TESTIMONY OF DAVID HOGAN
ON BEHALF OF THE NATIONAL RETAIL FEDERATION
before the
EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY SUBCOMMITTEE

MARCH 31, 2009

Thank you Chairwoman Clarke, members of the committee. My name is Dave Hogan. I am Senior Vice President, Chief Information Officer for the National Retail Federation.

By way of background, the National Retail Federation (NRF) is the world's largest retail trade association, with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet, independent stores, chain restaurants, drug stores and grocery stores as well as the industry's key trading partners of retail goods and services. NRF represents an industry with more than 1.6 million U.S. retail establishments, more than 24 million employees - about one in five American workers - and 2008 sales of $4.6 trillion. As the industry umbrella group, NRF also represents more than 100 state, national and international retail associations.

I have been with NRF for almost 7 years and have spent my entire career in retail information technology. Prior to joining NRF I was a business unit CIO for The Limited and most recently CIO for international retailer, Duty Free Americas. During that time I became familiar with the broad array of issues confronting retail CIOs, including matters related to data security. Both in my prior positions, as well as during my time at NRF I have helped design and upgrade the systems that protect my companies' core records.

Currently, I also work with the NRF's CIO Council. The Council is made up of more than 50 well known retailers who meet regularly to study, share and discuss best practices and challenges inherent in ever more sophisticated retail technology programs. As a result of that work I have become familiar with many of the issues involved with the Payment Card Industry Data Security Standards.

Credit card security is not, however, a new issue for retail. For years many retailers managed their own in-house credit programs. Companies such as Sears and JCPenney offered proprietary retail credit through cards issued in all fifty states. They were known as proprietary programs because for most of their history, the cards were owned by the retailer and used exclusively for the purchase of a retailer's merchandise. Beyond credit programs, many companies maintain information about their most valuable customers, often gleaned through loyalty programs. Those programs are used to encourage our customers to shop and to serve them better when they do. All of this information was valuable and proprietary.

For this reason retailers developed programs to secure their data. Each retailer's program was commensurate with the sensitivity of the data it sought to keep. Certainly, as to their cards, for example, no retailer wanted its credit card programs to be appropriated by thieves. Therefore, we retailers developed systems designed to minimize losses to us and inconvenience to our customers.

There have been two big developments in the last dozen or so years that have scrambled the playing field. The first has been the rapid proliferation of what are known in the industry as third party, general purpose credit cards. Visa and MasterCard are two examples. These cards are not issued by retailers, but rather are issued by independent banks under a particular card brand's name. Thus you might have a Citibank MasterCard or a Chase Visa or a Citibank Visa. Consistent with their internal standards, the banks issue the cards as broadly as possible, in hopes that each card will generate income for the bank.

The other big change has been increasing computerization and the related growth of the Internet. As you all know computers are now ubiquitous. And many of our governmental, commercial, and personal activities are greatly dependent upon access to the web. Unfortunately, the same processes that give us access also are available to the unscrupulous. Scams that would have been difficult to accomplish, or been limited in scope if they were attempted on a face to face, individual-by-individual basis, such as eliciting banking account information from individuals, can be much more efficiently accomplished on-line by "phishing," for example, among those who engage in banking from their home computers.

In a brick and mortar environment, retailers accept a variety of forms of payment: cash, checks, credit cards, gift certificates and other script. Retailers accepted credit cards for payment, in part, because they had been assured by the card companies that if the merchant followed a limited number of steps (e.g., confirming the card's presence; checking the signature; obtaining an approval; and keeping a copy of the completed charge media) they would be given a guarantee of payment. Whether it be by cash, check or otherwise, the payment mechanism is really just a means of accomplishing business. Most retailers are not in the payment acceptance business any more than their customers are in the payment delivery business. The form of payment simply facilitates the underlying business to be done. (The consumer is searching for something to wear; the merchant is seeking to find and display attractive merchandise that customers desire wearing.)

A few years back, outside of the brick and mortar environment, in the then newly developing world of Internet shopping, it soon became apparent to the credit card companies that they should take additional steps to minimize losses from the use of their card products for on-line purchases. Through a combination of rules and new security requirements the card companies were largely able to achieve that goal. They adopted special security requirements for on-line merchants (Visa's program was called CISP: Customer Information Security Program). They also declared that the then growing number of Internet merchants who accepted a credit card for payment on-line would be 100% liable for any loses if charges were challenged, either by the cardholder or by the

bank. As a practical matter, for on-line merchants, there was little or no payment guarantee.

