AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

DO THE PAYMENT CARD INDUSTRY DATA STANDARDS REDUCE CYBERCRIME?

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

MARCH 31, 2009

Serial No. 111–14

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

52–239 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
ANN KIRKPATRICK, Arizona
BEN RAY LUJÁN, New Mexico
BILL PASCRELL, JR., New Jersey
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
JAMES A. HIMES, Connecticut
MARY JO KILROY, Ohio
ERIC J.J. MASSA, New York
DINA TITUS, Nevada
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
PETE OLSON, Texas
ANH "JOSEPH" CAO, Louisiana
STEVE AUSTRIA, Ohio

I. LANIER AVANT, *Staff Director*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

YVETTE D. CLARKE, New York, *Chairwoman*

LORETTA SANCHEZ, California
LAURA RICHARDSON, California
BEN RAY LUJÁN, New Mexico
MARY JO KILROY, Ohio
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DANIEL E. LUNGREN, California
PAUL C. BROUN, Georgia
STEVE AUSTRIA, Ohio
PETER T. KING, New York *(Ex Officio)*

JACOB OLCOTT, *Staff Director*
DR. CHRIS BECK, *Senior Advisor for Science and Technology*
CARLA ZAMUDIO-DOLAN, *Clerk*
COLEY O'BRIEN, *Minority Subcommittee Lead*

CONTENTS

Page

STATEMENTS

The Honorable Yvette D. Clark, a Representative in Congress From the State of New York, and Chairwoman, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology 1
The Honorable Daniel E. Lungren, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology 4
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Chairman, Committee on Homeland Security .. 6

WITNESSES

Ms. Rita M. Glavin, Acting Assistant Attorney General, Criminal Division, Department of Justice:
Oral Statement 7
Prepared Statement 9
Mr. Robert Russo, Director, Payment Card Industry Data Security Standards Council:
Oral Statement 24
Prepared Statement 26
Mr. W. Joseph Majka, Head of Fraud Control and Investigations, Global Enterprise Risk, Visa, Inc.:
Oral Statement 30
Prepared Statement 32
Mr. Michael Jones, Senior Vice President and Chief Information Officer, Michaels Stores, Inc.:
Oral Statement 35
Prepared Statement 37
Mr. David Hogan, Senior Vice President, Retail Operations, and Chief Information Officer, National Retail Federation:
Oral Statement 40
Prepared Statement 42

FOR THE RECORD

Submitted for the Record by Chairwoman Yvette D. Clarke:
Statement of Andrew R. Cochran, Founder and Co-editor, The Counterterrorism Blog 18
Statement of Kirsten Trusko, on Behalf of the Network Branded Prepaid Card Association 20

APPENDIX

Questions Submitted by Chairwoman Yvette D. Clarke 51

DO THE PAYMENT CARD INDUSTRY DATA STANDARDS REDUCE CYBERCRIME?

Tuesday, March 31, 2009

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY,
Washington, DC.

The subcommittee met, pursuant to call, at 2:11 p.m., in Room 311, Cannon House Office Building, Hon. Yvette D. Clarke [Chairwoman of the subcommittee], presiding.

Present: Representatives Clarke, Richardson, Luján, Thompson [ex officio], and Lungren.

Ms. CLARKE. The subcommittee will come to order. The subcommittee is meeting today to receive testimony on whether the payment card industry data standards reduce cybercrime.

Good afternoon. In recent years, a number of well-known companies have experienced massive data breaches in 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 aid a number of criminal organizations. We know that some percentage of the fraudulent charges and illicit businesses from these activities is used to fund terrorist activity throughout the world.

In his 2002 autobiography, the Bali nightclub bomber specifically referred to on-line 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 fishing scams and Trojan horses to make more than 3.5 million in fraudulent charges. The jihadis reportedly used the numbers at hundreds of on-line 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 and to understand what is being done to curb this activity and to suggest that both merchants and the pay 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 computer 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 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 noncompliant 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 cost 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 be the victim of a data breach.

Take last year's data breach of Hannaford Brothers Company, for example. Hackers installed malicious code on servers to 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 the documents obtained by the committee, Hannaford was notified that a number of the credit card numbers from its 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 that 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. 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 being used by modern hackers and 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 must 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 2 years.

But 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 is 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 debit and credit 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, 3 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. customers was up 46 percent.

Why? The cards were being used by malicious actors in countries that had not yet implemented the technology. The United States is being blown away by security investments overseas and our 1950s-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 terrorists and other organized crime elements and 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 in all the weeks and months ahead.

The Chairwoman now recognizes the Ranking Member of the subcommittee, the gentleman from California, Mr. Lungren, for an opening statement.

Mr. LUNGREN. Thank you very much, Madam Chairwoman. I want to compliment you for scheduling this important data security hearing. It is an issue that most people are aware of, but few seem to understand the full extent of this threat or the remedies required to eliminate it as much as possible.

The new Information Age created by computers, the internet, and instant communication offers many benefits to the Nation, particularly our economy. Transacting business on the internet is one of the key benefits of the Information Age.

Utilizing, obviously, credit cards today is the way people normally transact business. It is the new currency of our age. A lot of people don't even carry cash around anymore. In fact, sometimes you try to pay with cash and people look at you, trying figure out what scam you have going on.

I was at one place where I actually had a 50-cent piece that I was trying to utilize and the woman would not recognize it as an American currency. I was trying to explain to her the image on the surface, and she just evidently missed that history lesson about that President.

The internet has acted as a powerful economic engine for the U.S. economy. Unfortunately, these new business opportunities carried via the internet have also transformed the landscape for the criminal, making available a wider array of new methods that identity thieves can use to access and exploit the personal and financial information of others.

Today's skilled computer hackers are capable of perpetrating large-scale data breaches that leave tens of millions of individuals at risk of identity theft. I recall my wife and I were at dinner one night, I gave the card to the waiter. After 5 minutes, the waiter came back kind of embarrassed and said, well, Mr. Lungren, this card doesn't seem to be working. So I turned to my wife and said, Why don't you give them the card? She gave them the card with the same account. They came back later and said it is not working. Luckily my wife had another card.

If I had been in Chicago, changing planes, and needed to stay overnight there, I would have been up the creek without a paddle, as we say. I went home that night, called in to the credit card company and they informed us there had been a credit card compromise. Our account had been compromised. They would tell us nothing more than that. My wife went on-line to see what our account was at that point in time. There was no such account. It was as if it had vanished.

The point I am making is we were never notified by the credit card company. We have a number of automatic payments that are made against the card and we tried to track every one of them, and missed one of them and got a notice that we had not paid that month for something.

So we are putting a tremendous obligation on the entire industry in this case. One is to try and secure things. The other one is when there is a breach, what is your requirement to notify people? Under what circumstances do you notify people? If you are not giving that information to those of us who are the consumer, is that information being given to law enforcement to follow up in all circumstances? Those are just some of the questions.

The key to this internet economic engine running smoothly is data security. There is no doubt about it. If we are unable to secure our on-line financial transactions from financial criminals, even those not involved in terrorism, then our economic growth will be jeopardized, and actually we have fulfilled the terrorist dreams of pulling down our country through an economic attack. Customers will reject on-line purchases if they can't be assured that their payment card transactions are protected. Without consumer or customer confidence in the safety of the payment card transaction, internet commerce would dry up and we could have problems with people just using the card when they are actually at brick-and-mortar stores.

We know it was a huge problem in the early days of the internet when it was an unknown frontier. Unchecked criminal activity will bring back those wild west days, undermine customer confidence, and cripple internet commerce. I applaud the payment card industry for investing their resources and personnel to develop and promote a universal data security standard. As was mentioned, it is voluntary. We understand that. A lot of work has gone into it. We understand that there is always the challenge. It is easy for those of us in Government to say we can do a better job. Thank God we haven't had any security breaches on the part—excuse me—I guess we have had a couple of them here and there. All that points out is it is a real challenge to stay ahead of the bad guys.

I mean, you have got mischievous hackers, you have got individual criminal hackers, you have got criminal enterprise hackers, you have got transnational organization hackers, you have got nation-state hackers and, frankly, you have got to try to protect against all of that.

The PCI Security Standards Council that includes all of the major card brands has at least understood that there is a need for a set of comprehensive requirements for enhancing payment account security. One of the questions I would ask: Is there any place for the retailers to be involved in discussion of those standards and part of that? Another question I would ask is: I know you have some flexibility within the standards as they exist now. But is it still too much of one size fits all? In other words, I know you have a demarcation between mom-and-pop stores and the big retailer, but in between does it make sense? Are the standards flexible enough to be effective on the one hand and at the same time allow for different business models to operate in a reasonable fashion for them?

So I realize that the first standard was developed in 2006 to improve the standard security in the payment card industry. It has improved the situation. More needs to be done. We are trying to identify those areas that need to be done. We have trying to make sure all the parties are brought to bear on the question. We are looking to see if Government regulation is needed.

The last thing I would say is this. The challenge for us in Government is to try to ensure that we don't interfere with the ingenuity of the private sector in being able to put the fixes into the security system that are necessary. If you can help us in that regard, not only will you benefit, we will benefit as well. Thank you very much, Madam Chairwoman.

Ms. CLARKE. The Chairwoman now recognizes the Chairman of the full committee on Homeland Security, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

Mr. THOMPSON. Good afternoon. Thank you, Madam Chair, for holding this very critical hearing on the effectiveness of the PCI standards.

From our personal computers to Government networks to our critical infrastructure, the United States is under attack in cyberspace. This adversary ranges in skill from unsophisticated to highly capable, from loan hackers to organized crime and nation-states. Their intent ranges from nuisance and disruption to theft, espionage, and warfare. Their successes are varied.

From every hacker that we have caught and prosecuted, thousands continue to work unabated. In December 2008, the Center for Strategic and International Studies concluded that the battle for cyberspace is one that we are not winning.

Willy Sutton was rumored to have said he robbed banks because that is where the money is. In today's world of payment card transactions, the money is now located on computer networks. On any given day, billions of dollars float back and forth between merchants and payment card networks which process credit card numbers for transactions in an area that is ripe for hackers to exploit, and they are taking advantage of weaknesses in the system.

We are here today to learn about the private sector's efforts to combat data breaches and cybercrime and to assess the quality of the payment card industry data security standards. The standards have been around for several years, but massive on-going data breaches at some of America's largest merchants suggest that the standards are inadequate to prevent breaches.

The essential flaw with the PCI standards is that it allows companies to check boxes, but not necessarily be secure. Checking boxes makes it easier to assess compliance with the standard, but compliance does not equal security. We have to get beyond checkbox security. It provides a false sense of security for everyone involved, and it is ineffective in reducing the real threats. Companies need to understand that even if 100 percent compliance with PCI standards is achieved, hackers will continue to develop techniques to exploit the computer systems of companies holding cardholder data. You are not safe unless you continually test your systems.

Today we are calling for change. I call on the payment card industry, and the thousands of merchants and vendors who have to comply with the standards, to rededicate themselves to the goal of securing their networks. For the payment card industry and the issuing banks, this is going to mean significant investment in the infrastructure upgrades. As the Chairwoman has pointed out, these investments are already on-going overseas.

I am puzzled and disappointed that we are not seeing similar upgrades here domestically, and I hope our witnesses can explain why the card industry appears not to be moving quickly to address these issues. I am also deeply troubled by the testimony that suggests credit card companies are less interested in substantially improving their product and procedures than they are in reallocating their fraud costs. The payment card industry's efforts to shift risk appears to have contributed to our current state of insecurity, and

I am concerned that as long as the card industry is writing the standards, we will never see a more secure system.

We in Congress must seriously consider whether we can continue to rely on industry-created and -enforced standards, particularly if they are inadequate to address the on-going threats.

I look forward to working with my colleagues on both sides of the aisle and across committee lines to further explore whether Government action is necessary to protect against these threats. One thing is certain: The current system is not working.

Madam Chairwoman, I thank you for your work in this area, and I look forward to the testimony of both panels.

Ms. CLARKE. Thank you very much, Mr. Chairman. Other Members of the subcommittee are reminded that under the committee rules, opening statements may be submitted for the record.

We are going to take a break right now for votes. They have come up and we are scheduled for three votes, which puts us at about 25 minutes. Well, now it is less than 25 minutes, maybe about 15. So please excuse us as we go and recess for votes.

[Recess.]

Ms. CLARKE. I welcome our only panelist on the Federal panel, Ms. Rita Glavin, Acting Assistant Attorney General, Criminal Division, Department of Justice. In June 2008, Ms. Glavin joined the Criminal Division as the Acting Principal Deputy Assistant Attorney General. Ms. Glavin began her service to the Department in 1998 through the Department's honors program as a trial attorney in the public integrity section where she worked until 2003. Since 2003, Ms. Glavin has been an assistant U.S. attorney with the United States Attorneys Office for the Southern District of New York.

Without objection, this witness' full statement will be inserted into the record. I now ask you to introduce yourself and summarize your testimony for 5 minutes.

STATEMENT OF RITA M. GLAVIN, ACTING ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE

Ms. GLAVIN. Good afternoon, Chairwoman Clarke, and thank you for the invitation to address the subcommittee. As you know, identity theft is not a new problem. However, in recent years, identity thieves have begun to capitalize on a variety of new methods to access and exploit the personal information of others. Skilled hackers are now capable of perpetrating large-scale data breaches that leave hundreds of thousands of individuals and, in some cases, millions of individuals at risk of identity theft.

The Department of Justice, along with our law enforcement partners, has been aggressively investigating and prosecuting these data breaches and other criminal activity associated with them. We are committed to continuing our efforts. We have historically had tremendous success in identifying, investigating, and prosecuting the perpetrators of these acts. But as always, we can and we will do more.

To that end, the continued and improving coordination with our partners in the international community and in the private sector

will be critical to ensuring our success. We are glad to have this opportunity to discuss these issues with your subcommittee.

The Department has responsibility for the investigation and prosecution of a wide range of cybercrime cases. But large-scale breaches are of significant concern to us because their effects can be amplified exponentially when criminals use the internet to quickly and widely distribute vast quantities of information stolen during these breaches.

The threat we face is wide and it is varied, ranging from very sophisticated individual hackers to international criminal organizations. The resulting losses, as you know, can be devastating and the criminals perpetrating these acts may be motivated by any number of factors, including personal financial gain and the desire to use this illegal activity to fund and facilitate other dangerous crimes.

The Department's benchmark prosecutions of large-scale data breaches and the criminal activity that results from such breaches highlight the range of our efforts that we have been using to address the growing problem. I want to give you a couple of examples. Most recently, the FBI announced the results of a 2-year undercover operation that targeted members of the on-line carding forum known as Dark Market. At its peak, the Dark Market Web site had over 2,500 registered members around the world. This operation has resulted in 60 arrests worldwide and it has prevented what we estimate to be approximately $70 million in economic loss.

In another example, in August 2008, the Department announced the largest hacking and identity theft case ever prosecuted, in which charges were brought against 11 members of an international hacking ring. Now, these various defendants who were from the United States, Estonia, the Ukraine, Peoples Republic of China, Belarus, were charged with, among other things, the theft and sale of more than 40 million credit and debit card numbers obtained from various retailers.

Another example, in 2004 the U.S. Secret Service and several components of the Justice Department coordinated the search and arrest of more than 28 members of the Shadow Crew, a criminal organization located in eight States in the United States and six foreign countries. Members of the group were later charged in a 62-count indictment with trafficking in at least 1.5 million stolen credit and bank card numbers that resulted in losses in excess of $4 million. The Shadow Crew Web site was disabled, which we believe prevented hundreds of millions of dollars in additional losses to the credit card industry. This was known as Operation Firewall, and this early effort paved the way for our more recent successes in this area.

Now, while investigation and prosecution are important, prevention and detection are key elements in the fight against this criminal activity. Keeping credit, debit, and other financial account information out of the hands of criminals in the first place is an essential step in reducing the frequency and minimizing the impact of large-scale data compromises. We suggest that all entities that store, process, or transmit credit, debit, and other financial account information should take steps, including complying with the payment card industry data security standards, to improve the secu-

rity of their computer systems and to decrease the vulnerability of the information they handle.

Of course, even 100 percent compliance with the PCI DSS, if that were achieved, it is likely that hackers will continue to develop techniques to exploit the computer system of companies holding cardholder data. For instance, in those instances where the hackers have succeeded, efforts by the Department and efforts by investigative agencies to look into and prosecute and punish those hackers and carders have been critical to deterring future criminals.

For us to have continued success on this front, it is imperative that, No. 1, victim companies embrace new measures to swiftly detect data breaches and system compromises. No. 2, that the victim companies immediately and consistently report detected data breaches to law enforcement. Finally, that the United States builds on its existing relationships with our international partners to strengthen law enforcement cooperation channels internationally. Thank you.

Ms. Chairwoman, I am prepared to answer your questions.

Ms. CLARKE. I thank you for your testimony.

[The statement of Ms. Glavin follows:]

PREPARED STATEMENT OF RITA M. GLAVIN

MARCH 31, 2009

Good morning, Chairwoman Clarke and Ranking Member Lungren. Thank you for your invitation to address the committee. The Department of Justice welcomes this opportunity to testify about our commitment to combating large-scale data breaches and the payment card fraud that results from such breaches.

As you know, identity theft is not a new problem. However, in recent years, the information age has transformed the landscape in which criminals operate, making available a wide array of new methods that identity thieves can use to access and exploit the personal information of others. Criminals have capitalized on these new and far-ranging opportunities. Skilled hackers are now capable of perpetrating large-scale data breaches that leave hundreds of thousands—and in many cases, tens of millions—of individuals at risk of identity theft. Today's criminals now have the opportunity to remotely access the computer systems of Government agencies, universities, merchants, financial institutions, credit card companies, and data processors, to steal large volumes of personal information, including individuals' financial information, made available simply by virtue of everyday acts like making credit and debit card retail transactions. Reflecting this trend, there are currently over 2,000 active cases related to identity theft pending in the U.S. Attorney's Offices (USAOs), and there has been a 138.2% increase in identity theft convictions by USAOs between fiscal year 2004 and fiscal year 2008. The Department of Justice, through its Criminal Division, the Federal Bureau of Investigation (FBI), the USAOs, and other components, along with our partners at the U.S. Secret Service (USSS) and the U.S. Postal Inspection Service, has been aggressively investigating and prosecuting these data breaches and other criminal activity associated with them, and we are committed to continuing our efforts. Historically, the Department has had tremendous success in identifying, investigating, and prosecuting the perpetrators of these acts. But as always, we can and will do more. To that end, the continued and improved coordination with our partners in the international community and the private sector will be critical to ensuring our success, and we are glad to have this opportunity to discuss these issues in particular with you.

