TESTIMONY OF MICHAEL JONES
Before the
EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY SUBCOMMITTEE

MARCH 31, 2009

Good afternoon, Madam Chair, fellow committee members, and distinguished panel members. I am Michael Jones; I serve as the Senior Vice President and Chief Information Officer (CIO) for Michaels Stores, Inc. reporting to the Chief Executive Officer. Thank you for inviting me to discuss the security aspects of credit cards as they impact consumers at retail locations and especially at Michaels.

Michaels Stores, Inc. is the largest specialty retailer of arts and crafts. With more than 1,000 stores in the United States and Canada, the company carries a wide selection of arts and crafts merchandise. Michaels also operates specialty stores under different brand names, including Aaron Brothers and Artistree manufacturing facility. We have annual revenues approaching $4 billion.

I have been with Michaels Stores in my current role for four and a half years. I held the CIO position at Hollywood Video prior to Michaels for over 3 years. Prior to that I spent over 12 years at Kmart, and Kmart related companies, in various leadership positions in Retail technology. I have been in the retail and restaurant industry since graduate school, and indeed, since my sixteenth birthday.

I appreciate the committee's invitation to provide a retailer's view of the state of credit card security. In addition to my own experience I often communicate about this issue with my peers at retailers, restaurants, and other establishments that take credit cards from consumers as a form of payment. My comments today are informed by those discussions as well.

At Michaels the Customer is at the center of everything we do. Her loyalty and patronage of our stores is something we can not afford to lose for any reason. We always want her to feel safe and secure when she is in our stores, with the products we sell, and with the payment mechanism she chooses: whether that be cash, checks, debit cards, gift cards, travelers checks, or credit cards. For many years we have implemented security standards and processes to protect our customers and their important financial information, with our preference always being to keep the least amount necessary to satisfy the payment process. Losing the trust of our customers because we can not safeguard their information is a risk we would not take, regardless of what mandates are imposed on us by an outside organization.

Michaels Stores, Inc. is a PCI certified organization and has been almost since the initial imposition of the standard (i.e., prior to the date where fines were threatened for non-compliance).

I wish I could say that attempting to follow the PCI mandates made me confident that one could say customers' credit card data is completely safe, but unfortunately that is not the case. That is because the mandates seem to have been developed from the perspective of the card companies, rather than from that of those who are expected to follow them.

The PCI Data Security Standards are an extraordinarily complex set of requirements. They are very expensive to implement, confusing to comply with, and ultimately subjective, both in their interpretation and in their enforcement. It is often stated that there are only twelve "Requirements" for PCI compliance. In fact there are over 220 sub-requirements; some of which can place an incredible burden on a retailer and many of which are subject to interpretation.

For example, one of the requirements is that all company associates must annually acknowledge the company security policy. Michaels has an average of 40,000 associates at any given time. In any one week we could have more then 1,000 changes in associates. Well, as you might expect, many of our associates are getting trained on the range of our merchandise, the operation of the registers, fire safety protocols, and other important procedures to assist our customers and protect our operations. So do we also need to get every associate to learn and sign a written statement of our understanding of the credit card companies' security policy? Or do we just need to get associates that may deal with credit cards to sign? This one little PCI mandate has been imposed by compliance vendors differently at retailers across the country both because of its subjective interpretation, and the inability for any large merchant to meet the standard in its most literal form.

We have often been questioned by customers, legislators, and even the credit card companies themselves "Why do you keep credit card information at all?" It would seem with the risk of a breach from the outside or from within, we would be better served not to keep the data at all. We agree completely. As a retail CIO, I would like nothing better than to not store a single credit card number anywhere in our network of systems.