Over time, however, the card companies realized that the number of fraudulent purchases was continuing to rise. And this was true not just on-line. Thieves and others learned that if they could obtain the data on the credit card companies' cards, they could accomplish a few fake transactions (on-line) or even create fake cards and accomplish many fraudulent transactions in a wide variety of brick and mortar locations.

The growth of computerization facilitated these breaches. Globally, there have been numerous instances of hackers accessing computer systems, stealing credit card information, and using this data to commit fraud. It has been reported that many of these hackers are operating out of Eastern Europe and some of the former Soviet states. In several cases they have targeted retailers' computer systems that process or store credit card data. But the thieves are really looking for the data anywhere they can find it.

As with the growth of on-line shopping fraud, these developments presented the card industry with a challenge. In response, they introduced what they call the Payment Card Industry Data Security Standards, commonly called PCI. Since its inception, PCI has been plagued by poor execution by Visa, MasterCard and the other credit card overseers of the program. The PCI guidelines are onerous, confusing, and are constantly changing. Many retailers say that basic compliance is like trying to hit a rapidly moving target.

As I mentioned, retailers take data security very seriously. Indeed, merchants, banks, the major card brands and the vendor community that supplies our industry with hardware and software all want to reduce the incidence of credit card fraud. PCI is an attempt to prevent large stockpiles of credit card data from getting into the wrong hands. But the premise of PCI, that hundreds of thousands or even millions of merchants will systematically keep pace with the ever evolving sophistication of professional hackers, is unrealistic.

PCI is little more than an elaborate patch. While PCI can reduce some fraud, at extraordinary cost, it is not nearly as effective as a redesign of the card processes themselves. Since its inception, our industry has spent billions on compliance programs and related data security systems. PCI protocols have required many merchants to scrap good, existing data security programs and replace them with different security programs that meet PCI rules but aren't necessarily any better. Retailers have been required to take extraordinary steps to ensure that somewhere, somehow, data is not inadvertently being retained by software. However, what is ironic in this scenario is that the credit card companies' rules require merchants to store, for extended periods, credit card data that many retailers do not want to keep.

To many NRF members, it appears that the credit card companies are less interested in substantially improving their product and procedures than they are with reallocating their fraud costs. In our view, if you peel off all the layers around PCI Data Security Standards, you will see it for what it is – in significant part, a tool to shift risk off

the banks' and credit card companies' balance sheets and place it on others. It is their payment card system and retailers -- like consumers -- are just users of their system.

As I mentioned, all of us - - merchants, banks, credit card companies and our customers - - want to eliminate credit card fraud. But if the goal is to make credit card data less vulnerable, the ultimate solution is to stop requiring merchants to store card data in the first place.

For example, rather than requiring that merchants keep reams of data - - currently required under card company rules in order to satisfy card company retrieval requests - - credit card companies and their banks should provide merchants with the option of keeping nothing more than the authorization code provided at the time of sale and a truncated receipt. The authorization code would provide proof that a valid transaction had taken place and been approved by the credit card company, and the signed sales receipt would provide validation for returns or poof of purchase. Neither would contain the full account number, and would therefore be of no value to a potential thief. Any inquiries about a credit transaction would be between the cardholder and the card-issuing bank.

If all merchants took advantage of this option, credit card companies and their member banks would be the only ones with large caches of data on hand, and could keep and protect their card numbers in whatever manner they wished. The bottom line is that it makes more sense for credit card companies to protect their data from thieves by keeping it in a relatively few secure locations than to expect millions of merchants scattered across the nation to lock up their data for them.

In fact, we proposed such changes to the PCI Security Standards Council in 2007. The card industry dismissed our proposal without addressing its merits but have yet to offer a viable alternative.

Once the payment system itself becomes a burden, commerce inevitably suffers. The NRF, with direction from our CIO Council, has engaged the PCI Security Standards Council directly and highlighted flaws with the existing "standard" and "governance" of the PCI Security Standards Council. There have been numerous suggestions made over the years that would significantly reduce the chances of major data breaches, but none have been adopted.

In conclusion, we believe any of our suggestions would be more effective and efficient approaches to protecting credit card data and preventing a continuation of the data breaches that have been seen in recent years.

Thank you for the opportunity to appear before the Committee today, I would be happy to answer any questions.