PREPARED STATEMENT
CHAIRWOMAN YVETTE D. CLARKE (D-NY)
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY
COMMITTEE ON HOMELAND SECURITY

MARCH 31, 2009 HEARING:
"DO THE PAYMENT CARD INDUSTRY DATA STANDARDS REDUCE CYBERCRIME?"

In recent years, a number of well-known companies have experienced massive data breaches on their internal computer networks, resulting in the compromise of sensitive customer data. The criminals who perpetrated these intrusions targeted the credit and debit card account information held by merchants or third party data processors as the result of retail transactions. With a thriving black market that rapidly packages and sells stolen cardholder data, the information compromised during these breaches may ultimately aide any number of criminal organizations.

We know that some percentage of the fraudulent charges and illicit business from these activities is used to fund terrorist activity throughout the world. In his 2002 autobiography, the Bali nightclub bomber specifically referred to online credit card fraud and carding as a means to fund terrorist activities, and encouraged his followers to use this method to obtain financing. More recently, a British case involving three jihadis alleged that the men used stolen credit card numbers obtained through phishing scams and Trojan horses to make more than $3.5 million in fraudulent charges. The jihadis reportedly used the numbers at hundreds of online stores to purchase equipment and other items, including prepaid cell phones and airline tickets, in order to aid jihadi groups in the field.

The Subcommittee is holding this hearing today to voice our concern about the growing number of data breaches; to understand what is being done to curb this activity; and to suggest that both merchants and the payment card industry have significant work ahead to meet our expectations.

The payment card industry – Visa, MasterCard, Discover, American Express, and JCB – requires every business that stores, processes, or transmits cardholder data to comply with specific data security standards. The intent of these standards is to reduce the likelihood of successful data security breaches. On an annual basis, these merchants must certify that they are compliant with the Payment Card Industry Data Security Standards, known as "PCI Data Security Standards."

The PCI Standards contain a number of security controls that businesses must implement. The PCI Standards allow smaller businesses to self-certify compliance, while larger merchants must be validated by a qualified security assessor. Enforcement comes through the card companies themselves, who can levy fines and/or prohibit non-compliant merchants from using their services. To be clear: the PCI Standards are not government regulations, and are not enforced by the government. This Committee supports industry created and managed security standards, as long as they are strong and effective.

In light of the rising number of publicly reported data breaches, Chairman Thompson launched an investigation to determine whether the PCI Standards have been effective in reducing cybercrime. The results of this investigation suggest that the PCI Standards are of questionable strength and effectiveness.

The effort to become "PCI compliant" is a daunting challenge for merchants, whose core competency is the selling of merchandise rather than expertise in security. The costs for the largest merchants can be as high as $18 million a year. Many believe that if they complete this arduous task, they will be rewarded with a secure system. But the Committee's investigation confirms what many analysts have known for years. In the words of one credit card company, "full compliance with the PCI standard does not guarantee that the merchant or vendor will not become the victim of a data breach."

Take last year's data breach at Hannaford Brothers Company for example. Hackers installed malicious code on servers at every one of the grocery stores in the Hannaford chain. The malware intercepted the data stored on the magnetic stripe of payment cards as customers used them at the checkout counter. Hannaford received certification that they were PCI compliant on February 28, 2008. But on February 27, 2008, according to documents obtained by the Committee, Hannaford received notice that a number of credit card numbers from Hannaford's network were stolen and being used on the black market. In other words, Hannaford was being certified as PCI compliant while an illegal intrusion into its network was in progress.

I do not believe the PCI Standards are worthless; in the absence of other requirements, they do serve some purpose. But I do want to dispel the myth once and for all that PCI compliance is enough to keep a company secure. It is not, and the credit card companies acknowledge that.

The bottom line is that if we care about keeping money out of the hands of terrorists and organized criminals, we have to do more, and we have to do it now. Specifically, we must improve our policies and our technology. First, the standards have to be better because they are inadequate to protect against the methods used by modern attackers. Despite what the credit card companies say, for millions of small and large businesses out there, the PCI Standards are the ceiling and not the floor. The bar has to be raised. In this dynamic threat environment, attackers are constantly ahead of defenders. And yet the PCI Standards are updated – only by unanimous consent – every two years. Part of the problem is that the standards do not require more frequent penetration testing. The only way to reduce breaches is by continuously testing and attacking a system through penetration testing and timely mitigation.

Second, the payment card industry and issuing banks need to commit to investing in infrastructure upgrades here in the United States. In a response to the Committee's investigation, one breached company noted that "the effectiveness of data security standards in inherently limited by the technology base of U.S. credit and signature debit card processing networks. Credit and signature debit transactions are not protected by encrypted PINs. Implementation of encrypted PINs for all credit and debit card transactions could be useful."

Countries in Europe and Asia are deploying new technologies – like chip and PIN – to fight fraud that could lead to organized crime and terrorism, and it is working. According to the U.K. payments association, three years after beginning the migration to chip-card technology, losses on transactions had reduced by 67 percent from 219 million pounds in 2004 to 73 million pounds in 2007. However, despite card fraud dropping 32 percent domestically between 2006 and 2007, overall counterfeit card fraud affecting U.K. consumers was up 46 percent. Why? The cards were being used by malicious actors in countries that had not yet implemented the technology.

The U.S. is being blown away by security investments overseas, and our 1950's era system is making us a weak link in the security chain. Magnetic stripe-based technology is outmoded and inherently less secure when compared to smart cards or other developing technologies. While I am deeply concerned about our security, the payment card industry and issuing banks should be ashamed about the current state of play and doing everything possible to immediately institute improvements in infrastructure.

I know that our witnesses care about keeping financial information out of the hands of the terrorists and organized crime elements. I know that the payment card industry cares; I know that the merchant community cares. But the time for waiting is over. The time for shifting risk is over. Today, the responsibility is yours to make this situation better.

This is the first step in the Committee's review of the payment card industry's efforts, a review that I believe the Chairman plans to continue. We look forward to hearing about your plans to improve America's cybersecurity posture, and working with you all in the weeks and months ahead.