

# Neiman Marcus | Group

February 26, 2014

Honorable Patrick Leahy  
Chairman, Senate Committee on the Judiciary  
224 Dirksen Senate Office Building  
Washington, DC 20510

Dear Chairman Leahy:

The Neiman Marcus Group appreciated the opportunity to testify before the Senate Committee on the Judiciary during the Hearing entitled “Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime” on February 4, 2014. In response to questions posed during and after the hearing, we have attached a response that has three parts.

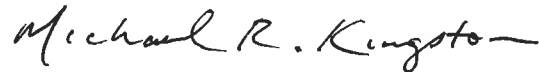
First, after the hearing, you and Senator Grassley sent us additional questions. Our responses are included in Parts A and B of the Attachment.

Second, during the hearing, Senator Blumenthal requested that we provide a more detailed description of how our security practices align with the recommendations issued by Symantec Corp. in its February 3, 2014 report entitled “A Special Report on Attacks on Point of Sales Systems” (the “Symantec Report”). Our response, including information regarding our security architecture, is included in Part C of the Attachment. Given that this information will become part of the public record, we hope you will appreciate our need to provide our response in a way that will not compromise the security of our systems.

Third, we have provided some updated information relating to the forensic investigations of the cybersecurity attack on our system, which is included in Part D of the Attachment.

The Neiman Marcus Group appreciates your interest and concern regarding this urgent matter, and we support the efforts of the Senate, House, consumer groups and the retail and financial services industries to ensure that consumers are able to shop in a secure and trusted environment.

Sincerely,



Michael R. Kingston  
Senior Vice President and Chief Information Officer  
The Neiman Marcus Group

cc: Honorable Chuck Grassley  
Ranking Member  
Senate Committee on the Judiciary  
152 Dirksen Senate Office Building  
Washington, DC 20510

Honorable Richard Blumenthal  
United States Senate  
724 Hart Senate Office Bldg.  
Washington, DC 20510

*Attachment to February 26, 2014 letter from  
Neiman Marcus Group Chief Information Officer Michael R. Kingston to Chairman Leahy*

*A. Response to questions from Chairman Leahy:*

- 1. At the February 4, 2014 hearing, you testified that Neiman Marcus did not currently use so-called "Chip and PIN" technology to process payments. But, you also testified that Neiman Marcus would explore this technology for payment processing at its stores.*
  - a. When do you anticipate that Neiman Marcus would adopt Chip and Pin technology?*
  - b. Do you have any concerns about this technology? If so, please explain.*
  - c. Has Neiman Marcus explored any other payment processing methods to help protect the privacy of sensitive financial and consumer data?*

As part of our ongoing evaluations of new technologies, the Neiman Marcus Group is actively evaluating Chip and PIN technologies. The National Retail Federation has pointed out that retailers like Neiman Marcus need the card brands, merchant banks, issuing banks and consumers to adopt cards with chips (EMV) in coordination with one another before retailers can take meaningful steps in this area.

We agree that "Chip and PIN" is worthy of discussion and has been a focus of the current conversation about payment card data security. We note that Chip and PIN is an older technology at this point, and also has well-documented security gaps, including its limited impact on card-not-present (CNP) fraud (such as online payments). Like many retailers, the Neiman Marcus Group has a growing online business presence. The prevention of CNP fraud is an important consideration for the U.S. economy. In the face of rapidly-changing technologies, we want to make sure that any significant investment we make in payment-card data security is clearly considered a strong and effective best practice that will keep all our customers' payment information safe over the long term.

In the meantime, we continue to evaluate practical improvements we can make in our own payment card environment to increase our robust consumer protections. In particular, we are currently exploring point-to-point encryption capabilities, as well as progressive payment technologies, including mobile payment technologies and platforms that may not require that consumers disclose certain financial information to Neiman Marcus as part of retail transactions.

