

January 22, 2014

Honorable Richard Blumenthal  
United States Senator  
724 Hart Senate Office Building  
Washington DC 20510

Dear Senator Blumenthal,

Thank you for your letter dated January 13, 2014. Like you, we at Neiman Marcus are deeply disturbed by the apparently widespread and sophisticated efforts to break into the computer systems of retailers in the United States in an attempt to steal payment card information. As you know, Neiman Marcus recently discovered that we too appear to have been the victim of such an attack, and that sophisticated malware that attempts to evade detection and can obtain credit card information had been clandestinely inserted into our system. We, of course, share your commitment to ensuring that, following such an attack, all reasonable steps are taken to protect consumers whose payment card information may have been put at risk. For over a century, our company's mission has been dedicated to delivering each of our customers exceptional service, and responding properly to this attack is our top priority.

Our internal investigation in this matter – started immediately upon receiving very limited information from our merchant processor that there might be a potential problem – is ongoing, and we will supplement this letter to you with additional information in the future. Based on the information we have to date, here is a summary of the situation:

- We have been notified by Visa, MasterCard, and Discover that about 2,400 unique credit or debit cards used at Neiman Marcus stores were subsequently used for fraudulent transactions. The credit card companies informed us that they believe these card numbers may have been obtained improperly through Neiman Marcus' system. 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.
- We have individually notified – by mail and/or email – each of the approximately 2,400 account holders for whom we have contact information (about 80% of the total). We sent out these email notifications within approximately one week of determining that this malware had been clandestinely inserted on our system, and the letter notifications followed the next business day. Given the uncertainties of investigations of this type, this number may rise as additional information becomes available.
- We have no information suggesting that social security numbers or dates of birth were compromised as part of this incident.
- No PIN data was compromised, as Neiman Marcus does not use PIN pads in our stores.

- We have received no reports from American Express that it has discovered any evidence that any of its card holders have had fraudulent transactions on their account that have been linked to their card use at Neiman Marcus.
- Similarly, we have not received evidence that any “Neiman Marcus” private label credit card holders have had fraudulent transactions on their account as a result of this incident.
- Online transactions at Neiman Marcus Group websites do not appear to have been implicated in any way, as this malware only had the ability to obtain data from cards swiped at physical stores.
- 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 the days following, that sophisticated, self-concealing malware that can “scrape” (fraudulently obtain) 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.
- The investigation is ongoing. Based on information received at this point in the investigation: 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. The number of unique payment cards used at all Neiman Marcus Group stores during this period was approximately 1,100,000. However, at this point in the investigation, it appears that the 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 of these payment cards may have been impacted by the scraping malware. This information is preliminary, and we expect the information to become more definite as the investigation continues.
- We have issued a public notice on our website explaining the data security incident and providing one year of free credit monitoring and identity-theft insurance to anyone who used a payment card at any time in the past year for any Neiman Marcus Group purchase – whether in a store or online. Today we are sending out individual notifications with this information to each of these customers for whom we have address information.
- Notably, these notices are being sent to a much larger group than 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. 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.

Your letter asks questions about the timing of our discovery that the scraping malware had been clandestinely inserted in our system and our notifications and publications of this information. As set out in the chronology below, Neiman Marcus (i) responded immediately upon receiving limited information suggesting the possibility of a data security compromise, (ii) promptly hired leading outside forensic investigative experts upon receiving additional information, and (iii) acted quickly to notify potentially affected cardholders after learning about the scraping malware on January 2 and taking prompt steps to assess and disable it. Specifically:

- On the evening of Friday, December 13, Neiman Marcus was notified by its merchant processor that Visa had identified an unknown number of fraudulently-reported credit cards with a common point of purchase at a small number of Neiman Marcus stores. But the merchant processor had no details concerning the number of cards affected, the credit card account numbers or prior Neiman Marcus transactions. Nevertheless, Neiman Marcus immediately began an internal investigation in an attempt to determine if our systems had been compromised in any way.
- Despite repeated requests from Neiman Marcus over that weekend and on Monday, Neiman Marcus did not receive any further information about fraudulent credit card use from our merchant processor or the credit card companies until Tuesday, December 17, when we received a report about 122 MasterCard cards that had been used in one Neiman Marcus store. The internal investigation focused on this information immediately. On December 18 and 20, Neiman Marcus was sent additional reports from Visa and MasterCard listing a total of 100 additional cards that had been used fraudulently after being used at Neiman Marcus stores.
- On Friday, December 20, based on these new reports, Neiman Marcus hired a leading forensic investigative firm – and one of the firms approved by the PCI Security Standards Council to provide PCI Forensics Investigator services in the U.S – to conduct a thorough investigation in an attempt to discover whether our system had been compromised in any way.
- On Monday, December 23, Neiman Marcus contacted federal law enforcement and reported the situation. Four days later, on Friday, December 27, federal law enforcement asked Neiman Marcus to begin assisting in an investigation. We have been working with federal law enforcement on their investigation since then.
- On Sunday, December 29, our counsel retained a second leading computer forensic investigative firm, Stroz Friedberg, to independently investigate whether Neiman Marcus' system had been compromised. At this point in time, neither the external nor internal investigators had identified a data breach or compromise in Neiman Marcus' system that appeared in any way related to the potential theft of credit card information.
- On New Year's Day, the first investigative firm notified Neiman Marcus that it appeared to have found malware on Neiman Marcus' system that bore indicators relating to payment card transactions and that therefore might be significant in the investigation. On