THE "CARDER" THREAT

The Department has responsibility for the investigation and prosecution of a wide range of cyber crime cases, but large-scale breaches are of significant concern to us because their fallout can be amplified exponentially when criminals harness the power of the internet to quickly and widely distribute for future fraudulent use the vast quantities of information stolen during these breaches. For example, international organized crime is currently one of the fastest-growing threats in the computer intrusion arena, and these groups—who are continuing to expand and become

more sophisticated—along with hosts of other cyber criminals, have made large-scale data breaches one powerful part of their profile.

Through activity known as "carding," large volumes of data are stolen, resold, and ultimately used by criminals to commit fraud. In recent years, the problem of "carding" has grown. "Carding" means not only the unauthorized use of credit and debit card account information to fraudulently purchase goods and services, but also a growing assortment of related activities including computer hacking, phishing, cashing out stolen account numbers, re-shipping schemes, and internet auction fraud. I will describe some of these schemes in more detail in a moment.

The internet provides a unique venue in which "carders" can advertise and sell stolen data to the highest bidder and self-organize to facilitate their activities. For example, carders often become members of Web site forums designed to provide an active marketplace for the sale of, among other contraband, stolen credit and debit card numbers; compromised personally-identifiable information, including an individual's address, phone number, social security number, personal identification numbers (PINs), credit history report, and mother's maiden name; and false identification documents.

Once stolen identity information is sold, the purchasers frequently engage in fraudulent activity including, among other things, the use of stolen credit card information to make purchases on-line and in person, and "cashing," which refers to the act of obtaining money—rather than retail goods and services—with the unauthorized use of stolen financial information. In recent years, criminal carding organizations engaged in what is known as "PIN cashing" have developed sophisticated "cash-out networks" in which stolen financial information is immediately disseminated to designated groups of criminals who withdraw money from ATMs all over the world within a short time period. In one example, PIN cashers made 9,000 withdrawals worldwide totaling $5 million in less than 48 hours from four compromised prepaid debit card accounts.

THE LINK BETWEEN CARDING AND OTHER CRIMES

In addition to the financial fraud perpetrated by carders, the Department focuses on criminals who engage in carding activities with a motivation other than personal financial gain. We know, for example, that drug traffickers engage in identity theft for the purpose of financing their activities.

Similarly, there is a well-documented connection between identity theft—in particular as it relates to obtaining fraudulent identification documents, but also as it may relate to credit card fraud—and terrorism. As one example, a convicted terrorist in Indonesia, Imam Samudra, wrote about the use of credit card fraud and carding as a means to fund terrorist activities in his 280-page autobiography. Samudra sought to fund the 2002 Bali nightclub bombings, of which he was convicted, in part through on-line credit card fraud.

Also illustrative of the connection between terrorism and credit card fraud, three British men were convicted in 2007 of inciting terrorist murder via the internet under the United Kingdom's Terrorism Act of 2000. Younes Tsouli, Waseem Mughal, and Tariq Al-Daour were participants in a network of extremist Web sites and communication forums through which al Qaeda statements were issued and which disseminated videos of beheadings, suicide bombings in Iraq, and other jihadi propaganda. The three men also pleaded guilty to conspiracy to defraud banks and credit card companies. Tsouli was sentenced to 16 years in prison, Mughal was sentenced to 12 years in prison, and Al Daour was sentenced to 10 years in prison. Al-Daour and his associates used stolen credit card numbers obtained through phishing scams to make more than $3.5 million in fraudulent charges in order to purchase equipment, prepaid cell phones, airline tickets, and other items, to support jihadi groups in the field. Tsouli and Mughal also used stolen credit card numbers to set up and host jihadi Web sites. Significantly, the investigation revealed that these individuals were members of carding organizations.

THE DEPARTMENT'S INVESTIGATIONS AND PROSECUTIONS

The Department of Justice plays a critical role in combating payment card breaches and the fraud and other criminal activity that results. United States Attorney's offices throughout the country actively prosecute these cases. Within the Criminal Division, the Computer Crime and Intellectual Property Section (CCIPS) also investigates and prosecutes large-scale data breaches and coordinates prosecutions that involve multiple USAOs and foreign countries. In addition, the Fraud Section of the Criminal Division recently established the Payments Fraud Working Group (PFWG), which it co-chairs with the Board of Governors of the Federal Reserve System. The PFWG is an inter-agency cooperative effort between law enforce-

ment and the bank regulatory agencies designed to examine issues related to various payments systems and establish initiatives to protect payments systems against fraud and other misuse. The Department also helped to lead the Identity Theft Task Force, which also addressed many of these issues. Finally, the Office of International Affairs in the Criminal Division supports international cooperation efforts by implementing mutual legal assistance treaties (MLATs) and international conventions that have yielded significant evidence for use in U.S. and foreign prosecutions and by marshaling efforts to extradite international fugitives.

The combined force of all of these efforts, along with the efforts of the FBI and the Department's other law enforcement partners, has resulted in a number of benchmark prosecutions that highlight the range of the Department's efforts to address the growing problem of large-scale data breaches and associated criminal activity.

Recent Successes

The Department, in coordination with its various USAOs, has worked with investigative agencies including the USSS, the FBI, and the United States Postal Inspection Service to combat carding and associated crimes, with great success:

- *Dark Market carding forum*.—Most recently, on October 16, 2008, the FBI announced the results of a 2-year undercover operation, conducted in conjunction with CCIPS, targeting members of the on-line carding forum known as Dark Market. At its peak, the Dark Market Web site had over 2,500 registered members around the world. This operation has resulted in 60 arrests worldwide and prevented an estimated $70 million in economic loss.
- *International hacking ring*.—In August 2008, the Department announced the largest hacking and identity theft case ever prosecuted, in which charges were brought by the USAOs in the District of Massachusetts, the Southern District of California, and the Eastern District of New York against 11 members of an international hacking ring, including Maksik, discussed later. The various defendants—who were from the United States, Estonia, Ukraine, the People's Republic of China, and Belarus—were charged with, among other things, the theft and sale of more than 40 million credit and debit card numbers obtained from various retailers including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21, Dave & Buster's, and DSW.
- *Operation CardKeeper*.—Operation CardKeeper, led by the FBI and the USAO for the Eastern District of Virginia, resulted in the arrests of 13 individuals in Poland and eight in the United States. International cooperation was required to execute search warrants in the United States and in Romania. Significantly, Operation CardKeeper resulted in the U.S. conviction of an individual known on-line as "John Dillinger." This defendant was sentenced in 2007 to 94 months in Federal prison for his carding activity, including aggravated identity theft, access device fraud, and conspiracy to commit bank fraud. Computers seized from him revealed more than 4,300 compromised account numbers and full identity information for over 1,600 individual victims.
- *"Iceman"*.—In late 2007, a major supplier of tens of thousands of credit card accounts to carding forums was indicted for wire fraud and identity fraud; he is currently awaiting trial. Max Ray Butler, known on-line as "Iceman," was the co-founder and administrator of the carding forum Cardersmarket. This case is being prosecuted by the United States Attorney's Office for the Western District of Pennsylvania.
- *"Maksik" and "Lord Kaisersose"*.—Maksym Yastremskiy, known on-line as "Maksik," believed to be one of the top traffickers in stolen account information, was arrested for his carding activity in Turkey in 2007. He was also indicted in several U.S. districts as the result of the Department's prosecution of the international hacking ring I discussed earlier. Maksik allegedly sold hundreds of thousands of credit and debit card numbers. One of his customers, an infamous carder known on-line as "Lord Kaisersose," was previously searched and arrested in France as the result of a joint investigation conducted by the USSS and the French National Police. He is currently awaiting sentencing.

"Operation Firewall"

Much of this successful investigative work has its roots in some of the Department's early efforts to dismantle highly-organized carding enterprises. As just one example, in 2004, as part of an undercover investigation known as Operation Firewall, the U.S. Secret Service (USSS) and several components of the Department of Justice coordinated the search and arrest of more than 28 members of the "Shadowcrew" criminal organization, located in eight States in the United States

and six foreign countries. Members of the group were later charged in a 62-count indictment with trafficking in at least 1.5 million stolen credit and bank card numbers that resulted in losses in excess of $4 million. As part of this takedown, the USSS disabled the Shadowcrew Web site. We believe that had the organization not been interrupted, the credit card industry could have faced hundreds of millions of dollars in additional losses. Instead, the Shadowcrew criminal organization's activity stopped, and to date, with the exception of two fugitives, all of the domestic Shadowcrew defendants have pleaded guilty and received sentences of up to 90 months in prison. This prosecution was the first of its kind—by prosecuting top-tier members of the organization for conspiracy, it held individuals responsible for the criminal offenses facilitated through the carding forum by virtue of their leadership role in a criminal organization that operated solely on-line. Operation Firewall enabled many of our more recent successes. In addition, the investigation into the Shadowcrew organization also revealed that the defendants were conspiring internationally to commit specific carding-related crimes, including bank fraud, and enabled us to successfully prosecute individuals for that conduct separately.

Operation Firewall, like many of the examples I have mentioned today, also illustrates how we can effectively respond to the increasingly global nature of carding organizations. With the cooperation of law enforcement agencies in the United Kingdom, Canada, Bulgaria, Belarus, Poland, Sweden, the Netherlands, and Ukraine, foreign searches and arrests went smoothly, and foreign individuals were successfully indicted in the United States. In addition, the United Kingdom pursued a separate domestic prosecution of Shadowcrew members, which has led to a number of guilty pleas.

PREVENTION, DETECTION, AND RESPONSE

Keeping credit, debit, and other financial account information out of the hands of criminals in the first place is an essential first step in reducing the frequency, and minimizing the impact, of large-scale data compromises. Merchants and processors who hold individuals' sensitive financial information are prime targets for hackers and carders. To address this vulnerability, the credit card associations developed a set of security standards, known as the Payment Card Industry Data Security Standards (PCI DSS), for merchants and third-party processors. We suggest that all entities that store, process, or transmit credit, debit, and other financial account information should ensure that they comply with all requirements of the PCI DSS in order to improve the security of their computer systems.

As is well understood throughout the security community, however, perfect security is impossible. Therefore, even if 100% compliance with PCI DSS were achieved, it is likely that hackers will continue to develop techniques to exploit the computer systems of companies holding cardholder data. For instances in which those hackers succeed, efforts by the Department and investigative agencies to investigate, prosecute, and punish hackers and carders are critical to deterring future carders, learning more about the nature of these crimes, and punishing offenders. For continued success on these fronts, it is imperative that: (1) Victim companies embrace measures to swiftly detect data breaches and system compromises; (2) victim companies report data breaches to law enforcement; and (3) the United States builds upon its existing relationships with international partners to strengthen law enforcement cooperation channels internationally.

Early Detection

Early detection plays two important roles in efforts to combat carding activity. First, it can assist in mitigation of potential damage. When victim companies are notified by law enforcement, credit card companies, or other entities about a potential compromise to their system, they should take all reasonable measures to determine whether a compromise did indeed occur. Successful detection empowers victim companies to take steps to address the vulnerability, fortify their systems, and notify individual victims as necessary. But to date, it has been our experience that following notification, victim companies can not and do not always do enough to determine the scope and severity of data breaches of their computer networks.

Moreover, law enforcement faces continued investigative challenges as a result of delayed detection and response. Often, victim companies detect compromises to their system weeks, months, or years after they occur, and as a result, meaningful investigative leads may have disappeared by the time the compromise is reported to law enforcement, if it is reported at all. Private entities must have the capabilities to identify compromises more quickly. To accomplish this, we recommend that all entities that store, process, or transmit credit, debit, and other financial account information implement security mechanisms designed to detect system breaches, such as tracking and monitoring all access to network resources and cardholder data.

Breach Reporting

Immediate reporting of incidents to law enforcement is also vital to law enforcement's ability to investigate large-scale data breaches. Immediate reporting necessarily relies upon each potential victim company's capacity to promptly detect an incident, but we know from experience that prompt detection will not itself result in a report from the victim company. For a variety of reasons, data breaches are significantly underreported, and as a result, law enforcement efforts to bring criminals to justice are significantly hampered. If law enforcement never learns of the incident, we will not investigate it; if we hear about it too late, we may be unable to preserve critical evidence or identify the perpetrators. On the other hand, several recent successes in tracking down the perpetrators of high-profile data breaches are the direct result of immediate information from victim companies on how the hackers entered and exited their systems, including the specific IP addresses used in the attack. For example, in the Dave & Busters case, which was a part of the international hacking ring prosecuted in 2008, when Dave & Busters became aware of intrusions, they took measures to log access to their computers, block the intruder's further attempts to collect credit and debit card data, and identify for law enforcement the intruder's IP address.

While companies like VISA require by policy that all entities that suspect or have confirmed that a security breach occurred must contact Federal law enforcement, few laws require the victim company to notify law enforcement. In its April 2007 Strategic Plan, the Identity Theft Task Force recommended the establishment of a national standard requiring entities that maintain sensitive data to provide timely notice to law enforcement in the event of a breach. Because only a handful of State laws currently require reporting to law enforcement and because private sector rules are neither universal nor consistently enforced across the various companies, we urge Congress to consider requiring security breach reports to Federal law enforcement using a mechanism that ensures that the USSS and FBI have access to the reports.

International Law Enforcement Cooperation

As illustrated by the array of cases I have mentioned, carders operating in carding forums on the internet reside in different countries, collaborate freely across borders, and can immediately and widely distribute stolen identity information around the globe. In addition, on-line carding forums provide networking opportunities for criminals interested in joining together to perpetrate other financial fraud or criminal activity on a global scale. As a result, coordination and cooperation from foreign law enforcement is vital to the success of carding investigations and prosecutions. In this regard, the Identity Theft Task Force's Strategic Plan also recommended that the Department of Justice and other departments and agencies take specific steps to improve coordination and evidence sharing with foreign law enforcement agencies.

We believe that on this front, the United States should continue to press other nations to accede to the Convention on Cybercrime (2001), which will improve cooperation between law enforcement agencies. The Convention, which the United States ratified in 2006, assures that other countries enact suitable domestic legislation criminalizing identity theft, in part to facilitate information-sharing under MLATs and the extradition of criminal defendants. In addition, the United States should continue to work closely with multilateral organizations to urge other countries to review their criminal codes and criminalize identity-related criminal activities where appropriate. This has historically proven effective. Last month, for example, the G–8 Roma/Lyon Group approved for further dissemination a paper that examines the criminal misuse of identification information and identification documents within the G–8 States and proposes "essential elements" of criminal legislation to address identity-related crime. The Identity Theft Task Force's Strategic Plan also directs the U.S. Government to identify countries that are safe havens for identity thieves and to use appropriate diplomatic and enforcement mechanisms to encourage those countries to change their practices. The Department of Justice has begun this process, gathering information from a range of law enforcement authorities. Finally, only by assisting foreign authorities can we expect them to reciprocate with critical evidence for our own investigations. The United States can improve international cooperation, in certain cases, by ensuring that our legislation provides U.S. authorities with the tools to assist foreign investigations effectively.

CONCLUSION

As I have attempted to outline for the subcommittee, the Department has been at the forefront of groundbreaking and historic efforts to identify, prosecute, and

punish the perpetrators of large-scale data breaches and the associated identity theft and fraud following from those breaches. In light of the growing sophistication and global scope of the threat, we are committed to continuing and improving our efforts to address this conduct. Thank you for the opportunity to provide the subcommittee with a brief overview of the Department's role in combating these crimes and the primary issues we must focus on as we press ahead.

Madam Chairwoman, this concludes my remarks. I would be pleased to answer any questions that you or other Members of the subcommittee may have.

Ms. CLARKE. I will remind each Member that he or she will have 5 minutes to question the panel. I will now recognize myself for questions.

Are we seeing more massive data breaches today, or is the media simply reporting more?

Ms. GLAVIN. I think you have a little bit of both. The media is reporting on it, but what we have seen over the last several years and in some of the operations specifically I have referred to in our testimony, including the Shadow Crew organization, is hundreds of thousands, if not millions, of personal financial information and identity thefts occurring.

The Operation Firewall, which was both the Shadow Crew organization and the Carder Market Forum, should demonstrate that for a number of years this type of data breach has been happening and that there are hackers all over the world that are looking to get into systems and slowly take the information out. It can be over a course of months, if not over a course of years.

So, yes, the data breaches are occurring and we know that because of undercover operations we have done and because of the publicly reported takedowns that we have done that I mentioned in my testimony. Yes, the media is reporting on those breaches.

Ms. CLARKE. Ms. Glavin, to what extent does the fact that a company is PCI-compliant help to mitigate criminal activity? How effective are PCI standards in lowering the risk of being breached?

Ms. GLAVIN. Having any security system and uniform standards are going to help, all right? It is a floor, and it is a way to begin the process of preventing breaches. That said, what we look at in terms of those PCI set standards is you have got to do continual monitoring and you have to do the testing, because you may have adopted those standards, but people may already be in your computer system by the time you have adopted those standards. It is the monitoring and the testing that is going to help companies see where they have been breached. We know that hackers are always coming up with new ways to get into your system. So it is going to be the monitoring and the testing.

The second thing that the Department would suggest is that there should be notification through Federal law enforcement when breaches occur. I know is that something that has been under subject of much discussion. But that would be an effective way of dealing with the data breaches on a number of levels, because we have a sense from our investigations and prosecutions around the country as to the means that the hackers used to do this. If we get early reporting, it helps us get a sense of what is going on such that we can stop it. We can stamp out, you know, Web sites that are doing this and help get in front of the problem.

Ms. CLARKE. Ms. Glavin, how successful do you think that the Department of Justice's efforts to combat credit card fraud will be

in the long run if neither improved standards nor technology and infrastructure changes are realized and there is no reduction in the amount of cardholder data being lost or stolen?

