Written Testimony of Michael R. Kingston
Senior Vice President & Chief Information Officer, Neiman Marcus Group

Before the Senate Judiciary Committee
February 4, 2014

Mr. Chairman, Senator Grassley, members of the Committee, I want to thank you for your invitation to appear today to share with you our experiences regarding the recent criminal cybersecurity incident at our company.

For over 20 years, I have held numerous positions in the information technology field, and since April 2012 I have been proud to serve as Chief Information Officer of Neiman Marcus Group. We are in the midst of an ongoing forensic investigation that has revealed a cyber attack using very sophisticated malware. From the moment I learned that there might be a compromise of payment card information at our company, I have personally led the effort, in conjunction with others in senior management, outside consultants, and counsel, to ensure that we were acting swiftly, thoroughly, and responsibly to determine whether such a compromise had occurred, to protect our customers and the security of our systems, and to assist law enforcement in capturing the criminals. Because our investigation is ongoing, I may be limited in my ability to speak definitively or with specificity on some issues, and there may be some questions to which I do not have the answers. Nevertheless, it is important to us as a company to make ourselves available to you to provide whatever information we can, as you attempt to address this important problem that confronts so many corporate and governmental entities around the world.

Introduction

Our company was founded 107 years ago. One of our founding principles is based on delivering exceptional service to our customers and building long lasting relationships with them that have spanned generations. We take this commitment to our customers very seriously. It is part of who we are and what we do daily to distinguish ourselves from other retailers.

We have never before been subjected to any sort of significant cybersecurity intrusion, so we have been particularly disturbed by this incident. It is clear that we are not alone, and that numerous retailers and others in the United States have been recently subjected to sophisticated attacks on their computer systems in an attempt to steal their customers' payment card information. The problem is clearly widespread. And the sophistication of these unprecedented cyber attacks makes the problem very challenging.

Through our ongoing forensic investigation, we have learned that the malware which penetrated our system was exceedingly sophisticated, a conclusion the Secret Service has confirmed with us. The malware was evidently able to capture payment card data in real time right after a card was swiped, and had sophisticated features that made it particularly difficult to detect. These features included some that were specifically customized to evade our multi-layered security architecture that provided strong protection of our systems and customer data. Our security measures included numerous firewalls at the corporate and store level, network segmentation, a customized tokenization tool, numerous encryption methods, an intrusion detection system, a two-factor authentication requirement, and use of industry-standard and centrally-managed enterprise anti-virus software. However, 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 crystallized the problem 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.

Because of the malware's sophisticated anti-detection devices, we did not learn that we had an actual problem in our computer system until ***January 2***, and it was not until ***January 6*** when the malware and its outputs had been disassembled and decrypted enough that we were able to determine how it operated. Then, disabling it to ensure it was not still operating took until ***January 10***. That day we sent out our first notices to customers potentially affected and made widely-reported public statements describing what we knew at that point about the incident.

Simply put, prior to January 2, despite our immediate efforts to have two separate firms of forensic investigators dig into our systems in an attempt to find any data security compromise, no data security compromise in our systems had been identified. A more detailed chronology of the period before January 2 is set out later in my testimony, but specifically:

Tues. Dec.17: We receive a "CPP report" from MasterCard showing 122 payment cards with confirmed fraud use, suggesting that the "common point of purchase" (CPP) *may* have been one Neiman Marcus store where these cards had been previously used over a several-month period.

Wed. Dec. 18: We call forensic investigative firms in order to start an investigation, consistent with the card brand protocol. A new CPP report is received showing 74 cards.

Fri. Dec. 20: We hire a leading forensic investigative firm to conduct a thorough investigation. They start immediately. A new CPP report is received showing 26 cards.

Mon. Dec. 23: We notify federal law enforcement. They follow up with us shortly thereafter and we have been working with them since then. A new CPP report is received showing 2,185 cards.

Sun. Dec. 29: The forensic investigation has not turned up any evidence of a data compromise, and we decide to bring on a second leading forensic investigative firm to accelerate the investigation and help us determine whether we have a problem.

Wed. Jan. 1: For the first time, the forensic investigators find preliminary indications of malware that may have the capability to "scrape" or capture payment card data. This is confirmed on January 2, but it remains unknown whether the malware was able to function on our systems.

Mon. Jan. 6: After days of highly technical work disassembling, decrypting, and decoding the malware and its output files, the investigators conclude that the malware appeared to have been capturing payment card data at numerous stores. The immediate focus of the Neiman Marcus team turns to containing and disabling the malware as it is unknown whether the malware is still capturing card data.

Fri. Jan. 10: The malware appears to be contained and disabled. Neiman Marcus issues public statements identifying the data security incident and begins sending notices to customers on the CPP reports. Prominent coverage follows. We subsequently send out additional notices on our website and to all customers who shopped in any Neiman Marcus store or website during 2013, whether or not potentially exposed to the malware.