January 2, the investigative firm informed Neiman Marcus that the malware appeared to have the ability to covertly obtain credit card numbers, and provided more information about the malware on January 3.

- Also on January 3, Neiman Marcus reported this information to its merchant processor, Visa, MasterCard, and Discover.
- The scraping malware was complex and its output encrypted. Over the next several days, the investigative firms worked to decrypt the output file by first reversing the malware to determine the encryption algorithm and then creating a script that employed the attacker's algorithm to the encrypted data in order to decrypt it. It was only after this decryption process was concluded that we were able to determine that payment card information had been captured.
- On January 6, Neiman Marcus was notified for the first time that evidence had been found showing that the scraping malware had been active in more than one store. Working with the investigative firms, Neiman Marcus took blocking actions on the scraping malware that disabled the malware in various ways between January 7 and January 10.
- On January 8, Neiman Marcus provided an investigative update and information about the scraping malware to American Express and Capital One Bank (the issuer of "Neiman Marcus" private label credit cards), neither of whom had provided Neiman Marcus with information indicating the fraudulent use of their cards following card use at Neiman Marcus.
- As set out above, on January 10, Neiman Marcus sent emails to those of the approximately 2,400 account holders for whom we had email addresses. We also issued a 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.
- On January 16, our CEO Karen Katz issued a public letter, posted on our website with an easy and prominent link from our home page, explaining that we had been the victim of a data security incident, and telling our customers that we would provide free credit monitoring and identity-theft insurance for one year to anyone who had used any payment card to conduct any transaction at any Neiman Marcus Group store or online during the past year. The notifications and FAQs can be accessed at this link: <http://www.neimanmarcus.com/infosecurity>. As you may know, in advance of our web posting, we shared this information and these questions and answers with your staff.
- Today, as noted above, we are issuing 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.

As I stated above, our investigations are ongoing, and we expect to obtain additional information as time goes on. But I trust that this detailed chronology will be useful in understanding the steps Neiman Marcus has taken to address this very serious matter.

Your letter asked several additional questions that are not addressed above:

*Did we have plans to announce the breach to the public prior to the breach being disclosed in the media?*

Once the first investigative firm informed us of its discovery of the scraping malware on January 2-3, we not only began an effort to fully understand the scope and effect of this discovery and to design counter-measures against the technology, but also worked to implement plans to notify the credit card companies, financial institutions, the approximately 2,400 credit-card holders for whom we had information, our customers generally, and the public. That effort led to the notification of affected customers which began on January 10.

*What protections are we prepared to extend to our affected customers?*

We have offered each customer that has conducted any Neiman Marcus Group transaction using a payment card in the past year, whether in a store or online, one year of free credit monitoring service, including identity theft insurance, regardless of whether they may have been affected by the data security incident. Today, January 22, we provided our customers with information regarding sign-up instructions for this service.

*Were we using encryption software to protect customer data?*

In an effort to protect our customer's data, we use a number of security protocols, including encryption methods, that exceed those PCI-DSS requirements which do not require encrypting network traffic within the retailer environment. Specifically, when a card is swiped at one of our store registers, its data passes through the register's memory and is then transmitted through an encrypted tunnel to a central point on our network. The data is then forwarded through a firewall to the merchant payment processor over a dedicated circuit.

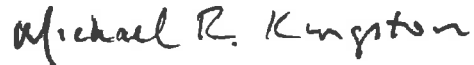
*Were we following a set of best practices with regard to cyber security?*

Neiman Marcus employs a cyber security strategy that is designed to detect, deter, and defend against threats across the enterprise. For example, we use tokenization to protect payment card data after authorization by the merchant processor. Additionally, we deploy technologies to prevent fraud and intrusion, and we also provide annual security awareness training for all our employees who access our systems, among other numerous security practices. Ultimately, we strive for a layered approach to security across the environment by leveraging technology and people to keep our customer data secure.

Neiman Marcus Group

We thank you again for your interest in enhancing cyber security and hope that our forthright responses to your questions help to convey how seriously we at Neiman Marcus take our customers' payment card information. We look forward to answering any further questions you may have.

Sincerely,

A handwritten signature in black ink that reads "Michael R. Kingston". The signature is written in a cursive style with a small dash above the letter 'i' in Kingston.

Michael R. Kingston  
Senior Vice President Chief Information Officer