The Neiman Marcus Group is committed to working with Congress, law enforcement, industry-leading cybersecurity providers, consumer groups, merchant banks, payment card brands, Payment Card Industry (PCI) stakeholders and others in order to enhance the already robust protections that it uses to protect our customers' personal data. We look forward to continuing this important work.

B. Response to questions from Senator Grassley:

1. *The recent attack your company suffered highlights the problem with the current patchwork of state notification laws. There are differing views whether a federal breach notification standard should serve as a “floor” or preempt the current breach notification laws. Given your recent experience with issuing notification, please discuss the following:*
  - a. *How would a federal notification standard that permits states to include additional requirements have affected the company during the wake of the breach?*
  - b. *What would the approach have been if a federal uniform notification standard was in place that fully preempted current notification laws?*
  - c. *What impact would the two different approaches have on a company’s resources as compared to the other, i.e., full preemption versus a federal standard that serves as a “floor”?*
  - d. *Is current law preferable to either of the approaches discussed above?*

The Neiman Marcus Group took swift action to notify its customers as soon as reasonably possible. A federal notification standard, whether with full preemption or serving as a “floor”, would not likely have affected the timing or approach of the Neiman Marcus Group’s response, unless it included substantially different considerations. The timing of our customer notifications was driven not only by our intention to comply with the law, but also by our commitment to providing the highest level of security and service to our customers.

Companies targeted by sophisticated cyber criminal organizations do face significant compliance costs in responding to these attacks because of the current patchwork of state laws. U.S. data breach notification obligations include all but a handful of states, plus the District of Columbia, Puerto Rico and the U.S. Virgin Islands each with their own, varying, data breach notification laws. A federal standard that serves as a floor would not have changed the compliance burdens in any meaningful way. A uniform federal standard, however, would have eliminated some of the complexity involved with the notice process.

2. *In the Congress there are several data breach notification proposals, all of which differ from the other. One important consideration is that of timing for issuing notification. Some legislation requires notice of a breach be issued as soon as possible; another says within 48 hours of discovery. Please describe the general process involved in issuing notice to consumers, including a consideration whether statutory time frames for issuing notifications would be helpful or harmful.*

As detailed in our written statement and further explained at the hearing, the Neiman Marcus Group notified customers as soon as reasonably possible after identifying the malware; disassembling and decrypting it to determine how it operated (including determining whether any consumer information could have been affected); and disabling it in a way that would not draw the attention of cybercriminals intent on harming our customers. The time period from which the Neiman Marcus Group confirmed the malware had the capability to capture payment

card information to the date of containment and customer notification was *four days*. The Neiman Marcus Group began notifying customers the *same day* the malware was contained.

Further, within two weeks, the Neiman Marcus Group took steps to directly notify *all* customers that had shopped at Neiman Marcus Group stores or online between January 1, 2013 and January 22, 2014, for which it had contact information, in addition to the broad public notice from our website and media coverage. The Neiman Marcus Group has no indication that online activity was affected, and we have now confirmed that the malware was in operation only between July 16 and October 30, 2013, and only at certain stores on differing dates within this time period. Nevertheless, out of an abundance of caution, the Neiman Marcus Group chose to make this significantly broader and direct notification, which included one year of free credit monitoring and identity-theft insurance. Fundamentally, our goal is to communicate directly to all our customers that taking care of them is and has always been our top concern.

In our view, any statutory time frame must consider the practical needs of ongoing investigations (including cooperating with law enforcement investigations), the need to restore integrity to compromised systems, the logistics of printing and mailing notices, the need to train customer service representatives with current and accurate information, and the importance of not alerting the criminals responsible for such attacks that they have been discovered at a time when they can inflict additional damage on the merchant and its customers.

3. *Another significant issue concerns the penalties associated with a company's failure to comply with any notification requirements. Do you believe that providing criminal – as opposed to civil – penalties for failing to notify consumers would be helpful or harmful? Why?*

The Neiman Marcus Group promptly provided customers broad and direct notice of its data security incident. The question asks about an entirely different situation, in which a company actually fails to provide any notification to customers whose information was compromised by an incident that falls within a future data-breach-notification statute. In such cases, civil liability would seem a more than adequate incentive to ensure notification is provided. Indeed, to impose criminal penalties on a company that itself has been subjected to a criminal attack seems inappropriate.