Ms. GLAVIN. This is going to have to be an on-going partnership. Law enforcement has been there and we are always going to be there. It is not just within the prosecution of the Department of Justice. The FBI is always looking at this. The Secret Service is always looking at this. We are working with our international partners around the world to have an international presence such that we are sharing information. We can't do that alone, and having help from private industry when they know there have been breaches and reporting that to us, it is going to help everybody in the long run.

So we can do what we do in terms of watching the technology, trying to stay on top of the hackers, continually looking out for these Web sites and carding forums. But we can't do everything alone. To the extent we get help from the private sector to stay on top of that, that is important. I think that the industry that has adopted the PCI DDS, that is a laudable effort. The question is: Can they continue to evolve from there?

Ms. CLARKE. Just finally, can you please explain the roles of the Secret Service, FBI, and ICE in investigating cybercrime, and what are the distinctions between those investigative units?

Ms. GLAVIN. Sure. The Secret Service has always been involved in looking at financial crimes and hackers. What the FBI brings to the table in addition to the Secret Service is that they have your counter-intelligence databases, which the Secret Service may not have. So they can be also checking, on a much more international level, what is going on around the world. They also have a presence through their legal attaches in other countries. So the Secret Service and the FBI both play critical roles and they both bring different tools to the law enforcement effort.

Ms. CLARKE. Well, thank you very much. I now recognize one of our new Members on the committee, new Member to the Congress, the gentleman from New Mexico, Mr. Luján, for his questions at this time.

Mr. LUJÁN. Thank you very much, Madam Chairwoman. Ms. Glavin, thank you very much for being with us today.

Ms. GLAVIN. Thank you.

Mr. LUJÁN. In your testimony you highlight many instances where there are projects or programs, recent success, investigations that the Department of Justice has engaged in, Dark Market carding forum, international hacking ring, Operation Card Keeper, Iceman, Operation Firewall.

With that being said and with the level of concern that the Department of Justice has with the level of crime that is taking place, in this case cybercrime, what standards exist today for keeping this data secure?

Ms. GLAVIN. In terms of private industry, the standards that are out there are the PCI DSS, plus whatever State laws there are. I mean, a number of States have consumer notification laws that require financial entities to report data breaches. Some have law enforcement notification laws.

In terms of Federal regulation, there is not a lot, other than you are speaking to someone from the Criminal Division, and I know we have the Title 18 criminal statutes that we use to prosecute. But in terms of standards across the industry Federally, such that people are required by law to comply with a certain set of standards, that is not out there.

Mr. LUJÁN. So it sounds like what States have done, they have a reporting mechanism that when there is a breach in security and data is compromised, that they are required to notify the consumer that may have been impacted. But with that being said, in your opinion, are these standards working the way they are being put together today?

Ms. GLAVIN. Which industries?

Mr. LUJÁN. The industry standards.

Ms. GLAVIN. In terms of whether or not they are working, we know what reports we get when there has been data breaches and when industry chooses to tell us; or sometimes we learn about it from our own investigations and we choose to tell them. Whether or not they are working, I think the industry representatives are in the best position to tell you that.

What I can say from the Department's perspective is that if we are going to do criminal investigations, there is going to have to be some cooperation between us and private industry so we can do those investigations, get a sense of the data breaches and to have cooperation such that they let us know what is going on.

We have a sense of how it happened, what is out there, and who may be responsible. As for whether or not they are working, I think they are a great bottom line to start with. But you have to be constantly watching, testing them, checking them to make sure they work, because the hackers are sophisticated people and they try to stay one step ahead of the industry. The industry tries to get one step ahead of them, and it is in everyone's interest that you keep moving ahead.

Mr. LUJÁN. Ms. Glavin, did I hear you correctly? Did you say that sometimes the Department of Justice will notify the companies that there has been a breach, as opposed to the other way?

Ms. GLAVIN. Yes. But sometimes that can happen—you know, if we get information that they may not have, that we may have access to through the course of our criminal investigations. It could be a company that may be PCI-compliant, but there was always something in the system before they got brought up to compliance.

But, yes, there have been instances that I know of, investigations where we have learned about information and that we have informed the company about, that you may want to check X, Y, and Z.

Mr. LUJÁN. Thank you very much, Ms. Glavin.

Madam Chairwoman, I know we had a lot of briefings and discussions with the committee as a whole and the various subcommittees on the importance and attention that is needed when it comes to data breaches, especially with the attacks that we know that are occurring on a regular basis, national security, as well as financial institutions.

I think that in the same regard, when we are talking about what the expectations are of the American public with feeling secure

about the data that could exploit them and expose them to these types of crime, often times without them ever knowing, is something that we have to take seriously.

So I thank you very much, Madam Chairwoman and Chairman Thompson, for bringing this to the attention and allowing us to have a hearing on this today.

Ms. CLARKE. Thank you very much, my colleague. I just want to correct the record, at least vocally, that my colleague's name is Mr. Luján.

Mr. LUJÁN. Thank you very much.

Ms. CLARKE. Very well. Some of your responses to my colleague's questions were a bit troubling to me. The fact that it could take some time before there is communication around a vulnerability that is existing within the system, and in that amount of time transactions can take place that can lead to financial support for criminal endeavors is something we should always be concerned about. Time is of the essence, right? If you are not getting the level of transparency, for whatever reasons, from the private side—in other words, maybe someone is ashamed that they met these PCI standards and now they have found a vulnerability. As you said, it couldn't have been one that existed there prior to them coming up to code. It is still important for that information to be shared, notwithstanding whatever reasons may inhibit someone from doing so. Because, again, these transactions take place so quickly.

What would you say could expedite the transfers of information? What do you think would open up private enterprise to really working with law enforcement on a much more timely basis, once something is detected, to address it? Do you think that perhaps some introspection about the PCI standards would help put them on a higher platform for detection?

Ms. GLAVIN. The PCI DSS standards—again, as I said before, I think one of the key components of those standards is going to be the regularly monitoring and testing. Sometimes these breaches aren't readily apparent and are hard to detect.

As I have had it described to me, the breaches can sometimes occur such that the best analogy could be that the front door of your house gets open and you don't know it. Slowly over a period of time, someone may take, piece by piece, all of your house. It could happen over a course of months, and an entity may not be aware of it.

So immediate notification could be hard in that type of instance. But regularly monitoring and testing, we hope, would be a way that they detect it sooner.

In terms of the information sharing, we support an effort such that there be some type of notification to Federal law enforcement. How that is done and what particular entity that is reported to is something that we are happy to work with this committee on, such that it can happen faster and it gets to the law enforcement entities that have been in the forefront of this, such as the FBI and the Secret Service. But it is immediate notification when you see the data breach. Yes, that is something that we would like. But sometimes it is not always easy that you are going to find that data breach right away.

Ms. CLARKE. Ms. Glavin, I want to thank you for sharing with us your perspective on the PCI standards and the payment card industry and its relationship to cybercrime. I want to thank you for sharing your expertise with us. We look forward to working with you further as we look for ways to strengthen this part of our concern with regards to the threats that exist, the vulnerabilities that may exist within the payment card industry. Thank you very much.

Ms. GLAVIN. Chairwoman Clarke, thank you very much. We look forward to working with you.

Ms. CLARKE. Thank you. I would like to acknowledge the work, Ms. Glavin, of your senior counsel, Kim——

Ms. GLAVIN. Kim Paretti.

Ms. CLARKE [continuing]. Kim Paretti in this field, and I would like to thank her and her colleagues for their service.

Ms. GLAVIN. They have done excellent work.

Ms. CLARKE. We appreciate it.

The Members of the subcommittee may have additional questions for the witness and we will ask you all to respond in writing to those questions.

At this time, the first panel is dismissed and the Chairwoman calls out the next panel.

I welcome the second panel of witnesses. Our first witness is Robert Russo, Director of the Payment Card Industry Data Security Standards Council. Welcome.

Our second witness is Joseph Majka, Head of Fraud Control and Investigation, Global Enterprise Risk for Visa.

Our third witness is Michael Jones, Chief Information Officer for Michaels Stores.

Our fourth witness is Dave Hogan, Senior Vice President and Chief Information Officer for the National Retail Federation. I thank you all for being here today.

Without objection, the witnesses' full statements of Andrew Cochran, an expert on terrorism financing, and Kirsten Trusko on behalf of the Network Branded Prepaid Card Association will be inserted into the record. Hearing no objection, so ordered.

[The information follows:]

STATEMENT FOR THE RECORD SUBMITTED BY ANDREW R. COCHRAN, FOUNDER AND CO-EDITOR, THE COUNTERTERRORISM BLOG

MARCH 31, 2009

Chairwoman Clarke, Ranking Member Lungren, and Members of the committee, I appreciate the opportunity to submit a written statement on the subject of terrorists' use of credit cards for this important hearing. I am the founder and co-editor of The Counterterrorism Blog, the first multi-expert internet-based center dedicated solely to reporting and analyzing terrorist attacks and counter-terrorism policies. Now in its fifth year of operation, The Counterterrorism Blog is a highly respected source of objective information and analysis in the counter-terrorism community. Our Contributing Experts work in non-governmental organizations and private businesses worldwide, and include over 20 noted experts, including Evan Kohlmann, Douglas Farah, Dennis Lornel, Walid Phares, Animesh Roul, Farhana Ali, and Matthew Levitt. In addition to earning the plaudits of law enforcement, intelligence officials, Members of Congress, and the news media, our credibility is evidenced by the fact that al Qaeda attacked us by name on Al-Ekhlaas, one of its central messaging

forums, last April.[1] You can find us on the internet at *http://counterterrorismblog.org/,* and you can e-mail me.

Our Contributing Experts have reported often on terrorists' use of stolen credit card information, and they speak often about the subject. On February 29, 2008, I chaired a special panel, "Meta-Terror: Terrorism and the Virtual World," with two Contributing Experts (Evan Kohlmann and Roderick Jones) and the senior vice president and chief technology officer of VeriSign.[2] During that event, our discussion included how a senior al Qaeda operative financed operations through the use of stolen credit card information. Dennis Lormel, who founded and ran the Terrorist Financing Operations Section at the FBI and investigated the financing of the 9/11 attacks, has several posts on terrorists' use of credit cards.[3] Matthew Levitt and Contributing Expert Michael Jacobson cited the use of credit card fraud to finance two deadly attacks in a *New Republic* article this year.[4] I invite the committee to review the cited works in detail, and I will quote from and/or summarize their main points for the committee's consideration as follows:

1. Credit cards are extremely vulnerable to fraud and are used extensively by terrorists. The internet not only serves as a learning tool for terrorists but also functions as a mechanism to steal credit card information through hacking, phishing, and other means. In many instances, when terrorist operatives are apprehended, they have multiple identifications and credit cards in a variety of names in their possession.
2. The terrorists who executed the devastating 2004 Madrid train bombings, which killed almost 200 people, and who carried out the deadly July 7, 2005, attacks on the transportation system in London were self-financed, in part through credit card fraud.
3. Imam Samudra was a key operative of the al Qaeda-linked terrorist group Jamaah Islamiah in Indonesia, and was the mastermind behind the Bali nightclub bombings in 2002 which killed over 200 people. While in prison in 2004, he wrote a jailhouse manifesto, with a chapter, entitled "Hacking, Why Not." In it, he urged fellow Muslim radicals to take holy war into cyberspace by attacking U.S. computers. Samudra described America's computer network as being vulnerable to hacking, credit card fraud, and money laundering. Samudra discussed the process of scanning for Web sites vulnerable to hacking and then discussed the basics of on-line credit card fraud and money laundering. Interestingly, in 2004, Indonesian police asserted that Indonesia had more on-line credit card fraud than any country in the world.
4. Younes Tsouli, aka "Terrorist 007," and his two associates, Waseem Mughal and Tariq al-Daour, used computer viruses and stolen credit card accounts to set up a network of communication forums and Web sites that hosted everything from tutorials on computer hacking and bomb making to videos of beheadings and suicide bombing attacks in Iraq. They raised funds through credit card information theft and fraud, which were used to support the communications, propaganda, and recruitment for terrorists worldwide, as well as to purchase equipment for Jihadists in the field. One expert described their activities as "operating an on-line dating service for al Qaeda." The three men pled guilty to inciting terrorist murder via the internet.

Set forth below is a snapshot of the extent of credit card information theft and fraud they were responsible for:

- Stolen credit card numbers and identities were used to buy Web hosting services. At least 72 stolen credit card accounts were used to register more than 180 Web site domains at 95 different Web hosting companies in the United States and Europe.
- On one computer seized from al-Daour's apartment, some 37,000 stolen credit card numbers were found. Alongside each credit card record was other information on the identity theft victims, such as the account holder's address, date of birth, credit balances, and limits.
- More than $3.5 million in fraudulent charges were made using credit card accounts stolen via on-line phishing scams and the distribution of "Trojan horses."

---

[1] "Al Qaeda Officially Hates The Counterterrorism Blog," April 16, 2008, at *http://counterterrorismblog.org/2008/04/al_qaeda_officially_hates_the.php.*

[2] Complete transcript at *http://counterterrorismblog.org/2008/03/event_transcript_and_related_l.php.*

[3] "Terrorists and Credit Card Fraud . . . a Quiet Epidemic," February 29, 2009, at *http://counterterrorismblog.org/2008/02/terrorists_and_credit_card_fra.php,* and "Credit Cards and Terrorists," January 16, 2008, at *http://counterterrorismblog.org/2008/01/credit_cards_and_terrorists.php.*

[4] Summarized in "Drug Wars," Michael Jacobson, January 27, 2009, at *http://counterterrorismblog.org/2009/01/drug_wars.php.*

- The men purchased sophisticated equipment needed by jihadists in the field and other operational resources, including hundreds of prepaid cell phones, and more than 250 airline tickets using 110 different credit cards at 46 airlines and travel agencies.
- They laundered money through on-line gambling sites, using accounts set up with stolen credit card numbers and victims' identities. The trio conducted 350 transactions at 43 different on-line wagering sites, using more than 130 compromised credit card accounts.

The terrorists apparently obtained some stolen data through contacts with Russian-based criminal gangs, and they traded this information with criminal syndicates. In the 1990's, al Qaeda would steal a handbag to get one credit card to raise funds. Now they will just buy this data on-line and get thousands of credit card details. Once credit card information winds up in the hands of criminal syndicates, it can be easily transmitted to terrorists.

5. The Liberation Tigers of Tamil Eelam (LTTE), a.k.a. the "Tamil Tigers," use credit card fraud as an international means of financing terrorist activities. Four men, believed to be associated with the Tigers, were arrested this year in Toronto on charges of debit and credit card fraud for possessing numerous gift cards containing bank account and debit information from individuals in the United Kingdom. Further investigation found laptop computers and memory sticks containing bank information for thousands of U.K. bank customers. A massive credit and debit card fraud case in the United Kingdom, involving up to 200 British gasoline stations, is apparently another Tamil Tigers operation. The alleged subjects obtained credit and debit card information at gasoline pumps through the use of skimming machines, with the loss was estimated to be as much as $72,000,000.

I look forward to reviewing the committee's review into the effectiveness of the PCI standards to reduce data breaches, identity theft, and the potential funding of terrorism, and I stand ready to assist the committee in that mission.

STATEMENT FOR THE RECORD SUBMITTED BY KIRSTEN TRUSKO, ON BEHALF OF THE NETWORK BRANDED PREPAID CARD ASSOCIATION

MARCH 31, 2009

Chairwoman Clarke and Members of the subcommittee, I am Kirsten Trusko, President and Executive Director of the Network Branded Prepaid Card Association ("NBPCA" or Association"). We are a non-profit trade organization, which seeks to serve consumers, businesses, and Government through unique applications of network branded prepaid cards, and in doing so supports the growth and success of network branded prepaid cards. We represent the common interests of the many players in this new and rapidly growing payment category. The NBPCA's members include banks and financial institutions, the major card networks, processors, program managers, marketing and incentive companies, card distributors and law firms. For additional information about our organization, may we suggest you visit our Web site, *www.NBPCA.com.* I am delighted to submit factual information that we hope will help to address your questions on a topic that is of utmost importance to our members: accurately understanding and mitigating the potential risks posed by network branded prepaid cards.

This document is designed to outline the following topics, at a high level. Should you have follow-up questions, please let us know.

1. What is a network branded prepaid card and how does it differ from other cards?
2. Why is this card type growing and popular (including quotes from the Federal Reserve and Office of the Comptroller)?
3. What are the facts to correct misperceptions about network branded prepaid cards?
4. How are NBPCA's members working with legislators, regulators, and law enforcement to mitigate the potential for misuse of the cards?

I. WHAT ARE "NETWORK BRANDED PREPAID CARDS"?

We hope to clarify some misconceptions by being clear about the facts.

- First, there are many types of plastic, magnetic-striped cards that are all called "prepaid." That is, before one uses the card to make a purchase, one must prepay the funds, which are held by a bank. The cardholder uses the cards to gain access to the funds. You cannot spend a $50 gift card, for example, until the $50 has been paid in advance.

- However, not all prepaid cards are "network branded." Network branded cards (sometimes referred to as "open loop" or "open system" cards) are issued by regulated financial institutions, carry the brand of a major card network (such as American Express, Discover, MasterCard or Visa) on the front of the card, and are generally[1] usable anywhere that brand is accepted. Some network branded prepaid cards are also usable at ATMs to obtain cash for limited daily amounts.
- Although many network branded prepaid cards display the word "DEBIT" on the front of the card, they are not "debit cards" in the classic sense of the word. That is, network branded prepaid cards are not linked to an individual's personal checking, savings, or other bank account. Instead, the funds are held in pooled bank accounts with data that links each card to the cardholder's funds. This distinction enables the under-banked population to use these cards to receive child support, unemployment, and other funds that are essential to daily life, transaction that are very difficult to administer on a cash-only basis.
- Network branded prepaid cards are also separate and distinct from "retailer gift cards" (sometimes referred to as "closed loop" cards). Retailer gift cards are not issued by a financial institution and can only be used at one location (or at one chain of affiliated locations). Retailer gift cards are issued by a restaurant, store, hotel, or other retail service provider solely for use to purchase goods or services at the issuing retailer's establishment.
- Attached to this testimony are pictures of some popular network branded prepaid cards issued by our members.*

II. WHY HAVE NETWORK BRANDED PREPAID CARDS BECOME SO POPULAR?

Network branded prepaid cards are a relatively new and growing product, largely developed in response to market needs not being met by other card types. They enable electronification of payments and the supporting data trail, to capture what was previously transacted with check or cash. They support specific applications by customer need (e.g. the under-banked consumer as mentioned earlier) and help to reduce costs and provide a better accounting/data trail for businesses and Government than when using cash or checks.