Based on the current state of the evidence in the ongoing investigation: (i) it now appears that the customer information that was potentially exposed to the malware was payment card account information from transactions in 77 of our 85 stores between July and October 2013, at different time periods within this date range in each store; (ii) we have no indication that transactions on our websites or at our restaurants were compromised; (iii) PIN data was not compromised, as we do not have PIN pads and do not request PINs; and (iv) there is no indication that social security numbers or other personal information were exposed in any way.

The policies of payment card brands protect our customers from any liability for any unauthorized charges if the fraudulent charges are reported in a timely manner. Nonetheless, we have now offered to any customer who shopped with us in the last year at either Neiman Marcus Group stores or websites – whether their card was exposed to the malware or not – one year of free credit monitoring and identity-theft insurance. We will continue to provide the excellent service to our customers that is our hallmark, and I know that the way we responded to this situation is consistent with that commitment.

December: CPP Reports and Forensic Investigation

This malware was discovered as a result of forensic investigative efforts by two of the leading computer forensic firms, hired by us upon receiving very limited information suggesting that there might have been a compromise regarding payment card data.

Specifically, on the evening of Friday, December 13, we were contacted by our merchant processor that Visa had identified an unknown number of fraudulently-reported credit cards with a possible common point of purchase at a small number of Neiman Marcus stores. The merchant processor provided no details concerning the number of cards affected, the credit card account numbers, or prior Neiman Marcus transactions. This initial report did not provide any indication of a cyber-incident or that our network may have been penetrated, but because even this limited information raised a potential concern, we immediately began an internal investigation to determine what could be responsible for the card fraud and whether our systems had been compromised in any way.

Despite repeated requests to our merchant processor over that weekend and on Monday for more information, we did not receive any additional information until Tuesday, December 17. On that date, we received a Common Point of Purchase ("CPP") report listing 122 MasterCard cards that had been used in one Neiman Marcus store and had subsequently been used fraudulently elsewhere.[1]

On December 18, we received another CPP report, this one listing 74 Visa cards. That day, consistent with Visa's protocols, we began contacting forensic investigative firms. On December 20, we engaged a leading forensic investigative firm to immediately start a thorough investigation of our systems in order to determine whether there was any evidence of a data compromise that might indicate the potential theft of payment card data.

[1] As we understand the general practice, accounts listed on CPP reports are accounts for which the issuing bank and the cardholder are both already aware that the card has been used fraudulently. These CPP reports provide some indication that a particular merchant *may* have a compromise regarding payment card data, based on analysis by the banks and the card brands. This analysis is tentative, not definitive. The reports indicate a level of suspicion that a problem may exist but do not establish that there actually is a problem, or the nature of the problem – including whether the potential theft of the cards relates to cybercrime or more traditional criminal methods. Nevertheless, our internal investigation focused on this information immediately.

Also on December 20, we received additional CPP reports listing a total of 26 Visa and MasterCard cards, bringing the total number of cards on the CPP reports to 222, which had been used at Neiman Marcus over a period of several months. Although we take any indication of potential payment-card theft seriously, this appeared to be a very small number of cards on CPP reports, especially in light of the millions of transactions Neiman Marcus Group conducts annually. News of the Target data security incident and its potential effect on 40 million payment cards was being reported, and this added to the uncertainty about whether the source of any payment card theft was within our system. And we had not received any CPP reports listing any American Express or Neiman Marcus private label credit card accounts.

On Monday, December 23, we received another CPP report which listed 2,185 MasterCard accounts relating to transactions at numerous Neiman Marcus stores. That day, we notified federal law enforcement of the situation, even though the forensic investigators had not found anything significant. In addition to giving them notice of our situation, we wanted to see if they could shed any light on areas where we should focus our attention and to determine if they had seen anything in their other investigations that would assist us in determining whether a compromise had occurred. The Secret Service followed up with us shortly thereafter, and we have been working closely with them since then.

Meanwhile, the investigation continued but was not turning up any evidence of a data compromise. This forensic work involved, among other things, experienced computer investigators looking at hundreds of thousands of files, logs, and other items of data in our system in an attempt to find anything out of the ordinary. However, by December 28, after a week of forensic investigative work, it was still not clear whether there was a problem in our system.

The next day, December 29, we decided to bring in a second leading computer forensic investigative firm to begin conducting an additional, independent investigation. Although the first firm had not found any evidence of a data compromise in our system that appeared in any way related to the potential theft of credit card information, we wanted another expert team to examine our system. Simply put, we wanted to accelerate the investigation and ensure that we were taking the best steps to protect our customers and to learn if our systems had been compromised.

January: Discovery and containment of the malware, and notice to the public and our customers

On January 1, the first investigative firm reported that they had discovered malware that they suspected to have card "scraping" functionality (malware that attempts to fraudulently obtain or capture payment card data). On January 2, the investigators reported that the malware appeared to actually have this functionality. However, they could not say whether the malware had functioned at all in our system, whether it had the capability to successfully capture and exfiltrate card data (that is, send data to an outside source), or whether exfiltration had actually occurred. For the next several days, the two investigative firms engaged in the difficult work of trying to learn what they could about the malware and look for evidence of its operation in different parts of our systems.