4. *Please provide any additional thoughts that you might have on the issues raised by the hearing, including but not limited to expanding on your testimony, responding to the testimony of the other witnesses and/or anything else that came up at the hearing, which you did not have a chance to respond to.*

The Neiman Marcus Group is committed to working with Congress, law enforcement, industry-leading cybersecurity providers, consumer groups, merchant banks, payment card brands, Payment Card Industry (PCI) stakeholders and others in order to enhance the already robust protections that it uses to protect our customers' personal data. We look forward to continuing this important work.



C. Response to question from Senator Blumenthal:

*“... I would like to ask ... you to provide perhaps some detailed answer in writing to the question about whether you were going beyond your present practices and procedures to adopt these steps that Symantec has recommended. Not saying they're the only solutions, but just a kind of benchmark. And if you could provide that in writing, I would appreciate it.”*

The Neiman Marcus Group applauds Symantec's efforts to increase awareness on these persistent, stealthy, and sophisticated criminals. As the report notes, “[d]espite improvements in card security technologies and the requirements of the Payment Card Industry Data Security Standard (PCI DSS), there are still gaps in the security of POS systems.” The Neiman Marcus Group is currently working with and committed to continue working with industry-leading cybersecurity providers, consumer groups, its merchant bank, the major payment card brands, and the other Payment Card Industry (PCI) stakeholders in order to enhance the already robust protections that it uses to protect our customers' personal data.

We view the Symantec Report as an important and respected voice in that dialogue, and we understand that the Symantec Report recommends the following “practical steps to take” in regards to security infrastructure:

1. Implementation of PCI Security Standard
  - Install and maintain a firewall to facilitate network segmentation
  - Change default system passwords and other security parameters
  - Encrypt transmission of cardholder data across open, public networks
  - Encrypt stored primary account number (PAN) and do not store sensitive authentication data
  - Use and regularly update security software
  - Use intrusion protection system (IPS) at critical points and the perimeter of the [Cardholder Data Environment, or] CDE
  - Use file integrity and monitoring software
  - Use strong authentication including two-factor authentication for remote systems
  - Monitor all network and data access [Security Information and Event Management] (SIEM)
2. Test security systems, perform pen-testing, and implement a vulnerability management program.
3. Maintain security policies and implement regular training for all personnel
4. Implement multi-layered protections including outside the CDE. Typically, the attacker will need to traverse multiple networks and layers of security before reaching a POS system. Any single layer that the attacker is unable to bypass prevents successful data exfiltration.
5. Implement [Point to Point Encryption, or] P2PE or EMV (“Chip and PIN”)
6. Increase network segmentation and reduce pathways between the CDE and other networks.

7. Maintain strict auditing on connections to between the CDE and other networks. Reduce the number of personnel who have access to systems that have access to both the CDE and other networks.
8. Employ two-factor authentication at all entry points to the CDE and for any personnel with access rights to the CDE
9. Employ two-factor authentication for all system configuration changes within the CDE environment
10. Implement system integrity and monitoring software to leverage features such as system lockdown, application control, or whitelisting

As I stressed in my written and oral testimony to the Committee, the security of our customers' data is our top priority. We have built, implemented, and maintained a comprehensive, multi-layered array of tools to protect our networks and systems. Our security design provides strong protection to our systems and customer data by any industry standard, including the Symantec Report recommendations. With this orientation, we provide specific responses to each of Symantec's recommendations.