The popularity of network branded prepaid cards is attributable to their unique ability to address cardholder needs in a variety of situations including health care, disaster relief operations, payroll, Government benefit payments, and gifting.

The benefits that network branded prepaid cards provide was noted in an article published by the Philadelphia Federal Reserve Bank's Payment Card Center:

"The benefits that open-system prepaid cards offer for consumers, providers, and issuing banks contribute to the increased adoption of these payment applications. Consumers use these cards to pay bills, make purchases, and access cash from ATM networks. Prepaid cards can also be used to secure car rentals and to make hotel and air travel reservations. At the same time, holders of prepaid cards need not secure a traditional banking relationship nor gain approval for a deposit account or revolving credit. Prepaid card providers may be nonbank third parties, such as employers and payroll processing companies, that can use prepaid cards as a means to convert paper disbursements, such as payroll checks, benefit claims forms, travel checks, gift certificates, and government checks, to less costly electronic payments. Finally, bank card issuers have an opportunity to serve a broader set of consumers. By offering prepaid cards, issuing banks may meet the financial needs of consumers who may not otherwise qualify for more traditional banking products, and these banks may do so with a card-based electronic payment application that essentially eliminates credit risk for the bank. (Cheney and Rhine, *Prepaid Cards: An Important Innovation in Financial Services,* Philadelphia Federal Reserve Bank Payment Center (Originally published in conjunction with the American Council on Consumer Interests (ACCI) (July 2006))."

Additionally, the Office of the Comptroller of the Currency, in a July 2005 report, (*http://www.occ.treas.gov/cdd/payrollcards.pdf*) compared the cost of network branded prepaid payroll cards versus the alternatives available to the under-banked, noting the following benefits:

Benefits to Employers

- Reduced bank processing fees and check handling fees;

[1] We say "generally" because some network branded prepaid cards have specialized usage which creates some limitations. For example, "teen cards" are designed so that they cannot be used in liquor stores, and health cards may have restrictions to health-only merchants and/or purchases.

* The information referred to has been retained in committee files.

- Reduced check printing costs;
- Reduced likelihood of check fraud;
- Reduced check reconciliation costs;
- Increased employee productivity (e.g., not needing time off during work to cash or deposit paycheck);
- Reduced lost/stolen check replacement costs.

Benefits to Employees

- Reduces or eliminates check cashing fees;
- Offers ability to make purchases using credit card networks;
- Offers 24-hour access to funds via ATMs; no need to wait in lines;
- Reduces the need to carry a lot of cash;
- Makes money transfers more easily available to families;
- Provides a pseudo-bank account—funds do not need to be withdrawn entirely as with using a check casher;
- Please refer to Table 5 in the OCC report as it documents their comparison of consumer costs across Payroll card, Check Casher, and Basic Bank account, reflecting Payroll card as the option least costly to the consumer.

III. MISUNDERSTANDINGS/MYTHS ABOUT NETWORK BRANDED PREPAID CARDS.

Despite the many benefits of network branded prepaid cards, aspects of these products are misunderstood. This may be because organizations not typically associated with financial products are sometimes involved in the creation and distribution of network branded prepaid cards. For example, some network branded prepaid cards are available through non-traditional distribution channels such as supermarkets and drug stores. Misconceptions about network branded prepaid cards, which have gained currency through repetition, have the potential to affect the industry negatively—particularly with respect to issues relating to money laundering risks. My testimony today addresses several major misconceptions by providing factual information that supports a fair and accurate assessment of money laundering risks associated with network branded prepaid cards. Here are some misunderstandings about network branded prepaid cards:

Myth No. 1: Prepaid cards are unregulated or loosely regulated.—Every network branded prepaid card (i.e., those carrying the logo of American Express, Discover, MasterCard, or Visa) is issued by a highly regulated financial institution or other regulated organization. As such, network branded prepaid cards are subject to exam, review, and oversight. For example, the FFIEC BSA/AML Bank Examination Manual (July 2006) sets forth specific requirements for examining banks regarding their "electronic cash" products (which encompasses "stored value") including OFAC screening, transaction testing, and monitoring for suspicious activity. In addition, many prepaid card program managers, distributors, and organizations that perform specific functions relating to processing or distributing network branded prepaid cards, are regulated by State banking departments as money transmitters or check sellers. As such, they also are subject to exam, review, and oversight. State regulators are increasingly requiring money transmitters to:

(1) Register as Mobs with FinCEN,

(2) Have AML policies that address customer due diligence, OFAC screenings, and suspicious activity monitoring, and

(3) Have independent reviews of their AML policies.

Altogether, there are over 50 laws/regulations that apply to network branded prepaid cards. The applicability of these laws/regulations depends on a number of factors including the charter of the financial institution issuer.

Myth No. 2: Prepaid cards are "ideal" for money laundering.—Network branded prepaid cards are actually less useful for money laundering than many other payment products for the following reasons:

- The value associated with network branded prepaid cards issued in the United States consists of funds held in a bank account in the United States. These funds can—at any time—be frozen by the card issuer and/or forfeited entirely. Unlike "bearer instruments" or chip-based cards, where whoever holds the product also holds the value, network branded prepaid cards keep the value separate, making the products less attractive to criminals.
- All network branded prepaid cards are processed through an on-line system that requires electronic authorization from the payment network prior to completing a purchase transaction at the point of sale or obtaining cash from an ATM.
- The system enables card issuers to decline an authorization and/or to cancel the ability to use a prepaid card. The ability of the card issuer to terminate a card's usefulness, without requiring possession of the card, is critical—and is a feature

not shared by most traditional payment products. The on-line system tracks and records every use of every network branded prepaid card. Unlike paper payment products (such as checks, travelers checks, money orders, and cash), network branded prepaid cards leave a traceable trail of use including place, time, date, amount, and often the nature of the transaction. This trail has already assisted law enforcement in tracking illicit activity through use of prepaid cards.

- If a network branded prepaid card issuer identifies unusual or suspicious activity, the card can be blocked from further use. Card programs routinely monitor card activity and, as appropriate, file suspicious activity reports (SARs) or notify law enforcement.

Myth No. 3: Network branded prepaid cards can be both anonymous and permit ATM access, with liberal load limits or no limits on the amount of cash that can be accessed.—Today, "anonymous" (meaning that no identifying information is obtained from the purchaser and verified) network branded prepaid cards are limited to the gift or reward card category (although many network branded gift/reward cardholders are identified and verified as well). Such anonymous gift/reward cards have significant restrictions that minimize risk of misuse such as a relatively low maximum dollar value, no ability to access cash through ATMs, and no ability to load additional funds after the initial funds are depleted. In addition, some issuers restrict usage of anonymous cards to the United States.

Myth No. 4: Prepaid card issuers do not require Customer Identification Programs (CIP) nor OFAC screening for individual prepaid cardholders.—Reloadable, cash-accessible network branded prepaid cards are not available anonymously. Issuers routinely subject individuals purchasing such cards to CIP and OFAC screening, to the same extent as is required for financial institutions opening "accounts" under the Bank Secrecy Act. These verification and screening procedures are identical to those conducted when any on-line bank account is opened.

Myth No. 5: A consumer can use cash to purchase a high-value, reloadable network branded prepaid card from a j-hook and use it anonymously.—When a consumer purchases a reloadable network branded prepaid card from a j-hook in a retail location, a process called "activation" is typically required before the cardholder may use the card for a purchase or to access cash. In other words, although the consumer may purchase the card without identity verification, he/she may not use the card until the identity verification process is complete. The activation process typically involves the cardholder telephoning the card issuing financial institution (or a specialized organization with which the issuer has contracted) and providing personal identification information. The financial institution then verifies various elements of customer information including name, address, Social Security Number, and/or date of birth using a third-party authentication system such as Experian, Lexis-Nexis, or Equifax—just as they would a bank account. The issuer also screens customers against the OFAC Specially Designated Nationals list. If the cardholder does not "pass" this process, the card is either not usable or not reloadable.

IV. THE NBPCA'S ANTI-MONEY LAUNDERING RECOMMENDED PRACTICES

In February 2008, the NBPCA released its "Recommended Practices for Anti-Money Laundering Compliance for U.S.-based Prepaid Card Programs." The document provides recommendations for all network branded prepaid card industry participants to support compliance with the U.S. Bank Secrecy Act (BSA) anti-money laundering (AML) program requirements. It recommends how to implement internal controls, monitor and manage third parties involved with prepaid card processes and mitigate risks associated with money laundering.

To ensure the document addresses the questions and concerns of law enforcement and Government agencies, the NBPCA has and will continue to maintain an open dialogue with Federal, State, and local regulatory agencies as well as law enforcement officials. The document address risks identified through information sharing between the industry and critical agencies that monitor financial crime. "Recommended Practices for Anti-Money Laundering Compliance for U.S.-based Prepaid Card Programs" is a practical guide to setting up, implementing, and auditing a compliance program. It covers the following areas:

1. How to conduct a risk assessment.
2. How to establish a set of internal controls to achieve compliance with AML program requirements of the BSA.
3. Federal reporting requirements and red flags to look for with respect to suspicious activity.
4. Adopting and implementing programs to comply with know your customer requirements.

5. Reducing risk when working with non-financial institutions, third-party agents, and processors.
6. How to implement independent compliance testing.
7. Training program guidelines for key personnel.

The NBPCA has made "Recommended Practices for Anti-Money Laundering Compliance for U.S.-based Prepaid Card Programs" available to anyone in the prepaid card industry. The report, which can be downloaded from the NBPCA Web site at *www.nbpca.com,* has been widely praised and was well-received both by Government and private entities.

V. THE NBPCA'S ROLE ON THE BANK SECRECY ACT ADVISORY GROUP (BSAAG)

In 2008 the NBPCA was selected for membership in the Bank Secrecy Act Advisory Group (BSAAG), a group made up of industry representatives, regulators, and law enforcement, implemented by an act of Congress. BSAAG's role is to advise the Department of Treasury's Financial Crimes Enforcement Network (FinCEN) on matters related to anti-money laundering risks and Bank Secrecy Act compliance. In addition to its role on BSAAG, the NBPCA co-chairs the Stored Value Subcommittee, a subcommittee focused on the potential risks presented by prepaid cards and the ways to mitigate those risks.

VI. RISKS PRESENTED BY DATA SECURITY BREACHES

Data security breaches and the misuse of consumer account information by criminals and money launderers is an increasing problem for the U.S. payment system. Because network branded prepaid cards use the same card payment infrastructure as credit cards, prepaid cardholders can be victims of such data security breaches. However, because prepaid cards are not connected to an individual's bank account or credit card accounts, the risks posed by such data breaches tend to be far less for prepaid card issuers than they are for credit and debit card holders. This is one of the reasons consumers who also use credit and debit cards, are attracted to prepaid card use as any breach of the card limits access to only the balance available on the card. And of course, like credit and debit cardholders, most network branded prepaid card holders are protected against losses from unauthorized use, thanks to the card brands' "zero liability" policies which are incorporated into the payment network operating regulations governing issuers.

VII. CONCLUSION

Network branded prepaid cards are a new and valuable payment product for consumers, businesses, and Government. As with any payment product, network branded prepaid cards can be misused by the criminal element. Nevertheless, the NBPCA has long encouraged practices that reduce the opportunities for prepaid cards to be used in illicit activities. Prepaid cards are vital and important products which serve a substantial number of people, including those that are under-banked and would have no other connection to the banking infrastructure so critical to daily life in the United States. The NBPCA continues to support national and international efforts to combat money laundering, terrorist financing, and financial crime. We are also committed to ensuring that our products are available to help consumers and businesses maintain access to the payment system, have secure and protected payment products, and reduce costs and inefficiencies for consumers, businesses, and government.

Ms. CLARKE. I now ask each witness to introduce yourself and summarize your statement for 5 minutes beginning with Mr. Russo.

STATEMENT OF ROBERT RUSSO, DIRECTOR, PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS COUNCIL

Mr. RUSSO. Thank you, Chairwoman Clarke. Thank you for the opportunity to testify on the critical issue of payment card data security. Payment card fraud concerns every American and, in a global economy, every consumer worldwide. The payment card system is one that manages billions of transactions representing trillions of dollars moving across a global network. Reducing payment card fraud and constantly innovating to stay ahead of it is a critical challenge.

The PCI Security Standards Council was formed in 2006 just for that purpose. Our mission is to protect cardholder data from criminal elements who constantly manufacture new and inventive ways to compromise security systems.

At the center of our efforts to do this are three standards. Let me tell you about each.

First, the PCI Data Security Standard, or the DSS, is a set of 12 security practices based on six core principles. The DSS covers everything from securing applications, to networks, to their perimeters, to maintaining an incident response plan.

Second, our payment application data security systems is designed to ensure that payment applications, which are found in many retailers, are not storing sensitive payment card data.

Third, the PIN security requirements ensure that the PIN entry devices, devices that you may see at a checkout line to enter your PIN number, have been designed to properly encrypt the customer's PIN and are tamper-proof.

But new threats continue to emerge. That is why development and review of the PCI standards is a critical process and why the PCI Security Standards Council takes it seriously. We engage our community of participating organizations, more than 500 merchants, processors, financial institutions, technology companies, Government, academia, and trade associations worldwide to ensure our standards meet the latest threats, and when new threats emerge we have mechanisms to take swift action.

These include regular updates to our testing procedures, monthly Webinars with both assessors and merchants; flash bulletins on emerging threats; as well as on-going updates to the standards themselves.

Our goal is simple: To have every organization that stores, processes or transmits cardholder data do so in accordance with the PCI standards. I have no doubt that compliance with the PCI standards is an entity's best line of defense against payment card data compromise. In fact, we have never found a breached entity to have been in full compliance with the PCI standards at the time of a breach.

But we also recognize that the dynamic nature of any organization can render a validated system noncompliant almost immediately after a satisfactory compliance report has been issued. Effective security is not a one-time snapshot, but really a full-length feature film where the organization is compliant at each and every frame.

No standard is perfect. But the PCI security standards have proven to be the most effective means of preventing data breaches and protecting consumers.

One final point. In order to assist organizations with maintaining and achieving compliance with our standards, the Council provides a wide range of resources. For example, the on-going training, approval and quality assurance of qualified security assessors; a worldwide network of professionals that conduct on-site compliance assessment; the validation of a worldwide network of approved scanning vendors who do remote scanning of networks, secure them against network threats; and finally, an education program

that includes printed materials, on-line resources, Webinars and face-to-face training sessions.

Payment card fraud is a serious concern demanding a serious, continuous and vigorous response. The PCI Security Standards Council has made its sole mission the securing of cardholder data.

Thank you and I look forward to answering your questions.

Ms. CLARKE. Thank you for your testimony.

[The statement of Mr. Russo follows:]

PREPARED STATEMENT OF ROBERT RUSSO

MARCH 31, 2009

INTRODUCTION

Chairwoman Clarke, Ranking Member Lungren, Members of the subcommittee, thank you for the opportunity to testify on the important issue of payment card data security.

My name is Bob Russo and I am the general manager of the PCI (Payment Card Industry) Security Standards Council. The Council is an industry standards body responsible for developing security standards that merchants (such as retailers, transportation companies, hotels, etc.) and payment card transaction processors use to protect customers' payment card data as it is stored, processed, or transmitted from the point of sale to the card issuer for authorization and subsequent processing.

Payment card fraud is something that concerns all of us, both businesses and consumers alike—from the pizza shop down my street to the country's largest retailers; from a single parent who manages the household finances to the businesswoman who conducts trade globally. For the consumer, having one's card data stolen can be an inconvenient and stressful experience, even though here in the United States the consumer normally bears no liability for any ensuing fraudulent transactions. It is also very costly for financial institutions that have to mitigate the damage associated with a payment card compromise, and for businesses that can lose customer confidence and suffer damage to their reputations. Data theft impacts everyone in the payment stream.

The PCI Security Standards Council was formed with the intent of providing tools and resources to protect payment card data from all threats, regardless of motivation. In the less than 3 years since our formation, we have made tremendous strides toward this goal—and our efforts continue. We welcome the subcommittee's interest in the topic of payment card data protection, and appreciate the Government's on-going commitment to understanding and exploring the initiatives underway to contain and reduce fraud for consumers and businesses globally. We look forward to working with the subcommittee to continue to reduce payment card data compromise and invite the subcommittee to use the Council as a resource as it develops policies to combat cybercrime.

My testimony today will cover the background and history of the Council, how we came about, what we seek to do and with whom we work to develop and maintain the standards in a dynamic security environment. I will also detail some of the tools and resources we have made available to the market to enable businesses to secure payment card data wherever it is processed, stored, or transmitted.

ABOUT THE PCI SECURITY STANDARDS COUNCIL

The PCI Security Standards Council, LLC is a global forum for the on-going development, enhancement, dissemination, and implementation of security standards for payment card data protection.

The Council was founded in September 2006 by the five major payment card brands: American Express, Discover, JCB, MasterCard, and Visa. Together, these five brands represent the vast majority of payment card transactions both Nationwide and globally. In coming together, these organizations agreed to work together to develop and recognize one set of data security standards to protect payment card data that is stored, processed, or transmitted.

Prior to the formation of the Council, each of the payment card brands developed their own set of requirements to ensure that the data of those carrying their respective cards was maintained in a secure fashion. Consequently, retailers and other merchants expressed frustration at the challenges of securing payment card data in a way that was not universally recognized by all the payment card brands with

which they did business. Organizations involved in the payment process also highlighted their desire for a mechanism to contribute to the payment card data security agenda and to provide input and gain insight into the security standards they would be using. It is for this reason that broad participation and transparency are core tenets of the Council's operating principles.