Attempting to figure out how the malware functioned was complicated work, requiring the investigators to disassemble the malware program and run tests in our technology labs to try to recreate its functionality. After some time they determined that the malware's output files were encrypted. They then developed a custom decoder to decrypt the output files. They also created a custom-coded scanning tool to determine where and how the malware was operating.

By January 6, we had succeeded in decrypting the output files and in locating the malware at various points on our system. As a result, certain observations about the malware could be made for the first time: the malware apparently operated at point-of-sale registers in multiple stores, and it appeared to have been successful in "scraping" and capturing payment card data at the moment a card is swiped through our Point of Sale system. However, it was unknown whether the malware had actually managed to steal data, the dates when it had been operating, and the full scope of how and where it had been operating.

In addition, our expert computer forensic investigators told us that the malware was highly sophisticated and was different than any other malware they had ever analyzed. Its complex, specialized elements helped to explain how the malware had successfully evaded detection, despite all of the security measures we had in place, in at least five different ways. First, the malware was apparently not known to the anti-virus community and had been written to evade anti-virus signatures. Second, the malware erased its tracks by removing the disk file that had caused it to run, even while the program itself was still running in memory – a highly unusual and difficult-to-achieve feature. Third, when the malware scraped and captured card data, it created encrypted output files, so the output files did not exhibit evidence of card-

scraping activity – until they were decrypted. Fourth, the malware appeared to have features that were custom-built as a result of reconnaissance efforts within our systems that appear to have been clandestinely conducted earlier in 2013. Finally, the malware carefully covered its tracks with a built-in capability that wiped out files evidencing its operation by overwriting them with random data – making forensic detection much more difficult.

Although the investigators knew more about the malware by January 6, they did not know whether the malware was still scraping and capturing card data, and they were concerned that additional customer card data might be getting captured on an ongoing basis. The investigators discussed with us an immediate problem: since the malware was not yet contained, if the attacker learned that we had discovered the malware, there was a significant risk that the attacker might accelerate efforts to obtain captured account numbers, or that other cyber criminals might be encouraged to test our systems for vulnerabilities. Thus, our top priority at that point became disabling the malware.

From January 7 through January 10, we took a variety of steps in an attempt to ensure that the malware could not function. Since we did not yet know the full contours of how the malware functioned, designing a containment strategy was highly challenging. Nevertheless, by January 10, the investigators had a substantial level of confidence that the malware had been disabled.

That day, January 10, Neiman Marcus announced publicly that we had suffered a data security incident and that some customers' payment card information had been potentially compromised. This announcement was widely disseminated by the media in prominent print and broadcast coverage, and appeared on social media. We also sent email notices that same day to all customers whose payment cards were listed on the CPP reports (about 2,400) for whom we had email addresses. The next business day we sent letter notices to all customers in that group for whom we had postal addresses.

On January 16, our CEO Karen Katz issued a public letter, posted on our website with a prominent link from our home page, explaining that we had been the subject of a data security incident, and offering free credit monitoring and identity-theft insurance for one year to any customer who had used any payment card to conduct any transaction during the past year at any Neiman Marcus Group store or website.

Around this time, the investigators became confident that the dates during which the card-scraping malware had been active was July 16 to October 30, 2013. The number of unique

payment cards used at all Neiman Marcus Group stores during this period was approximately 1,100,000. However, the ongoing investigations have not found evidence of the malware operating in all Neiman Marcus Group stores, and it appears that the malware was probably not operating each day during this period based on current evidence. Thus, the number of payment cards that were potentially exposed during this period appears to be lower than 1,100,000, although we have not yet determined how much lower. Because the investigation is ongoing, this information is preliminary.

On January 22, we issued an updated public notice on our website explaining the July 16 – October 30 period and stating that 1,100,000 payment card accounts were potentially exposed. The same day, we sent out individual email and letter notices about the incident to any customer who used a payment card at any time in the past year for any Neiman Marcus Group purchase – whether in one of our stores or on our websites – and for whom we had address information. Our individual notices again provided information about the offer of free credit monitoring and identity-theft insurance.

Notably, we sent this notice – and offered free credit monitoring and identity-theft insurance – to a much larger group than the cardholders whose information appears to have been potentially exposed. Our expanded group included anyone who had used a payment card over a much longer period of time (one year), and website customers (who do not appear to have been exposed to the malware). We took these steps in an abundance of caution because of the ongoing nature of the investigation, and because we want all of our customers to know that we place the highest priority on the security of their personal information.

The ongoing investigation

As with other investigations, computer forensic investigations into data security incidents evolve over time, sometimes in unpredictable ways. We remain in close contact with law enforcement. My statements today are based on the current evidence from the investigations into this recent incident, and therefore should be considered tentative and subject to change. But even though we are still in the midst of discovering the facts, we are pleased to have had the opportunity to provide information to this Committee.

Thank you for your invitation to testify today, and I look forward to answering your questions.