1. The Neiman Marcus Group's security protocols adhere to, and in many cases exceed, those required by the Payment Card Industry ("PCI") Standards. Indeed, although the Neiman Marcus Group is a Level 2 merchant, we voluntarily apply Level 1 assessment practices to our compliance processes by employing a PCI approved annual external assessor. Our level of compliance with the PCI-DSS has just been assessed by a forensic investigative firm with respect to the very systems that were the subject of the incident. That forensic investigative report has now found that the Neiman Marcus Group was fully compliant for all systems relevant to the data security incident and that no recognized deficiency in the security architecture contributed to the incident. (We provide further information about the report in our update below, the last section of this attachment.)

We are not surprised by this result because the Neiman Marcus Group uses numerous firewalls at the corporate and store level, network segmentation, a customized tokenization tool, numerous encryption methods, regular software updating, file integrity monitoring, network access monitoring, and an intrusion detection system. We also require two-factor authentication for external access to user accounts and for various other parts of our networks. We not only require default system password changes, but require users change network login credentials more frequently than the 90 day requirement. And our encryption methods exceed those PCI-DSS requirements which do not require encrypting network traffic within the retailer environment.

2. In addition to the PCI Security Standards, and as recommended in the Symantec report, the Neiman Marcus Group routinely tests its security systems, performs pen-testing, and uses industry-standard and centrally-managed enterprise anti-virus software that is regularly updated.

3. All Neiman Marcus Group personnel who have access to customer data receive regular training on our security policies, including our strict access control policy, which allows only those employees with a legitimate business purpose to access customer data.

4. The Neiman Marcus Group employs a multi-layered defense-in-depth approach to security across the environment by leveraging technology and people to keep our customer data secure. We create multiple roadblocks to intrusions by segmenting our network and applying restrictions to limit traffic for legitimate business purposes only in each segment.

5. The Neiman Marcus Group is committed to working with all relevant industry stakeholders – including, most importantly, our customers – to assess new technologies that can improve the security of our customer’s data, including the use of P2PE, EMV (“Chip and PIN”) technology, as well as next-generation mobile payment mechanisms with even further security protections.

6. We use multiple pairs of firewalls to segment our network and inhibit an intruder’s lateral movement.

7. We maintain significant monitoring and segregation of the connections between the CDE and other networks, and strive to minimize the number of personnel who have access to systems that have access to both the CDE and other networks.

8. The Neiman Marcus Group uses two-factor authentication for all external access to the servers and workstations on the network. Access to the CDE is controlled via policy-based routing, so that a user must be on a host in the network. If the user is not local, then they have to VPN into the correct network, pass two-factor authentication checks, and then be in the right active directory group to be able to remotely access a host in the CDE.

9. The Neiman Marcus Group uses two-factor authentication for all external access to the servers and workstations on the network as described above, but not specifically for system configuration changes within the CDE.

10. The Neiman Marcus Group employs advanced system integrity and monitoring software features including strong system lockdown and application control.

Despite these significant protections, no system – no matter how sophisticated – is completely immune from cyber attack. A recent report prepared by the Secret Service and others in federal law enforcement confirmed this unfortunate reality when they concluded that comparable RAM-scraping malware (perhaps less sophisticated than the one in our case, according to our investigators) had a *zero percent* anti-virus detection rate. Through our ongoing forensic investigation, we have learned – and the Secret Service has confirmed – that the malware which penetrated our system included exceedingly sophisticated features, including some specifically customized to evade our multi-layered security architecture. Therefore, while the Neiman Marcus Group will continue to further improve our systems to better shield against cyber attacks, our recent incident demonstrates that attackers using sophisticated tools to gain access to company networks and systems remain a serious concern for all of corporate America, and we must confront these threats with continued vigilance in coordination with the federal law enforcement officials committed to protecting America’s customers and companies from cybercriminals.



D. Update regarding forensic investigations:

First, we have now completed the next phase in the more detailed review of the time period when the card-scraping malware was operating (July 16 to October 30, 2013), with assistance from our forensic investigators. We therefore have updated numbers to report regarding potentially affected cardholders.