The Council is but one example of the hundreds of private sector-based entities that have been formed to develop voluntary consensus standards across virtually all branches of industry to serve new needs as they arise, thereby helping to ensure that businesses can conduct their operations responsibly at home, and competitively around the globe. This private sector role in standards development was mandated by Congress in 1995 by its enactment of the National Technology Transfer and Advancement Act (Pub. L. 104–113) ("the Act"). The Act requires Government agencies to dramatically decrease the creation and use of "Government-unique" specifications in their procurement activities, and instead rely on voluntary consensus and private sector standards whenever possible, as well as to report, via the National Institute of Standards and Technology, their compliance with this directive. In 1998, the Office of Management and Budget (OMB) updated Circular A–119 to provide additional guidance to the Federal agencies on implementing the Act. Under the Act, Government agencies are requested to participate in developing voluntary consensus private sector standards to the extent that their resources allow. Consistent with this mandate, several governmental entities participate in the PCI Security Standards development process.

THE COUNCIL'S MISSION

The mission of the PCI Security Standards Council is to enhance payment card data security by developing and maintaining appropriate security standards and related tools, and driving education and awareness of the critical importance of data security. Even though the Council is a business-focused organization, this mission has at its heart the protection of consumers. The Council works to provide the necessary tools and resources that organizations should use to protect their customers' payment card data successfully.

As discussed below, the Council achieves this end by enabling a sophisticated, global security infrastructure based upon five highly specialized and important mechanisms:

1. Standards for implementation by both those that store, process, and transmit payment card data, as well as those that sell the devices and other equipment that access and transmit such data.
2. Approval, training, and on-going quality assurance of a worldwide network of "Qualified Security Assessors" (QSAs) that conduct on-site assessments to determine whether those with access to payment card data are in compliance with applicable Council standards.
3. Approval, training, and on-going quality assurance of a worldwide network of "Approved Scanning Vendors" (ASVs) that conduct remote scanning of networks to determine whether those networks are secure against most network-based attacks.
4. Training and approval of laboratories that can in turn approve certain products to be in adherence with applicable Council standards.
5. Training and education of payment process participants through classroom sessions, collateral material and webinars, so they are aware of the importance of protecting payment card data from emerging threats and can actively participate in protecting themselves and their customers from attacks.

HOW THE COUNCIL DIFFERS FROM OTHER PARTIES IN THE PAYMENT CHAIN

As a standards body, the Council is responsible for developing and maintaining the security standards and other tools necessary to protect payment card data within the payment process. The Council publishes these standards for anyone to access but specifically for the payment card industry's use in security and compliance programs. It is important to distinguish between this role as standards custodian and industry body from those organizations that may validate compliance or enforce compliance through rules, rewards, or actions against parties not yet compliant with applicable security standards.

The Council does not validate the compliance of any entity or vendor with its core standard, the PCI Data Security Standard ("PCI DSS"). Indeed, like any other organization that develops voluntary consensus standards, it does not have the authority or mechanisms to enforce compliance to its standards. Consequently, the Council does not run standards compliance programs. Instead, each payment card brand maintains its own compliance programs based upon the Council's standards, adding

their own stipulations and requirements for demonstrating compliance for those businesses that must comply. Therefore, the Council has no direct business relationships with those entities that store, process, or transmit payment card data, and does not have the responsibility or contractual right to validate compliance, enforce, or levy fines for non-compliance with the security standards that it publishes. Each of these roles is performed by the payment card brands.

THE COUNCIL'S STAKEHOLDERS

In order to be certain that the Council's standards are as clear and comprehensive as possible, we seek input from a wide range of stakeholders as part of the standards development process. For instance, the Council's Participating Organization program is open to any organization involved in the payment chain—merchants, banks, processors, Government, and academia. To date, more than 500 leading national, regional, and global players are part of this effort.

Participating Organizations provide the Council with real world insight and experience in deploying security standards in the field, and have deep understanding of the challenges and threat vectors that security standards must address. Together, these Participating Organizations represent the people who are responsible for securely handling and defending consumers' payment card data against attack on a daily basis, and therefore provide a valuable resource in feeding front-line threat information into the Council.

From among the Participating Organizations, a smaller group of 21 representatives are seated as the Council's Board of Advisors every 2 years through an open election and appointment process. Two-thirds of the Board of Advisors are elected, with the remainder appointed to ensure adequate geographical and industry representation. These organizations act as spokespersons for their respective industries and regions and ensure that the Council is able to partner with industry at a very detailed and actionable level in the standards-setting process. The Board of Advisors is a critical enabler in our mission to secure businesses' payment processes and consumers' payment card data globally.

Our current Board of Advisors is composed of leaders in their respective industries such as Wal-Mart Stores, Inc., Microsoft, PayPal, First Data Corporation, and British Airways. The Board has worked tirelessly with the Council over the past 2 years to highlight areas of need in the market, and to devise educational resources that are of immediate benefit to organizations looking to improve their security.

I want to recognize here for the record the hard work of our Participating Organizations and Board of Advisors, all of whom contribute to the Council's security standards in an entirely voluntary capacity.

In addition to our Participating Organizations, the Council's QSA and ASV communities, together numbering more than 250 companies worldwide, provide valuable insight from the front lines of examining merchants and processors systems. QSAs and ASVs are able to provide feedback on where the implementation challenges lay and when common security vulnerabilities appear. The Council is in constant two-way communication with this group through webinars, newsletters, and, of course, the Council's annual QSA and ASV retraining and examination processes.

THE PCI SECURITY STANDARDS

The Council's security standards—the tools it makes available for use by public and private sector entities to secure payment card data—are designed to protect specific parts of the payments process. The Council is constantly looking for new ways to secure the payment process and maintains a dialogue with its Board of Advisors and other industry stakeholders to bring new resources to the market to further protect consumer's payment card data. As a result, since its inception in 2006, the Council has assumed management responsibility for several payment security standards in addition to the more-well known PCI DSS, with the mission of increasing payment card data security. I'd like to give a brief overview of the standards the Council currently manages and updates:

PCI Data Security Standard

The PCI Data Security Standard is a set of 12 detailed requirements designed around six principles fundamental to securing payment card data. At the heart of this standard is the requirement that organizations do not store sensitive payment cardholder information typically contained in the magnetic stripe on the back of the payment card. This is the information that criminals want to steal to create counterfeit cards. The fundamental principle of the PCI DSS is that organizations must not store sensitive data. Where information such as the Primary Account Number (PAN) or expiration date is stored, it must be rendered unreadable. This generally

means that it must be truncated, hashed, or encrypted, so that unauthorized access to such data will be of limited use to a criminal.

Along with these fundamentals, the very detailed requirements of the PCI DSS cover areas ranging from securing applications, networks, and perimeters to maintaining up-to-date security patches and anti-virus software, to things like developing and maintaining an incident response plan and processes for an organization to follow in the event of a breach.

The Payment Application Data Security Standard (PA–DSS)

The Council developed this standard after feedback from our Participating Organizations and member brands indicated that software applications represented a point of weakness in the payment chain. These payment applications range from touchscreen applications you might see used in a restaurant, to point-of-sale software used in ticketing kiosks in museums and theme parks. Unless otherwise required by the customer demanding PA–DSS compliance, some of these payment applications may be designed to store sensitive payment card data thereby undermining an organization's efforts to comply with the PCI DSS. The Council introduced a process that enables payment applications to be tested in laboratories to determine whether they are secure, not storing payment card data, and whether they are capable of helping, rather than hindering, an organization's efforts to comply with the PCI DSS. The Council maintains a list on our Web site of validated payment applications that have been tested in and approved by laboratories for merchants to use in assessing their own applications and making informed purchasing decisions.

The PIN Entry Device Security Requirements

The PIN Entry Device security requirements have the same underlying principle as the PA–DSS. They are designed to enable organizations to protect consumer's payment card data and ensure that PIN Entry Devices have been designed not to store payment card information, thus jeopardizing organizations' PCI DSS compliance efforts. As a PIN Entry Device is a physical object, these requirements cover not just ensuring that a device does not store sensitive data, but also that it is tamperproof, and that, should the device be compromised, its contents will self-destruct.

The Council maintains a list at its Web site of approved devices that have been successfully tested in Council-approved laboratories for merchants to cross-reference against their own devices and to assist them in making informed purchasing decisions. The Council is currently working to expand the scope of this program to include a broader array of device types, including unattended payment terminals such as ticket kiosks and self-service machines.

Development and review of the PCI standards is a continuous process. In the case of the PCI DSS, the Council follows a defined 24-month life-cycle process that incorporates a feedback period from stakeholders and allows for periods of review by the Council's Board of Advisors, Participating Organizations, QSAs, and ASVs.

While a planned life-cycle process is important, it is equally important that the Council be responsive to emerging threats. As a result, we have several mechanisms for on-going communications with assessors (QSAs and ASVs), merchants and other stakeholders to provide guidance as new threats emerge. These include:

- Errata to the DSS itself;
- Flash bulletins on emerging threats;
- A monthly newsletter to the Assessor community with the latest threat information & corresponding changes required to the assessment process;
- Regular updates to the ASV test scanning environment to reflect new threats emerging "in the wild";
- Monthly Webinars with both assessors and merchants;
- Updates to the Council's on-line searchable FAQ and training materials to ensure they include the latest information on the threat landscape.

THE NATURE OF THE COMPLIANCE CHALLENGE AND PROCESS

Validation of compliance with the PCI Data Security Standard can only represent a snapshot in time that coincides with information shared with and interpreted by a QSA during the assessment period. Unfortunately, the dynamic nature of any organization's systems and network environments can result in a wide variety of actions or inactions that can render a validated system noncompliant almost immediately after a satisfactory compliance report has been issued. As a result, effective compliance is a full-length feature film where the organization is "compliant" at each and every frame of that film. For that reason, the Council believes achieving and maintaining compliance with PCI DSS and continuous vigilance regarding other

security practices is an on-going process that must systematically be integrated into every organization's development and operational practices and policies in order to serve as the best line of defense against a data breach.

The evidence of data breaches demonstrates that criminal elements continue to manufacture new and inventive ways to compromise security systems, and we can assume that this will continue to be true. The Council, its members and others are working diligently to secure payment card data against increasingly experienced and organized criminals. In spite of the severity of this continually dynamic threat landscape, the Council believes achieving and maintaining compliance with the PCI DSS is the best line of defense against data breaches.

It is important to note that the members of the Council report that they have never found an entity that has been subject to a data breach that was also in full compliance with the PCI DSS at the time of the breach. Nonetheless, there is no such thing as perfect security. An organization could very well be compliant on the day its QSA wrote its assessment report, but noncompliant thereafter, at the time of a data breach. Many things can cause the protection to break down—logging rules not being followed, delaying installation of software patches, installing untested software, etc. Any of these examples (and many more) may cause a previously validated company to no longer be compliant, and therefore vulnerable to attack. Organizations must not take solely a checklist approach to security, or rely on periodic validation on a specific day as their security goal, but must instead exercise continuous vigilance and maintain a strict security program that ensures constant and ongoing PCI DSS compliance.

THE FUTURE OF THE COUNCIL'S EFFORTS AND PAYMENT SECURITY

To succeed in the fight against cybercriminals who target our payment systems will require the continued vigilance and work of all parties involved in the payment chain. No system is perfect, and while breaches can be expected to continue to occur, through our efforts and the pervasive adoption of the Council's standards and the best practices it advocates, the work of these thieves will remain as difficult as possible.

When breaches do occur, the Council works with its member brands, forensics investigators and, at times, through direct outreach to seek information from breached entities, to determine the root causes of the breach. If a need to strengthen the Standards or the Council's Assessment programs is identified, we have mechanisms in place for taking swift action.

CONCLUSION

Once again, I want to thank Chairwoman Clarke, Ranking Member Lungren and the subcommittee Members for their oversight of this issue and for providing me the opportunity to testify on the important issue of payment card data security. We hope that those entities that handle payment card data take from this hearing the understanding of their responsibilities to consumers, shareholders, and society at large to increase focus on their payment security efforts. Using the PCI Security Standards should act as a baseline for their doing so. We also hope that many more of them will join us as Participating Organizations, willing to help shape the future of payment security standards based on their own experience of defending payment data against attack on a daily basis.

Ms. CLARKE. I now recognize Mr. Majka to summarize his statement for 5 minutes.

STATEMENT OF W. JOSEPH MAJKA, HEAD OF FRAUD CONTROL AND INVESTIGATIONS, GLOBAL ENTERPRISE RISK, VISA, INC.

Mr. MAJKA. Chairwoman Clarke and Members of the committee, my name is Joe Majka. I am head of Fraud Control and Investigations for Visa, Inc. I have been with Visa for over 12 years, and I have over 28 years of experience in corporate security investigations and law enforcement, specializing in the area of financial crimes.

I want to thank the committee for this opportunity to appear at today's hearing and to explain who Visa is in our role as a leader in global data security. It is important to note that Visa's funda-

mental role is to facilitate transactions between millions of consumers and businesses. Visa is not a bank and we do not issue payment cards. Visa is a network that connects 1.6 billion global payment cards, 29 million worldwide merchants, and over 16,000 financial institutions in 170 countries.

Through electronic payment networks like Visa, the entire economy benefits from a more transparent, cost effective, and secure commercial activity.

I am pleased to be here to talk with you about data security and about the payment card industry data security standard in particular. In our view, the best way to secure payments is by applying two core principles.

First, security must be a shared responsibility among all relative parties—law enforcement, payment companies, regulatory agencies, retailers, and others. Only together can we protect all parts of our shared system.

Second, we must collectively apply multiple layers of security to protect the system. That includes measures applied at the card level such as card verification values or transaction alerts, and includes measures applied at the point of sale, such as standards for secure devices and best practices for data storage, and it includes measures applied at the network level, including neural networks and fraud monitoring.

One of the most effective layers we have collectively applied to date is the PCI Data Security Standard. Visa acquires all entities that store transmitter Visa card data to comply with the standards. To our knowledge, no organization that is fully implemented and maintained compliance with the standard has been a victim of a data compromise event. We believe full compliance with the standard is a valuable component of a comprehensive security program and greatly reduces the risk of data compromise.

While there have been a few instances where an entity that previously validated compliance was a victim of a compromise, in all cases our review concluded gaps in the compromised entity's PCI DSS controls were major contributors to the breach.

Approximately 90 percent of the U.S. merchants and 80 percent of third-party processors have validated PCI compliance. These organizations, like Michaels, deserve credit to enhancing their security practices to meet the minimum industry standard and for validating their compliance on at least an annual basis.

This month in Washington, DC, Visa held our third Global Security Symposium, a symposium on payment security where Visa called on system participants for continued industry investment, collaboration, and innovation to keep the electronic payment system secure for the future. At this summit we heard from numerous individuals and organizations who reaffirmed the importance of ongoing compliance with the PCI standards.

Visa has maintained a long-standing relationship with law enforcement agencies over the years, supporting efforts to investigate and prosecute criminals committing payment card fraud. This relationship continues and is stronger than ever today as Visa and law enforcement agencies work together to combat cybercriminals in today's high-tech world.

Visa was a founding member of the U.S. Secret Service Electronic Crimes Task Force in San Francisco and continues to actively participate in U.S. Secret Service task force groups. Visa also works closely with the FBI Cyber Division, U.S. Postal Inspection Service, State attorneys general, and the Department of Justice Computer Crime and Intellectual Property Section.

In 2004, Visa provided investigative support to law enforcement which resulted in the indictment and extradition of Roman Vega, one of the most significant high-level cybercriminals at the time. Visa continues to support high-profile investigations, including the arrests of criminals responsible for hacking into Dave and Busters and T.J. Maxx. Visa values our partnership with law enforcement and is committed to continuing to work closely with law enforcement to bring cybercriminals to justice.

Protecting card holders is always a primary goal in responding to data compromise incidents. After learning of a data compromise, Visa immediately begins to work with the compromised entity, law enforcement, and the affected client financial institutions to prevent card-related fraud.

In closing, securing consumer data within the U.S. economy is a shared responsibility, and every industry should deploy focused resources to protect consumer information within its care. We look forward to working with all participants to continue to develop tools to minimize the risk and the impact of data-compromise events.

Thank you for the opportunity to be here today. I would be happy to answer any questions.

Ms. CLARKE. Thank you for your testimony.

[The statement of Mr. Majka follows:]

PREPARED STATEMENT OF W. JOSEPH MAJKA

MARCH 31, 2009

INTRODUCTION

My name is Joe Majka. I am the head of Fraud Control and Investigations for Visa Inc. I have been with Visa for over 12 years and have over 28 years of experience in corporate security, investigations, and law enforcement, specializing in the area of financial crimes. I want to thank the committee for this opportunity to appear at today's hearing and explain who Visa is and our role as a leader in global data security. Visa plays a unique role in the financial system, facilitating commerce among millions of consumers and businesses here and around the globe. It is important to note that Visa's fundamental role is to facilitate transactions between consumers and businesses. Visa is not a bank. We do not issue payment cards (credit, debit, or prepaid), make loans to consumers, or set the interest rates or fees associated with card usage or acceptance. Visa is a network that serves as the connection point between 1.6 billion global payments cards, 29 million worldwide merchants, and 16,600 financial institutions in 170 countries. In making these connections, Visa helps create significant value for each of the participants in our system. Consumers receive a more convenient, secure, and widely accepted way to make payments. Retailers benefit from the speed, efficiency, security, and reliability that only electronic payments can provide. They also receive guaranteed payment and can avoid the need to extend credit directly to their own customers. In fact, the entire economy benefits from electronic payments through more transparent, secure, and cost-effective commercial activity. The Visa Payment System plays a pivotal role in advancing new payment products and technologies, including initiatives for protecting cardholder information and preventing fraud.