The reason we must still keep credit card information is related to the results of another credit card company procedure designed to protect their banks from loss. It is called a chargeback. It can occur in a number of different ways. It can be initiated by a bank on its own, or it can be initiated at the request of a bank's customer. For example, if a customer spots a charge on his bill that he does not recognize he might initiate a chargeback by contacting his card issuing bank. The card issuing bank asks the merchant's bank to retrieve documentation proving that the purchase took place. The merchant's bank then requires the retailer to produce the underlying documentation for the sale: typically sales media

showing the customer's credit card number, signature and date of purchase. The merchant's bank forwards the information back to the card issuing bank. Often, once the customer sees the underlying documents he remembers the purchase and the matter is closed. (Confusion might occur, for example, if the formal name of the business on the customer's monthly statement –e.g. the XYZ Medical Complex – is different from the name of the business where the customer received services – The Offices of Dr. MDA.)

However, if the retailer is unable to produce the sales media, the sale is reversed and the cost of the transaction is "charged back" against the retailer. This is true even if the transaction were actually made. As I mentioned, banks can also initiate retrieval requests for documentation on their own – it does not have to be triggered by a customer. If the retailer cannot produce the underlying data, the cost of the purchase is taken from the retailer and credited back to the card issuing bank.

We have a department in Michaels dedicated to handling chargebacks. Chargebacks may be for a single transaction or an entire block of transactions. Card issuing banks file retrieval requests that come to us. We must first look up the charge on our systems to match the transaction and identify the store location where the transaction took place (this is what we need the credit card number for). We then initiate a request to the store to "pull" the receipt for that transaction. Since we do not have an electronic signature system we have to get the paper receipt. We then submit that back to the bank along with the original request. If the bank/credit card company determines that the charge was not made by the customer (this is pretty much at their discretion and we have little effective recourse), then we are charged back the amount of the transaction, plus a processing fee.

Thankfully at Michaels, chargebacks are not a very large problem, but my brethren at big ticket companies are not so lucky,

as I know from my previous work experience. We could choose to take the hit and just accept the chargebacks as a cost of doing business so we would not need the credit card number stored but, over time, as word of our vulnerability spreads among the unscrupulous, this would likely cause an increase in chargebacks to the point where we could no longer sustain the losses.

This could have been fairly easily solved and saved retailers hundreds of millions of dollars by having the credit card companies send retailers a unique approval ID back for each approval transaction. We could store that ID and a signature, and if there were a question on the transaction the unique approval ID would indicate how we locate the transaction. This would eliminate the need for us to store the credit card number, but still enable us to respond to retrieval requests. This method would have required changes for retailers, credit card companies, and the banks, but the overall expenditure would have been much less and the consumer data would be much safer.

PCI states that all credit card data must be encrypted. This is a very important component of any data security standard, and one we use for sensitive data all across our organization. There is an exception to this requirement, however. PCI says that data traveling over a "private network" need not be encrypted. It does not state that it can't be, just that it need not be. I have been told that in theory a private network is "more secure" than one that is not private. Well, there is no question about that. A land line data communication connection that is direct between two organizations is certainly more secure then one that traverses the Internet or a wireless network. Michaels has a private network between our stores and corporate headquarters. This network is also isolated from our other networks in the headquarters and the Internet. Access is extremely limited. It is private and secure, and we continually look for ways to make it more secure, after all this is the network millions of our customers' credit card numbers traverse

every year. The security of this network is paramount and probably at least two thirds of the PCI requirements deal with this very subject.

Yet I would still not choose to send my customers' credit card numbers through this network unencrypted. Why? They are encrypted at the pin pad or register by mandate of the standard. It only makes sense that we would keep this information encrypted through our entire network.

Unfortunately this is where the system breaks down. The credit card companies' financial institutions, the very organizations that have created and are mandating this rigorous and highly complex standard, do not accept encrypted transactions. We must decrypt the credit card number at our corporate headquarters prior to sending to the merchant bank for approval!

The transaction is then returned to us un-encrypted and we then re-encrypt it to send back to the store. We, at Michaels, have asked for the past three years for the ability to send encrypted information to the bank. To date, this has not happened. We have heard various ancillary responses to the request such as, "It is too expensive to implement;" "If you (i.e. the retailer) are willing to pay the costs (i.e. the credit card banks' cost) to implement it we will consider it;" to "It would be too difficult to implement a standard encryption routine in the industry."