I explained in my February 4 testimony to the Committee that, based upon the information we had at that time, approximately 1.1 million payment cards were potentially exposed during this period, because this was the number of cards used at all Neiman Marcus Group stores during the date range. But I also explained that the malware was not operating at all stores, and where it was operating, it was not operating on each day during the date range. Analysis has now been completed that calculates the number of unique payment cards used at the particular stores and on the particular days when the malware was operating.

This analysis shows that approximately **350,000** cardholders were potentially exposed to the malware, a significant reduction from the previously reported 1.1 million figure. This number may be reduced further in the future, since even on the days when the malware was operating at a particular store, the forensic evidence shows that the malware was not operating during the entire day. The company has now received reports from the card brands and issuing banks that approximately 9,200 cards used at any Neiman Marcus Group store during the July 16 – October 30 period were subsequently used fraudulently. We have updated our website to provide these updated numbers to our customers.

Second, the computer forensic investigative firm we initially hired in this matter – one of the firms approved by the PCI Security Standards Council to provide PCI Forensics Investigator services in the U.S – has now finished its work, and we recently received a final report from them (“the PFI report”). This report (which is highly confidential and contains very sensitive information about Neiman Marcus’ internal security systems) is still under review by the card brands. Nonetheless, we wish to highlight a few points from the report.

The report finds Neiman Marcus to be in compliance with PCI DSS for the relevant systems – that is, all required PCI DSS controls are noted as “In Place,” and the key question, “Potential Contribution to Breach?” is marked “No” for every set of controls.

The report also confirms the date range I previously provided to the Committee regarding the operation of the card-scraping malware. Specifically, the report finds that the first and last known dates that the card-scraping malware was operating in the POS environment were July 16 and October 30, 2013.

The report confirms that, as I testified, related malware that ultimately helped the card-scraping malware function and escape detection was present in Neiman Marcus’ systems earlier in 2013 (March 2013 as set out in the report), and remained undetected in Neiman Marcus’ systems during this time period. The report points out that because of the sophisticated customization of the card-scraping malware, the entries in Neiman Marcus’ endpoint protection logs during the July 16 to October 30 period that showed activity by this malware only listed a program name that was almost identical to the name of the company’s legitimate POS software. These entries on the endpoint protection logs, which occurred over a 3 ½ month period and

numbered in aggregate about 60,000, would have been on average around 1% or less of the daily entries on these logs, which have tens of thousands of entries every day. These logs and numerous other protection logs gathered by the company to analyze information about potentially suspicious activities were regularly examined using various security tools, but because of the sophisticated anti-detection measures taken by the attacker, these well-concealed entries did not reveal the attack. Again, having said this, the report finds that the first and last known dates of card-scraping malware operating in the POS environment were July 16 and October 30, 2013.

Regarding exfiltration, the report states that it did not find any evidence of successful exfiltration of credit card information. According to the report, no known attacker is operating in the environment, and all known malware related to this attack has been mitigated by the containment plan. Moreover, the report confirms that the malware operated at 77 of 85 stores, and that the execution of the malware was not continuous at each store.

*Third*, we also continue to work closely with the U.S. Secret Service on its ongoing criminal investigation. On February 5, the day after this Committee's hearing, the House Committee on Energy & Commerce's Subcommittee on Commerce, Manufacturing, and Trade held a similar hearing. During that hearing, the Deputy Special Agent in Charge of the Cyber Operations Branch of the Secret Service's Criminal Investigations Division testified that the cyber attack on Neiman Marcus – and the malware that was inserted in Neiman Marcus' systems – was highly sophisticated and unprecedented in the manner in which it was customized to defeat Neiman Marcus' defenses and remain undetected. The Secret Service also testified that Neiman Marcus used a robust security plan to protect customer data, but that the attacker nevertheless succeeded in having malware operate in Neiman Marcus' systems because of the attack's level of sophistication.

The PFI report reaffirms the Secret Service's view that this was an extremely sophisticated attack, and confirms that the card-scraping malware was customized for the Neiman Marcus environment and included tools designed to help it escape detection, such as secure deletion, communication across surreptitious channels, and customized encryption.

\*\*\*\*\*