We're pleased to be here to talk with you about data security in the payment card industry and about the Payment Card Industry Data Security Standard in particular. But, I want to put this discussion in the context of a multi-layered approach

to security that includes fraud control measures from the card, to the terminal, through to the Visa network. Visa understands that we must protect each link within our control and work with others to preserve the trust in every Visa payment. Visa is keenly focused on ensuring that payment products are not used to perpetrate identity theft or other criminal activity. Our goal is to protect consumers, merchants, and our client financial institutions from fraud by preventing fraud from occurring in the first place. To that end, Visa employs multiple layers of security, of which the PCI standard is an important one, but only one of many. We have taken a leading role in promoting cardholder information security within the payments industry. Visa and our participating financial institutions also provide solutions to prevent fraud and protect cardholders in the event of a data compromise. These include real-time fraud monitoring, identity theft assistance, consumer alerts, and zero liability for cardholders on fraudulent transactions. Visa provides sophisticated neural networks that enable our client financial institutions to block authorization transactions where fraud is suspected. Thanks to massive investments and innovative solutions, compromise events rarely result in actual fraud and fraud rates in the payments industry remain near all-time lows.

The payment card industry, regulatory agencies, and law enforcement have individually and collectively taken extensive measures to prevent and mitigate the effects of consumer information compromises. In this regard, Visa has required all entities that store, transmit, or process Visa card data to comply with PCI DSS standards, has implemented incentives to encourage payment participants to make the significant investments needed to attain compliance, and has taken numerous steps to minimize the amount of cardholder data stored by system participants.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

PCI DSS was the first security standard adopted by the PCI SSC, but it has not been a static standard. The PCI Security Standards Council is charged with reviewing and updating the standard to ensure that it remains effective to protect card data, by incorporating input from stakeholders as well as technological developments in the evolution of the standard over time. Visa recognizes that no set of standards can provide an absolute guarantee of security in a changing world, and PCI DSS is not an exhaustive list of all the security practices that may be effective to safeguard card data. To our knowledge, however, no organization that has fully implemented and maintained compliance with the PCI DSS has been the victim of a data compromise event. Therefore, we believe that full compliance with the standard is a valuable component of a comprehensive security program and greatly reduces the risk of data compromise. We also believe that PCI DSS controls are highly effective in mitigating the impact of data compromise events.

Validating PCI DSS is a major milestone, but achieving and maintaining compliance requires companies to make an on-going commitment to keeping consumers' data safe—24 hours a day, 7 days a week, 365 days a year. While there have been a few instances where an entity that previously validated compliance was the victim of a compromise, in all compromise cases our review concluded that gaps in the compromised entity's PCI DSS controls were major contributors to the breach. As such, Visa continues to believe that standards validation is a valuable process that drives organizations to undertake the minimum steps necessary to protect cardholder data. While it is easy to focus on the failures that some entities have had with on-going compliance, we believe it is likely that many compromises have been prevented as a result of the strenuous efforts of merchants and processors to maintain compliance with PCI DSS.

VISA SECURITY INITIATIVES

Visa leads the payment industry in providing merchants and service providers with incentives to validate and comply with PCI DSS in order to ensure that they properly protect cardholder data. In particular, Visa launched a Compliance Acceleration Program offering $20 million in incentive payments to promote compliance among the largest U.S. merchants that account for more than two-thirds of Visa annual transactions. Visa's combination of incentive payments and potential fines ultimately drove the vast majority of large U.S. merchants to validate their initial compliance with PCI DSS and to revalidate annually thereafter. At this time, approximately 90 percent of large U.S. merchants have validated PCI DSS compliance. Visa also publishes a list of service providers that have validated compliance with the PCI DSS, which has been the principal incentive in driving 80 percent of U.S. service providers to validate their compliance on an annual basis. These organizations, like Michaels, deserve credit for enhancing their security practices to meet the min-

imum industry standard and for validating their compliance on at least an annual basis.

Visa has also made considerable strides toward eliminating the storage by merchants and processors of authorization data, which criminals covet to perpetrate fraud. This "prohibited" data includes full magnetic stripe information, the CVV2 or "Card Verification Value 2" and PIN. Visa has executed a "drop the data" campaign over the past 3 years to encourage merchants to discontinue storage of prohibited data and reduce overall cardholder data storage. Additionally, Visa developed security standards for payment application vendors to support merchants in their security efforts by driving vendors to reduce data storage and provide more secure payment application products.

Visa has executed a robust data security educational campaign to engage payment system participants in the fight to protect cardholder information. This campaign includes training for financial institutions, merchants, and service providers. Most large merchants, including Michaels, have attended one of Visa's security training seminars. Visa is also committed to educating system participants on emerging security threats and publishes regular security alerts and bulletins, and holds seminars focused on data security and fraud mitigation. Visa has partnered with organizations like the National Retail Federation to promote data security among its members and commends the NRF and Michaels for their data security efforts. Visa outreach also extends to participation in industry forums on data security, media campaigns, and partnerships with other industry groups made up of merchants, such as the U.S. Chamber of Commerce. This month in Washington, DC, Visa held our third Global Security Summit, a symposium on payment security where Visa called on system participants for continued industry investment, collaboration, and innovation to keep the electronic payment system secure for the future. The Global Security Summit reaffirmed the importance of on-going compliance with security standards and highlighted opportunities to actively engage consumers in the process of fraud prevention through Visa's transaction alerts and notifications service which can not only help consumers track and manage their accounts, but also provide an early warning of potentially fraudulent activity.

COLLABORATION WITH LAW ENFORCEMENT

Visa has maintained a long-standing relationship with law enforcement agencies over the years, supporting efforts to investigate and prosecute criminals committing payment card fraud. This relationship continues and is stronger than ever today, as Visa and law enforcement agencies work together to combat cyber criminals in today's high-tech world. In 2002, Visa was a founding member of the U.S. Secret Service San Francisco Electronic Crimes Task Force and continues to actively participate in U.S. Secret Service task force groups in San Francisco, New York, and Los Angeles. Visa also works closely with the Federal Bureau of Investigation's Cyber Division, United States Postal Inspection Service, State Attorneys General and the Department of Justice Computer Crime and Intellectual Property Section.

In 2004, Visa provided investigative support to Federal law enforcement, which resulted in the indictment and subsequent extradition to the U.S. of Roman Vega, known on-line as "Boa". Roman Vega was allegedly one of the most significant high-level criminals specializing in the on-line sale of stolen payment card data at the time. Visa has continued with our investigative support on other high-profile investigations, including the Federal prosecution of Max Ray Butler known on-line as the "Iceman", arrested by Federal agents in 2007 and the 2008 arrest of Albert Gonzales, Maksym Yastremskiy, and Aleksandr Suvorov for their scheme in which they hacked into Dave & Busters, Inc. restaurants. Visa also works closely with local law enforcement agencies and local retailers in supporting their effort to investigate and prosecute street level criminals using payment cards to commit fraud. Visa values our partnership with law enforcement and is committed to continuing to work closely with law enforcement to bring cyber criminals to justice.

RECENT COMPROMISE EVENTS

After learning of data compromise events, Visa immediately begins working with the compromised entity, law enforcement, and affected client financial institutions to prevent card-related fraud. Visa notifies all potentially affected card-issuing institutions and provides them with the necessary information so that they can monitor the accounts and, if necessary, advise customers to check closely all charges on their statements or cancel or reissue cards to their customers. Visa card-issuing institutions have the direct responsibility and relationship with cardholders, and because of Visa's zero liability policy for cardholders, bear most of the financial loss if fraud

occurs. Visa financial institutions can best determine the appropriate action for each customer that might have been affected.

Based on Visa's findings following recent compromise events at Heartland Payment Systems and RBS WorldPay, we have taken the necessary step of removing both companies from our on-line list of PCI DSS-compliant service providers. In addition, we are activating our account data compromise recovery programs, which are in place to protect our system and help issuers recoup some of their losses from compromise events. Visa is committed to working with these processors so they can be reinstated to this list upon successfully revalidating their compliance and Visa is not penalizing merchants that continue to utilize these processors. Protecting our cardholders was, and remains, Visa's primary goal in responding to this incident.

CONCLUSION

In closing, securing consumer data within the U.S. economy is a shared responsibility, and every industry should deploy focused resources to protect consumer information within its care. In this regard, the payment card industry has done more than any other to provide stakeholders with the tools and guidance that they need to properly secure the data they are trusted to protect. Visa has led the industry in protecting cardholder data and stands ready to continue to support industry participants in our collective fight against the criminals that perpetrate card fraud. We look forward to working with all participants to continue to develop tools to minimize and eventually eliminate the risk of data compromise in our economy. Thank you for the opportunity to present this testimony today. I would be happy to answer any questions.

Ms. CLARKE. I now recognize Mr. Jones to summarize his statement for 5 minutes.

STATEMENT OF MICHAEL JONES, SENIOR VICE PRESIDENT AND CHIEF INFORMATION OFFICER, MICHAELS STORES, INC.

Mr. JONES. Good afternoon, Madam Chairwoman, Members of the committee.

I have been in retail for 30 years, 20 in retail IT, the last 4 with Michaels, a $4 billion merchant. I wish I could say that attempting to follow the PCI mandates made me confident that credit card data is completely safe, but unfortunately that is not the case. This is because the mandates have been developed from the perspective of the card companies rather than from those who are expected to follow them.

The PCI data and 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. The program is rife with ambiguity and complexity. As an example, must every company associate acknowledge the security policy of a company? All 40,000 of our associates, or just those involved with credit transactions? This one PCI mandate has been imposed by compliance vendors differently at retailers all across the country.

We have been questioned by customers, legislators, and even the credit card companies themselves, why do you keep credit card information at all? One reason we keep the information is related to another credit card company procedure designed to protect their banks from loss. It is called a chargeback. It can be initiated by a bank on its own, or it can be initiated at the request of the bank's customer.

For example, if a customer spots a charge on their credit statement that they don't recognize, they can initiate a chargeback by contacting the issuing bank. The retailer is then charged with retrieving sales media by card number. If the retailer is unable to

produce that sales media, or something on that sales media does not match, the retail sale is reversed, and the cost of the transaction is charged back against the retailer. This is true even if the transaction may have actually been made. This could have been fairly easily solved using a unique approval ID for each transaction, thus eliminating the need for credit card number storage by the retailer.

PCI states that all credit card data must be encrypted. There is an exception to this requirement, however; PCI states that data traveling over a private network need not be encrypted. While a private network is more secure, I still would not choose to send credit card numbers through this number unencrypted. Why? Because it adds unnecessary risk. However, the credit card companies' financial institutions do not accept encrypted transactions.

We at Michaels have asked, for the past 3 years, for the ability to send encrypted information to the bank. To date, this has not happened. Why is this an issue? One might ask 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 this flaw.

What can be done to improve this situation? First, many of the PCI requirements are covered by the 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 the mandates themselves.

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 credit card companies and banks retain all power over the ultimate mandates, fines, and anything else connected to PCI. It is not an industry standards body.

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 company's data—which, by and large, we do not want—is seized from a retail location. The retailer is in the press, the retailer is demonized, the retailer is threatened with damages and sanctions. The retailer pays the cost of the fraudulent transactions. 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.

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.

In conclusion, 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 what is necessary to keep card data safe, but in the future we would be more secure, and the risks to us all far lower, were the card companies to take greater responsi-

bility for the inadequate system of payment they have created and asked us to use.

Thank you. I am happy to answer any questions.

[The statement of Mr. Jones follows:]

PREPARED STATEMENT OF MICHAEL JONES

MARCH 31, 2009

Good afternoon, Madam Chairwoman, 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 4½ 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 3 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 e-mail. 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 organizations 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 Chairwoman, 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.

Ms. CLARKE. Thank you for your testimony.

I now recognize Mr. Hogan to summarize his statement for 5 minutes.

STATEMENT OF DAVID HOGAN, SENIOR VICE PRESIDENT, RETAIL OPERATIONS, AND CHIEF INFORMATION OFFICER, NATIONAL RETAIL FEDERATION

Mr. HOGAN. Thank you, Chairwoman Clarke and Members of the committee, for this opportunity to appear on behalf of National Retail Federation, the world's largest retail association. I have been with the NRF for almost 7 years and have spent my entire 25-plus-year career in retail information technology.

Whether it be by cash, check, or plastic, the payment mechanism is really just a means of accomplishing business. Retailers accept credit cards for payment, in part because they have been assured by the credit card companies that if they follow a limited number of steps, they will be given a guarantee of payment. Most retailers are not in the payment-acceptance business any more than their customers are in the payment-delivery business.

There have been two big developments in the last decade or so that have changed the playing field. The first has been the rapid proliferation of general purpose credit cards. With over 80 percent of the market share, Visa and MasterCard are two primary examples, these cards issued broadly by banks in the hope that each card will generate income for them.

The second change has been society's increased computerization. Globally there have been numerous instances of hackers from outside of our borders accessing computer systems, stealing credit card information, and then using this data to commit fraud. In several cases these have targeted companies that process or store credit card data.

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 Standard, also called PCI.

PCI is an attempt to prevent large stockpiles of credit card data from getting into the wrong hands. However, the PCI guidelines are onerous, confusing, and constantly changing. Indeed, PCI is little more than an elaborate patch.

The premise behind PCI, that millions of retail establishments will systemically keep pace with ever-evolving sophistication of today's professional hacker, is just not realistic. Our industry has spent billions on compliance programs related to data security. PCI protocols have required many merchants to scrap good existing data security programs and replace them with different security programs that meet PCI rules that aren't necessarily any better. Even companies that have been certified as PCI-compliant have been compromised.

Unfortunately, the economic incentives for the card companies to remedy these flaws in their system have been diminished. It appears to our industry that the credit card companies are somewhat less interested in improving their product and procedures than they are in reallocating their fraud costs. In our view, if you peel back the layers around PCI, you will see it for what it really is, a tool to shift risk off the banks and credit cards' balance sheets and place it on others. It is their payment card system, and retailers, like consumers, are just users of their system. What is really ironic here is that merchants are forced to store and protect credit card data that many don't want to keep anyway. The credit card companies' own rules around retrieval requests essentially require merchants to keep credit card data for extended periods of time.

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 credit card data in the first place. In fact, we proposed such changes to the PCI Security Standards Council back in 2007. The card industry dismissed our proposal without addressing its merits.

There have been numerous suggestions made over the years that would significantly reduce the chances of major data breaches, but none of them have been adopted yet. Here are just a few.

First, go on record and stop requiring merchants to store credit card data and eliminate any penalties they impose for not doing so.

Another, change the system and allow consumers to enter in a pin or personal identification number for credit card transactions, just like you do with debit card transactions.

Third, quickly develop and roll out the next generation of credit card and give merchants the hardware and software necessary to handle these new products.

In conclusion, once the payment system itself becomes a burden, commerce inevitably suffers. We believe any one of these recommendations will significantly reduce credit card fraud.

Thank you for the opportunity for appearing in front of this committee. I will be happy to answer any of your questions.

[The statement of Mr. Hogan follows:]

PREPARED STATEMENT OF DAVID HOGAN

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 50 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 losses 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.

Ms. CLARKE. I thank the witnesses for their testimony.

I will remind each Member that he or she will have 5 minutes to question the panel. I will now recognize myself for questions.

My first question goes to both Mr. Russo and Mr. Majka. Since the PCI standards have become mandatory, there has been no shortage of massive data breaches. Is there any hard evidence to suggest that the standards have reduced the number of data breaches or the amount of credit card fraud? What metrics are in place to judge the effectiveness of these standards?

Mr. RUSSO. Chairwoman Clarke, let me answer first.

The council's purview does not include keeping statistics on breaches, on who is compliant, as we do not have that relationship with the merchants. I can tell you, as I stated earlier, that based on what we have seen in forensics and what we have seen our information has given us by reaching out to these breached entities, that they were, in fact, not compliant at the time of the breach. Very similar to Ms. Glavin, who mentioned locking your doors, you don't lock your doors on Monday, Wednesday, and Friday and not on Tuesday, Thursday, Saturday, and Sunday. So it is constant vigilance that must be there when it comes to protecting this data. It is everyone's responsibility, including the merchant, including the consumer, to be looking after their own data.

Mr. MAJKA. Madam Chairwoman, I would like to say that entry into these data systems, while the criminal is very complex, we found that the entry methods have been very simple, and they would have been addressed by the PCI data security standard in all cases. Even those entities where they have had validated compliance, our review of those incidents found that either they hadn't maintained compliance, and there were significant gaps that allowed the breach to occur.

I would also like to say that the standard itself has been improved over the years. One of the success stories of the standard is the removal of prohibitive data from merchants' servers. This has led to incidents where we no longer have a breached entity who

has been storing data for 3, 4, or 5 years that the criminals can access 5 years' worth of data. So those are things that the standard itself has addressed and has helped.

I would also like to say that I think that we don't know how many breaches have been prevented by those entities that have, in fact, gone as far as implementing and maintaining the standard properly.

Ms. CLARKE. I think that is really at the core of the issue here is that we can't get some tangible evidence of how effective this is in actually eliminating the breaches. It is clear that if people aren't following the protocols, that opens them up in terms of more vulnerability. But it would seem to me that as a part of the build-out of the floor of the PCI standards, that we would develop some sort of metric that gives us an ability to objectively judge the effectiveness of these standards. Are you saying that those don't exist right now?

Mr. RUSSO. No, Madam Chairwoman. They do exist in various entities, those entities being the acquiring banks, as an example, which own the relationships with the merchants. They require PCI compliance, they track PCI compliance, they have those numbers. Again, the council does not have any input into that or any view into that because we do not have the relationships with the merchants. The banks, the acquirers have the relationship with the merchants. But there are tens of thousands, hundreds of thousands that are going through programs every day and validating their compliance on a regular basis.

Ms. CLARKE. Mr. Russo, do you have a relationship with the banks?

Mr. RUSSO. The council does not have a relationship with the banks other than to put its standard out there and make sure that they are creating awareness among their constituents that they need to be compliant with the standard.

Ms. CLARKE. Thank you.

The next question then is both to you, Mr. Russo, and Mr. Majka. The PCI standards include requirements for encrypting data at rest and data that travels over the internet. But the Heartland breach, for instance, involved data in transit between terminals and hosts on nonpublic networks.

As Mr. Jones notes in his testimony, there are no PCI standards for this. Is this a fundamental weakness in the standards? Why doesn't PCI require end-to-end encryption, including internal encryption? How are you going to address this?

