several steps:

- Check your payment card statements and if any suspicious or fraudulent activity appears, please call your card issuer to report it.
- Contact your local store or call our credit division 1.800.685.6695, if you see fraudulent activity on your Neiman Marcus Card.

The policies of the payment brands such as Visa®, MasterCard®, American Express®, Discover® and the Neiman Marcus card provide that you have zero liability for any unauthorized charges if you report them in a timely manner.

If you have made a payment card purchase at Neiman Marcus between January, 2013 and January, 2014 we will be offering you one year of free credit monitoring service for an added layer of protection. Sign up instructions for this service will be provided at **www.neimanmarcus.com/infosecurity** by Friday, January 24, 2014.

Even as the world of retailing changes and threats to our business such as criminal cyber-security attacks occur, Neiman Marcus Group remains steadfast in our commitment to delivering exceptional customer service.

Thank you for your patience, your trust in us and your business as we deal with this unfortunate and regrettable intrusion.

Sincerely,

Karen Katz

Karen Katz
President and CEO
Neiman Marcus Group

U.S. State Notification Requirements

For additional information, you may contact Neiman Marcus' hotline, hosted by Experian®, at (866) 579-2216, or visit our informational website, www.neimanmarcus.com/infosecurity.

For residents of *California, Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, West Virginia,* and *Wyoming*:

It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account by contacting any one or more of the national consumer reporting agencies listed below. They can also provide you with information about fraud alerts and security freezes.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2104	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834-6790
1-800-685-1111	1-888-397-3742	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com

For residents of *Iowa*:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of *Illinois, Maryland* and *North Carolina*:

State laws require us to tell you that you can obtain information from the Federal Trade Commission about steps you can take to avoid identity theft (including how to place a fraud alert or security freeze). If you are a Maryland or North Carolina resident, you may also be able to obtain this information from your state's Attorney General.

MD Attorney General's Office	NC Attorney General's Office	Federal Trade Commission
Consumer Protection Division	Consumer Protection Division	Consumer Response Center
200 St. Paul Place	9001 Mail Service Center	600 Pennsylvania Avenue, NW
Baltimore, MD 21202	Raleigh, NC 27699-9001	Washington, DC 20580
1-888-743-0023	1-877-566-7226	1-877-IDTHEFT (438-4338)
www.oag.state.md.us	http://www.ncdoj.gov/	www.ftc.gov/bcp/edu/microsites/idtheft/

For residents of *Massachusetts* and *West Virginia*:

State laws require us to inform you of your right to obtain a police report if you are a victim of identity theft. You also have the right to place a security freeze on your credit report. A security freeze is intended 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.

To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a 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 you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

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
www.equifax.com	www.experian.com	www.transunion.com