Why is this the case? One might ask all the consumers affected by the Heartland Payment systems data breach, or TJX Corporation for that matter. It has been suggested that methods used in those breaches capitalized on that flaw. The criminals used a "Trojan Horse" that read the credit card data "in flight." This is not the stored data I spoke of earlier, but rather the numbers that were flowing through the communication channel for approval. One reason thieves could capture this data is because it was not

encrypted. Had it been encrypted they would most likely not have been able to read the data.

Now there are several requirements in the PCI standards for "scanning" systems that look for these types of Trojan Horses. But this is not an ordinary virus that is written and sent to millions of PCs via email. These are incredible technical programs often designed by organized crime syndicates with technical resources that dwarf those of the average company. And with just one inside source in a company they can be made virtually invisible. So why take the chance?

So, are the PCI standards bad? No, however there are some major issues with both the program and the way in which it is implemented.

First, many of the requirements of PCI are already covered in many companies' Sarbanes-Oxley audits. This causes a lot of duplicative work around proof of compliance, and is arguably unnecessary.

Second, the requirements are one-sided against the merchants. The very financial institutions that impose them are not subject to all the mandates themselves. The idea that these organization don't "need" to be audited because they are already held to an audited examination standard is inconsistent with the arguments they make to us (i.e., Sarbanes-Oxley).

Third, The PCI Data Security Standards Council was allegedly spun off from the credit card companies and set up as an independent governing body of credit card company, bank, and merchant representatives. In fact, the council is set up so that the credit card companies and banks retain all power over the ultimate mandates, fines, and anything else connected to PCI. Because of this, the mandates do not represent what is the "best" security, but

rather what is best for the credit card companies and their financial institution partners.

When a breach occurs and card data is stolen, clearly the consumer potentially suffers the most inconvenience. Fortunately, the law provides that promptly reporting consumers must be held financially harmless.

However, the largest financial impact is on the retailer, especially if the credit card companies' data (which by and large we don't want) is seized from a retail location. We are the ones in the press; we are the ones who are demonized; we are the ones states' attorneys general and others threaten with damages and sanctions. Consumers may make decisions not to shop at a breached retailer not realizing that it was the card company processes that caused the data to be placed at risk.

The retailers pay the costs of the fraudulent transactions, either through chargebacks or credit card company imposed fees and penalties. All of this arises from rules that initially grew from a card monopolist that we have no choice but to do business with, or risk the loss of a large portion of our business. It would be impossible for a retailer like Michaels to survive without taking Visa. So we, like other retailers, swallow the tens of millions we have spent to become PCI compliant, in many cases unnecessarily spent, which both reduces profitability and increases the costs of everything we, the merchant, sells.

Is credit card data any safer now than it was before PCI was put in place? Yes. Would it be had PCI not been put in place? Probably. Could the consumers data be safer then it is right now? Most definitely!

But we do not need more laws. The existing (sometimes) misguided enforcement and the proliferation of state regulations

around these issues have created a difficult, if not impossible, environment for retailers to effectively meet the legal requirements imposed on them should a breach of information occur.

Madam Chair, Committee members, and Distinguished panel and guests, if I can leave you with but one message, it is that the precepts underlying the massive dissemination of credit card data need to be rethought. As a CIO, I was informed by one of the top security officers of a major credit card company that based on their analysis our company credit card data had been breached. Although I thought this unlikely, they told me that they had never been wrong. After an agonizing week of internal research, twice daily "all hands on deck" calls, many, many dollars and hours spent, the voice at the other end of the line went dead. The next day a breach of over 40 million credit card numbers was announced at a bank processor. Our "incident" apparently showed that the card company's analysis at that time had not counted on breaches of such magnitude, since we were later told that the data which had triggered all of our activity was more likely a subset of "another issue" they were dealing with.

I am proud to report that Michaels has never had evidence of a breach of consumer data. Regardless of the outcome here we will continue to do whatever is necessary and prudent to keep the loyalty of our customers for, without that, we cease to exist. But the future would be more secure and the risks to us all far lower were the card companies to take greater responsibility for the inadequate system of payment they have created and asked us to use.

Thank you. I am happy to answer any questions you may have.