Mr. RUSSO. There are provisions within the standard now that address this data and address the inside network that should, in fact, either stop this from happening, or at least give you a warning that something is happening so that you can immediately stop it and cut the breach off. We do go out to, as I mentioned, all of our participating organizations—one of whom is sitting at the table with me today, the NRF—and we do ask them for their feedback on the standard and what needs to be done.

One of the things that we are in the process of doing right now is that we have issued a proposal to a number of technology companies to give us an independent study on what we are calling emerging technologies, one of which is end-to-end encryption, another of

which is tokenization, another of which is chip and PIN. So we are looking at these technologies and how they make the standard more robust. But it is important to the say that there really is no silver bullet here.

Ms. CLARKE. I am a bit over my time, but I would like to get Mr. Jones' and Mr. Hogan's response to this end-to-end encryption dilemma.

Mr. JONES. First, I think on encrypted, I am not sure I would call it an emerging technology; it has been around for some time. Obviously, since it is a requirement for anything traveling outside the private network, I think that not having it as part of something that travels on your internal network was something originally to reduce some of the costs involved with implementing the standards, because it costs money to implement encryption end-to-end, and that would have involved a lot of cost to merchant banks all across the country, as well as retailers. Every retailer would have had to implement encryption on their side. But we have already had to do it from—and most retailers do transact across the internet in one way or another, so we have had to do that.

So I would separate that out from a chip and PIN discussion as far as what we should be looking at going forward. As far as whether it should be in the standard or not, I feel that it should have been in the standard long ago as part of something simply because there are things that may have caught the Heartland Payment thing. But when we talk about very sophisticated thieves, the Heartland Payment software that was used was so sophisticated that it was virtually impossible for highly technical, highly sophisticated people to pick up. Most of the existing scanning technologies would not have even picked it up, but had it been encrypted, it wouldn't have mattered. I think that is the way of looking. So why not lock your front door? Why leave it open?

Ms. CLARKE. Mr. Hogan, do you concur?

Mr. HOGAN. Yes, I do concur. I think it is very interesting that the merchants, universities, doctors' offices, anybody who accepts credit cards and processes credit card data has to go through extraordinary hoops to adhere to a PCI standard; however, when it is convenient, the information is sent open in the free and clear, when it is transmitted to the banks, so on and so forth.

So I think you have a double standard going on here where in one case you have to adhere to a standard, and spend a lot of time, effort, and money to do it, and then all of a sudden you send it back out wide open that anybody could potentially read unencrypted downstream.

Ms. CLARKE. Thank you. My time is expired.

Let me now acknowledge the gentleman from New Mexico, Mr. Luján.

Mr. LUJÁN. Thank you, Madam Chairwoman. I know we have some votes we have to get to, if I am not mistaken, so I will try to keep this brief.

Mr. Russo, what recommendations of standards have been made that have not been implemented by those that follow your standards?

Mr. RUSSO. Congressman, we have a feedback process in place, which Chairwoman Clarke mentioned a little earlier—actually, I

am a little perplexed because Mr. Hogan earlier said that this is constantly changing, yet Chairwoman Clarke indicated it was a 2-year process that we go through. We go through two feedback periods where we get feedback from all of those participating organizations, again, one of which is the NRF, and we then discuss all of this information at two community meetings that we have on a yearly basis, one in North America and one in Europe. That information is then taken back from what we are getting again at that community meeting and gone through another feedback period before a new standard is released.

I might also mention that the difference between the initial standard that we came out with in 2006 and the 1.2 version, which we came out with in October, was not that different. There were clarifications, there were documentation changes, more guidance information was put in to make it easier to understand the intent and, in fact, comply with it. These were all recommendations from these participating organizations, from our board of advisors. There are things that we put out on a regular basis based on their input. We do not create this standard in a vacuum. This is something that the entire group of participating organizations and the assessment community and our board of advisors advise us on.

Mr. LUJÁN. Let me narrow the question a little bit.

Mr. Russo, there was some discussion about end-to-end encryption for its databases. Isn't that a recommendation that was made by the Heartland Payment Systems CEO?

Mr. RUSSO. After the breach it absolutely was, after the breach. We agree that encryption is a good thing—again, not a silver bullet. Encryption is a good thing. As the gentleman from Michaels mentioned, encryption is an expensive proposition. If we make this mandatory in the standard, there will be a number of merchants who will not be able to afford this immediately. There are provisions within the standard that actually affect what happens there. So the need for end-to-end encryption within the internal network is really not there. If you are following the standard religiously, the need is not there. Why put these people through the expense?

That being said, we are now investigating it from an independent third party, and we will present that information in the form of feedback to our entire community and get their feeling on whether or not they actually want this to be part of the standard.

Mr. LUJÁN. Mr. Russo, you said something earlier that I found interesting, that you have never found PCI not to be in compliance at a time of breach, meaning that at a time of breach, there may have been some break in compliance. But with the system that we have today, who is responsible for monitoring compliance?

Mr. RUSSO. The merchant himself. Basically what we do is we take a snapshot—let me give you a brief example, if I have a minute or so. If you need fire insurance on your house, and you come to me and ask me as the insurance company to give you fire insurance, I send an inspector out, and you have everything in place—smoke detectors that work, fire extinguishers, sprinklers, and such. Three months later, your house burns down. I send an inspector out again, only to find out that there was no pressure on the sprinklers at that time, all of the batteries weren't working in your smoke detectors, and so on. This is the responsibility not only

of the council to make sure that you are compliant, but it is your responsibility as a merchant, your responsibility to the consumers to make sure that you are doing this on a regular basis.

Mr. LUJÁN. Mr. Russo, if I could interrupt, I think that that example is a perfect illustration, because I would ask that the regulator that was responsible for monitoring the fire suppressant system, if you come back after there was a fire, and you found out that my fire suppressant system wasn't adequate to be able to protect my home or my place of business, then the regulator wasn't doing their job. But in this case, there is no one overseeing this. It is, here is a set of rules; if you want to be able to utilize our product, please follow them. In the case if there is a breach, we depend on the Department of Justice to step in, often times informing a group of people that maybe there was a breach.

Madam Chairwoman, I know that my time is expired, but this is really interesting to see, when we talk about a set of standards, to truly see how we can work together to look to see where the weak points are. But also from a compliance perspective, I know that there aren't compliance efforts moving forward to truly work with the retailers if it is their responsibility to be held in compliance. But it seems to me that the system that we have today, I think we all agree, from different sides, that it is not working.

Ms. CLARKE. Thank you very much for your observations, Mr. Luján. Thank you for your responses.

We are in the process of votes right now, but I would like to get in one final question for this panel, and this question is for the entire panel actually.

A large part of the data theft problem is the amount of valuable data stored in the system. Mr. Hogan and Mr. Jones testified that the credit card companies are actually requiring merchants to keep more data than they would otherwise prefer. Can the panel please explain what requirements exist for merchants to store credit card data in their systems, and why did the credit card companies dismiss the suggestion from NRF that these requirements be changed?

Mr. MAJKA. Madam Chairwoman, if I may start by answering that question. Visa does not require merchants to retain card holder data. We embarked on a campaign about 3 years ago to educate merchants on what data they absolutely need to maintain, and the campaign was called Drop the Data. In those cases, they are not required to retain the account number.

We have found that some merchants do, in fact, retain the account number, customer name, maybe the expiration date, and in those cases, should a merchant choose to maintain that data, they do have to secure it properly. But all merchants have the ability to work with their acquiring merchant bank to not store that data, and use whether it is an authorization code or transaction ID as a reference number to then research a transaction that may be in question. So from a Visa perspective, we do not require storage of that data.

Ms. CLARKE. Mr. Hogan.

Mr. HOGAN. That statement is quite interesting, because we hear from numerous, numerous merchants, restaurants, hotels that if they don't keep some credit card data for a period of time to handle

the retrieval or chargeback request process, they will be fined and penalized. So I would love to have somebody go on record here from Visa or so on and so forth that would basically make a statement that, again, retailers and merchants do not need to store any credit card data at all, just keep an authorization code, and they will not be penalized at all in context of the chargeback or retrieval request process. Maybe that could be a question you could pose back.

Ms. CLARKE. I find this discrepancy to be very troubling, very troubling.

Mr. Jones.

Mr. JONES. I think we have to look at two entities, too. As the question was being answered, there was Visa does not require. Then the second part was, we recommend they work with their acquiring merchant bank to understand what data they need to keep or don't need to keep.

Visa is not the person that we work with on a day-to-day basis. We work with our merchant bank. If your merchant bank cannot provide you back the information for you to look up among your thousands, tens of thousands, hundreds of thousands, or millions of transactions which we deal with on a basis to pull that transaction—and we have to physically pull a receipt again; we go from the point of we get a piece of paper with a card number on it, and we have to get to a point where we pull a receipt within a certain time period, otherwise we lose that transaction. So it is not a requirement. We could not do that. We could say that is a cost of doing business. By doing that, then, we would just automatically lose those dollars.

My brethren in places like Best Buy or Big Ticket, it would cost them a fortune. Places like Marriott, or a hotel or a car reservation where you hold a reservation with a credit card number, or they put a $400 charge on your credit card where it is being held but not charged yet, they do have to keep that; otherwise they have no way to charge you after.

So I think we are dealing with which organization is requiring versus PCI doesn't require you, they are not a credit card organization. Visa just transports it; the merchant bank is something else. The retailer is left holding the bag and has no input or say, but yet is paying the transaction fee, is the one who pays for the transaction when the customer says that they are not responsible for it and has no say in it.

There is a solution out there, but there has been no interaction, there has been no partnership to really develop that solution, I think.

Ms. CLARKE. Well, let me just close by saying that this is something that we have to fix. Mr. Majka, I look forward to speaking with you further about this.

To all of you, thank you very much for your testimony today. This has been very interesting, very enlightening. I think we have got a lot of work to do, as I said in my opening statement. Certainly I think some things have come to light here today that should concern all of us and that we should be working together as a team to make sure that we address.

I thank the witnesses for their valuable testimony and the Members for their questions. The Members of the subcommittee may

have additional questions for the witnesses, and we will ask you to respond expeditiously in writing to those questions.

Hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 3:15 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE OF NEW YORK FOR RITA M. GLAVIN, ACTING ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE

Question 1. How do you prosecute criminals in cyberspace when it is virtually impossible to identify and attribute attacks to specific individuals?

Answer. Response was not received at the time of publication.

Question 2. What attraction does card fraud have for criminals and terrorists?

Answer. Response was not received at the time of publication.

Question 3. Would you say that card fraud is the financing method of choice for terrorists?

Answer. Response was not received at the time of publication.

Question 4. How many people and man-hours are devoted to investigations and prosecutions related to card fraud, including both data breaches and the criminal activity card fraud underwrites?

Answer. Response was not received at the time of publication.

Question 5. You testified that by disabling Shadow Crew's Web site, the Department of Justice believed they "prevented hundreds of millions of dollars in additional losses to the credit card industry." Is it the Department's understanding that the fraudulent charges that are the result of a data breach are a financial liability to the card brands, issuing banks, or acquiring banks?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE OF NEW YORK FOR ROBERT RUSSO, DIRECTOR, PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS COUNCIL

Question 1. Why aren't penetration tests required on a quarterly basis? Why don't they conform to NIST standards?

Answer. The PCI DSS requirement for penetration testing is not based exclusively on time intervals. Tests are also required after any significant changes to a data system environment that has been validated as compliant with the PCI DSS—as frequently as that may occur, which may be more frequently than quarterly. The Council's information supplement regarding penetration tests is attached as Exhibit A.* This is in addition to the annual validation of static controls. It is also important to note that penetration tests are only a small part of the comprehensive set of controls and layers of security identified in the PCI DSS.

Vulnerability assessments, which share many of the characteristics of penetration tests by identifying the same threats, are required, at a minimum, quarterly. Penetration tests are additive to, rather than substitutes for, the standards promulgated by the National Institute of Standards and Technology (NIST), which are also a critical part of the process that our Approved Scanning Vendors (ASVs) utilize to identify vulnerabilities in networks. Indeed, all ASVs rely on the NIST National Vulnerability Database *(http://nvd.nist.gov/),* a U.S. Government repository of standards-based vulnerability management data and each entity must receive a passing score quarterly to be considered compliant with the PCI DSS.

Question 2. Given the prevalence of insider attacks (both physical and virtual), which have grown by 55% according to the intelligence community, why has two-factor authentication not been required of all users who access payment data within networks as well as all system administrators' who have privileged rights?

Answer. The PCI DSS requires two-factor authentication (Requirement 8.3) as a mechanism for external access (internet/remote) into cardholder data environments. The primary focus of PCI DSS Requirement 8.3 is to prevent unauthorized access from the outside, focusing on protecting from external intrusion, not internal access.

* Attachments referred to have been retained in committee files.

For internal threats with respect to unauthorized authentication attempts, the PCI DSS provides a layered security approach that requires numerous other controls to minimize risks within the internal network. Two-factor authentication is one method for meeting this layered approach. Other approaches that address the internal risk of user account takeover include prohibiting the use of risky protocols that expose user names and passwords (Telnet and FTP) and requiring passwords to be encrypted/hashed during transmission and storage within the internal network. There are also numerous user account management and password controls (Requirement 8), along with logging and monitoring requirements (Requirement 10) that address internal controls to help mitigate internal risks including two-factor authentication.

Question 3. How are Qualified Security Assessors trained?

Answer. Because the quality of PCI DSS validation assessments can have a tremendous impact on the consistent and proper application of security measures and controls, the Council's QSA qualification requirements are exacting and detailed, involving both the security companies themselves as well as the individual employees involved in assessments.

In broad terms, prospective QSA companies must:

- Apply for qualification in the program;
- Provide documentation adhering to the Validation Requirements for Qualified Security Assessors v. 1.1, a copy of which is attached as Exhibit B;*
- Qualify individual employees to perform the assessments, which requires annual training and testing of those employees, and;
- Execute an agreement with the Council governing performance of validation assessments.

In turn, each individual QSA employee who will be performing and/or managing on-site PCI DSS assessments:

- Must attend annual PCI DSS training provided by the Council, which includes training in Scoping a PCI DSS Assessment, PCI DSS v1.2 Requirements, and Compensating Controls;
- Must pass all examinations conducted as part of training;
- Has access to face-to-face feedback sessions with the Council every 6 months;
- Has access to the numerous fact sheets, information supplements, frequently asked questions, and webinars that the Council makes publicly available at its Web site at *www.pcisecuritystandards.org/education.*

Our management of QSAs does not end with training. In 2008, the Council launched a Quality Assurance program to promote consistency of both services and results provided by the security assessment community. This program specifies eight guiding principles QSAs must commit to and outlines a number of criteria QSAs must adhere to in order to provide a more uniform experience for merchants and other customers. The criteria include evaluating QSAs based on consistency of the opinions rendered, competency of the professionals, credibility of the organizations, and business ethics. To staff this program, the Council has also invested in a dedicated team responsible for assessor performance monitoring.

Each assessor is required to use the template report associated with the PCI DSS (attached as Exhibit C*) as the framework for reporting validation to the standard. Each requirement contains one or more testing procedures that must be evaluated by the assessor and appropriately documented to demonstrate that the control has been tested by the QSA and is operating correctly. The quality assurance team reviews these reports to confirm that all testing procedures in the framework are completed and documented, indicating consistency of practice in the assessor community.

The Council's quality assurance team evaluates trends among Report of Compliance documents in an effort to identify common inconsistencies and reports findings to the Council in order to consider and implement appropriate curative actions. Any such actions are communicated to the assessors via training, newsletters, and webinars. This information is also shared with the Council's Technical Working Group for future consideration and possible adjustment of the PCI DSS.

Question 4. Mr. Jones of Michaels Stores stated that "Many of the PCI requirements are covered by the Sarbanes-Oxley audits." Could you report to the committee on the redundancies between the Sarbanes-Oxley audits and the PCI Council's own requirements?

Answer. The Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley") applies exclusively to publicly traded companies in the United States, addresses a host of concerns and is not primarily concerned with data security. Sarbanes-Oxley instead focuses primarily on addressing accounting standards and practices. The provisions of Sar-

* Attachments referred to have been retained in committee files.

banes-Oxley are not intended, nor would they be adequate, to enable the marketplace to achieve and maintain data security, particularly with respect to payment card data. The Council does not believe there is extensive overlap between Sarbanes-Oxley and PCI Standards.

The PCI Standards are specifically designed to protect payment card data. They apply to both public and private companies of all sizes, both inside and outside the United States. Further, they are far more detailed and specific in the way they address data security issues: for example, the PCI DSS has over 225 requirements and 525 testing criteria specific to data security.

Given the specific nature of the PCI DSS and the absence of similar specific controls in Sarbanes-Oxley, we are unclear about precisely what redundancies Mr. Jones is referring to.

Question 5. You testified that the PCI council does not develop or use metrics to evaluate the effectiveness of the council's standards. How then does the council weigh proposals to the PCI standards if they cannot measure the costs and benefits of past and future additions to the standards?

Answer. There are a number of readily available industry metrics that the Council uses to track the effectiveness of the standard. For example, the *Nilson Report* is a widely used industry publication with extensive metrics on payment card fraud and a wide range of other data security issues.

Moreover, the payment card brands regularly receive and assess forensic information regarding the cause of payment card data breach incidents. This type of data provides critical information regarding where the PCI Standards may need to be strengthened or modified. This guidance is provided by the payment card brands as members of the Council's technical working group.

Proposed changes to the PCI Standards are shared with our Participating Organizations, which represent over 500 companies, all of which have first-hand experience in implementing standards and protecting payment card data on a daily basis. A formal feedback process enables the Council to receive robust feedback from this group. This feedback ensures additions and changes to the PCI Standards are weighed by those with a front-line perspective on what measures are most beneficial to protect payment card data.

One example of how this broad industry feedback has directly resulted in changes to the PCI Standard is in the case of wireless security. In 2007, forensic investigators indicated that insecure wireless implementations were at the core of a number of breaches. As a result of that, the Council started investigating wireless security with its stakeholder community—making it a key agenda item for discussion at our first Community Meeting. Feedback from that discussion led to changes in version 1.2 of the PCI DSS. Finally, in order to help organizations meet the new requirements, our stakeholders suggested creating a Wireless Special Interest Group—comprised of representatives from dozens of our Participating Organizations—to examine implementation issues. That group is expected to release an implementation guide on meeting the new wireless requirements in the coming weeks.

It is broad participation such as this—coupled with the knowledge that the payment brands bring to the table—that gives us confidence in our ability to measure the cost and benefits of future additions to the standard.

Question 6. You stated in your testimony that "no standard is perfect. But the PCI security standards have proven to be the most effective means of preventing data breaches and protecting consumers." Given that the Council has not developed or applied any metrics to measure the effectiveness of the PCI standards or to compare their resulting security to other payment technologies, how have the PCI security standards proven to be effective at all?

Answer. Necessarily, evidence demonstrating that a particular standard is effective in preventing a particular outcome must be inferential. However, it is noteworthy that with more than 10,000 payment card transactions per second worldwide (Source: American Bankers Association, March 2009) and the usage of payment cards steadily increasing, payment card fraud rates are at historic lows. The Council believes that the PCI Standards have been an integral driver of this trend, and industry data supports that conclusion.

Question 7. You stated that the council does not have a relationship with banks "other than to put the standard out there and make sure that they are creating awareness among their constituents." Since it is the banks which, according to you, monitor compliance and the effectiveness of the standards, should not they be central to the drafting process?

Answer. My statement pertained to lack of a direct contractual business relationship between the Council and the banks. It was not intended to suggest that banks are not intimately involved in data security standards. Any suggestion to the contrary was inadvertent.

Banks are a pivotal part of our organization. Over 40 financial institutions worldwide—including such leading U.S. banks as Bank of America, Capitol One, and Wells Fargo—have joined the Council as Participating Organizations. These organizations receive draft copies of the PCI Standards for comment prior to publication and have the opportunity to contribute feedback during the drafting process. Financial institutions also comprise nearly one-quarter of the Council's elected Board of Advisors.

Question 8. Merchants who have experienced data breaches also face significant class action lawsuits. What liability exists for the payment card industry and the assessors if a PCI-compliant company is breached?

Answer. The PCI Standards do not assign liability to any party in the event there is a data breach. Any liability from a data breach would arise from agreements between participants in a network and/or applicable law.

Consistent with its role as a standards development organization, as discussed above, the Council does not impose any liability allocation requirements between assessors and merchants, nor does it have knowledge of the contractual terms entered into between individual payment card brands (who are competitors of each other) and their industry partners. Consequently, the Council does not have special insight into how any liability for payment card breaches is allocated.

Question 9. In response to the committee, JCB said that they expect the PCI standards will continue to "become even more stringent in future iterations." Is this also your expectation? What changes will the next iteration likely have?

Answer. At this point in our standards lifecycle process, we are not in a position to predict what specific changes will be included in the next major iteration of the PCI Standards—our open comment period for the most recent release starts in July. This comment period is a pivotal part of a rigorous, end-to-end review undertaken within a 2-year lifecycle process that includes input and feedback periods for our Participating Organizations. Any changes introduced to meet new and evolving threats will be debated with all of our stakeholders before release.

In order to address interim threats, as previously noted in my written testimony, the Council maintains on-going two-way communications with its assessors, merchants, and other stakeholders, and has the ability to issue errata to the PCI DSS, flash bulletins on emerging threats, monthly newsletters to the Assessor community, regular updates to the ASV test scanning environment, monthly webinars with both assessors and merchants, and updates to the Council's on-line searchable FAQ and training materials.

Question 10. Currently, requirements of notification of breaches vary from State to State. Given that the Department of Justice stressed the importance of notification, both of law enforcement and consumers, has or will the Council consider mandating notification as part of its standards? How would or could that be enforced?

Answer. As a standards body, the Council has no direct contractual power that would enable it to mandate or enforce such notification by retailers or processors when they suffer a breach. Although we do not have the power to require notification, each of our members feels strongly that notification of law enforcement and affected consumers is an important component in a security breach response plan.

In fact, PCI DSS Requirement 12.9.1(b), which addresses Incident Response, requires entities to have a communication and contact strategy in the event of data compromise as well as an analysis of legal requirements for reporting compromises.

Question 11. You stated in your testimony that "in fact, we have never found a breached entity to have been in full compliance with the PCI standards at the time of a breach." Can you please explain the discrepancy between that statement and the statement of Ellen Richey, Chief Enterprise Risk Officer at Visa, Inc., that Heartland had validated PCI compliance "but it was a lack of ongoing compliance and ongoing vigilance in maintaining security that left them vulnerable to attack". Can you please explain exactly how Heartland was not in full compliance with the PCI standards?

Answer. These two statements are consistent. As noted in my written testimony, validation of compliance with the PCI DSS only represents a snapshot in time that coincides with information shared with and interpreted by a QSA during the assessment period. No entity that has custody of customer data can afford to gear up for an assessment, and then relax its vigilance thereafter. While assessment is a useful tool to uncover vulnerabilities, stakeholders across the payment chain must realize that data security, and not passing assessments, is the goal of an effective compliance program. The 2009 Data Breach Investigations Report from Verizon Business (attached as Exhibit D*) found that effective tracking and monitoring of network access was not in place at 95% of breached entities at the time of compromise. This

* Attachments referred to have been retained in committee files.

provides a good example, because the tracking and monitoring requirement is a security practice that requires on-going compliance to be effective. Its value is severely limited if it is in place only during validation of compliance to the PCI DSS.

Unfortunately, the dynamic nature of any organization's complex information technology systems and network environments, as well as turnover of human resources, can require the taking of a wide variety of actions that, absent appropriate steps to restore system integrity can render a validated system noncompliant quickly after a satisfactory compliance report has been issued. To use an analogy, effective compliance should be viewed as equivalent to a full-length feature film where an organization must be "compliant" at each and every frame of that film. In contrast, validation of compliance is determined by a QSA only in a single, specific frame of that film.

Question 12. Mr. Majka of Visa stated in his testimony that "security must be a shared responsibility among all relative parties—law enforcement, payment companies, regulatory agencies, retailers and others." How is the financial risk and liability shared between these parties?

Answer. The Council is not involved in the allocation of risk within a particular network. This question is better directed to participants in the respective networks, including the networks themselves.

Question 13. Mr. Majka of Visa stated that "we must collectively apply multiple layers of security to protect the system. That includes measures applied at the card level such as card verification values." It is the committee's understanding that not all issuing banks are required to support CVVs and not all transactions are required to include CVVs. Can you explain how the Council develops and enforces standards for the card brands and issuing and acquiring banks?

Answer. It is important to recall, as noted above, that the Council manages and develops—but does not enforce—the PCI Standards, nor does it enforce operational regulations imposed by the payment brands. Instead, it makes standards available to the market as tools to be used in order to protect the payment card data of any entity that stores, transmits, or processes payment card data. Members of the payment chain then individually decide which industry partners must comply with the PCI Standards, define required compliance validation mechanisms, and manage any enforcement programs that may exist.

Requirements that exist between individual card brands and their issuing and acquiring banks are not within the Council's purview.

Question 14. According to Mr. Jones' testimony, PCI states that all credit card data must be encrypted, with the exception that it need not if the data travels over a private network. Nonetheless, Mr. Jones says in spite of that his company does not send this information over their own private network unencrypted. Surprisingly, he notes, "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!" And Mr. Jones' company has to re-encrypt this data when it is sent back to its stores. As a result of his company's strong objection to this policy, it has asked for the past 3 years for the ability to send encrypted information to the banks but nothing has happened. One reason given is that it is too expensive to implement. Mr. Jones has been told if the retailers "are willing to pay the costs (i.e., the credit card banks' cost) to implement it, we will consider it."

How important is the cost to the credit card banks in your analysis?

Answer. Cost to all stakeholders, including merchants is one of many factors that are taken into account in considering changes to the PCI Standards. Effective data security must be affordable to the millions of participants in the payment chain that must invest in it or they cannot be expected to act quickly and effectively enough to meet on-going threats. Any effective security stance must therefore realistically take cost into account. For example, our Participating Organizations, and particularly our merchant Participating Organizations, have told us that internal encryption would be extremely—even prohibitively—expensive, and have urged us to pursue more affordable, alternative ways to make further security advances in this area.

Question 15. Can you explain your process for evaluating Mr. Jones' 3-year effort to be able to encrypt information to the banks? Also, who has opposed this suggestion?

Answer. Until our introduction at the hearing, Michaels Stores, Inc. ("Michaels") had not presented its opinions regarding this issue to the Council. Moreover, Michaels is not a Participating Organization and so to date has not attended any of our community meetings or feedback sessions in the almost 3 years since the Council's inception. The Council had therefore not had any prior opportunity to evaluate

the Michaels suggestion, nor is it aware of who may or may not be supportive of this suggestion. The Council would welcome Michaels as a Participating Organization so that its views could be heard and debated among our stakeholder community.

Question 16. A large part of the data theft problem is the amount of valuable data stored in the system. What requirements exist for merchants to store credit card data in their systems? Please explain how the chargeback/retrieval process affects what kinds of data can or should be stored on a merchant's system.

Answer. The Council is not involved in the assessment of the chargeback and retrieval process. Those processes are dictated by participants in the payment network and those participants are therefore in a better position to respond to the question, and speak to the necessity of various kinds of data in connection with the chargeback/retrieval process.

To more broadly answer the question of what data merchants are required or permitted to retain, the fundamental premise of PCI DSS is "if you don't need it, don't store it." That is why requirement 3.1 of the PCI Data Security Standard stipulates that organizations should only retain data that is required for business, legal and/or regulatory purposes. In other words, the PCI DSS does not itself mandate that merchants retain any specific kind of data. To the extent card data must be stored for legitimate purpose, it must be stored in a secure manner.

Question 17. Why do card brands require merchants to retain cardholder data for the purpose of chargebacks? Since this is such vulnerability for merchants and cardholders, why not mandate that no cardholder data be retained and provide transaction IDs for the purpose of chargebacks?

Answer. As noted above, the Council is not involved in the chargeback process.

Question 18. Why does the PCI Council not mandate PINs for credit card transactions?

Answer. What data is presented in a transaction is part of the authorization format used by the payment systems. Since the Council is a security standards body, we are focused on providing standards to secure payment data within the current payment system. The Council has nothing to do with authorization format requirements or the authentication of a transaction at the point of sale. The Council does not run a payment network, nor do we have influence over vendors' product platforms.

If the system evolves to mandate PINs for all transactions, the Council will then address the issue of how to best provide the market with any necessary standards to secure this process. For example, the Council already maintains a comprehensive standard for PIN Entry Devices. This standard lists requirements that address physical and logical requirements for devices that process PIN transactions and would likely be an integral part of securing PINs if they were to be used more broadly in authentication.

Question 19. The basic design and security model of credit cards has not changed since the 1950s. What major investments would be required for a large scale migration to a different payment technology? Who would make those investments? For example, if we were move to a chip and PIN system?

Answer. The design and security model of payment cards has changed extensively since the 1950s. Advances have included advanced hologram technologies, on-line authorizations, Card Verification Codes, 3–D Secure, address verification, real-time heuristic fraud detection solutions, on-line PIN and off-line chip & PIN. This is just a sample.

However, any migration decisions are driven by the underlying value proposition, which may differ from market to market and vary by payment brand. The Council in its role as a standards body does not have insight into these elements.

Question 20. Your responses to the committee concerning adopting technological changes to the PCI standards, such as the end-to-end encryption embraced by other witnesses, seems to be: (1) We have addressed this issue ["there are provisions within the standard now that address this data, address the inside network that should, in fact, . . . stop this from happening . . . "]; or (2) it's unnecessary to address this issue ["so the need for end-to-end encryption within the internal network is really not there."]; or (3) we are considering addressing this issue ["we have issued a proposal to a number of technology companies to give us an independent study on what we are calling emerging technologies, one of which is end-to-end encryption."]. Given the skepticism toward Visa and the PCI Security Standards Council expressed by the other members of the panel, can you point to specific actions you are taking that will reassure this committee that you are approaching the adoption of end-to-end encryption and other security-enhancing solutions with the degree of urgency and level of seriousness warranted by the current threat?

Answer. The introduction of any new technology—whether it is end-to-end encryption or other security enhancing solutions such as virtualization and tokenization—is a matter of utmost importance to the Council and is treated as a high priority. We are constantly evaluating the potential uses of new technologies to improve the security of payment card data. As noted in your question, we have issued a proposal to a number of technology companies to research and submit to us an independent study of emerging technologies, one of which is end-to-end encryption. As discussed further in the response to Question 21 below, we expect to commission that study in the coming weeks. The issuing of this technology study demonstrates the Council's commitment to examining the relevance on an on-going basis of technologies such as encryption to the PCI Standards.

It is important to note, however, that the message from our stakeholders regarding end-to-end encryption has been mixed. During the last feedback period in 2007, we received input from more than 350 organizations. It is noteworthy that not a single organization requested that end-to-end encryption be mandated or even examined. Our Board of Advisors has similarly not requested an examination of end-to-end encryption.

Question 21. What technology companies are providing these "independent" studies of emerging technologies? Mr. Jones testified that end-to-end encryption is not an "emerging" technology. If that is correct, what do these companies need to study with regard to end-to-end encryption?

Answer. The Council conducted an RFP process for selecting a vendor to assist in the technology study. We are currently in the negotiation process with the finalist—one of the major public accounting firms. Our RFP asked vendors to examine the impact that emerging technologies—including end-to-end encryption as well as technologies such as virtualization and tokenization—might have on the PCI Standards, and how broad adoption of these technologies might serve to simplify the process of securing payment card data.

To Mr. Jones' point, while encryption itself is not a new technology, no standard currently exists on how to apply end-to-end encryption in a comprehensive data security framework.

Question 22. Visa asserts that consumers bear zero legal liability for fraudulent use of credit cards. How is this policy financed?

Answer. Council members understandably avoid discussing any matters that might in any way relate to the pricing and financing models of the individual payment brands, and the Council accordingly does not address such areas. This question is best directed to Visa, but we do note, that U.S. Pub. Law 93–495 (commonly referred to as "Reg E") protects a consumer against fraud in excess of $50.

Again, I appreciate the opportunity to assist the committee in this matter, and support its goal of reducing the number and impact of data security breaches. The Council remains available to provide the committee with information to more fully understand and address cybersecurity concerns as they relate to the PCI DSS and other payment chain-related standards for which the Council has responsibility.

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE OF NEW YORK FOR W. JOSEPH MAJKA, HEAD OF FRAUD CONTROL AND INVESTIGATIONS, GLOBAL ENTERPRISE RISK, VISA, INC.

Question 1. The PCI requirements are directed solely at merchants and retailers. Why shouldn't there be a prescriptive security mandate for Visa or other payment card brands to secure your own networks?

Answer. The PCI Data Security Standard (PCI DSS) applies to all entities that store, process, or transmit payment cardholder data, including financial institutions, processors, third party service providers, and merchants. Visa, Inc. has validated and maintained on-going PCI DSS compliance on an annual basis using an independent qualified security assessor (QSA) since the creation of the PCI DSS in 2006. In addition, Visa, Inc. adheres to more rigorous security measures to protect the overall Visa payment system. Visa is subject to oversight by U.S. regulatory bodies under the auspices of the Federal Financial Institution Examination Council (FFIEC) and undergoes regular reviews by the FFIEC.

Question 2. Given the central role the card brands play in the American economy, what responsibilities do you believe they have to consumers and to the Nation?

Answer. Securing consumer data within the U.S. economy is a shared responsibility, and every industry should deploy focused resources to protect consumer information within its care. In this regard, the payment card industry has done more than any other to provide stakeholders with the tools and guidance needed to properly secure the data they are trusted to protect. Visa has led the industry in protecting cardholder data and stands ready to continue to support industry partici-

pants in our collective fight against the criminals that perpetrate card fraud. Thanks to massive investments and innovative solutions, compromise events rarely result in actual fraud and fraud rates in the payments industry remain near all-time lows.

Question 3. Is a breached company (whether compliant with the PCI Standards or not) subject to increases in interchange rates?

Answer. Visa does not increase or modify the interchange rate structure that applies to an entity that is breached. In fact, since October 1, 2007, to encourage and provide incentives for stronger protection against data breaches, acquiring financial institutions have been able to qualify transactions for lower interchange rates under the "tiered" interchange rate system by, among other best practices and volume requirements, ensuring that their merchant customers comply with the PCI DSS. Acquirers of merchants that have been compromised and are found not to have been in compliance with the PCI DSS may therefore lose the benefit of these incentive-based "tiered" interchange rates, until they demonstrate that they have come into compliance.

Question 4. In responses to the committee's investigation, you stated that "while there have been a few instances where an entity with previously validated PCI DSS compliance was the victim of a compromise, in all compromise cases our review concluded that gaps in the compromised entity's PCI DSS controls were major contributors to the breach." What gaps are normally found in a victim's security controls after they have been certified PCI compliant, but later found to be out of compliance?

Answer. In all compromised cases within Visa's purview, third-party investigations concluded that gaps in the compromised entity's PCI DSS controls were major contributors to the breach. Gaps commonly include failures to secure and monitor non-payment-related systems that are connected to the payment environment, which are then targeted to gain access to the network. Corporate Web sites are an example of non-payment-related systems commonly targeted by criminals through Structured Query Language (SQL) injection attacks. Another common gap is insufficient monitoring of logs for firewalls, anti-virus, intrusion detection systems, as well as monitoring of privileged user accounts. The PCI DSS requires that not only should there be mechanisms in place to monitor for intrusions, but also that the organization regularly monitors the logs generated to identify and investigate anomalous activity.

Visa works with its acquiring financial institutions, through its compliance programs to ensure merchants and their service providers achieve and maintain PCI DSS compliance. It is the responsibility of the acquiring financial institution, which deals directly with their merchants and their service providers, to ensure these entities continue to eliminate unnecessary risk to the overall payment system. To determine overall success of these measures, Visa actively requests frequent reporting from its acquiring financial institutions on the status of the PCI DSS compliance of their merchants and service providers. In support of these compliance programs, Visa has actively communicated, since 2006, common vulnerabilities and corresponding mitigation measures that merchants and service providers mistakenly leave susceptible to attack on their systems. In addition, Visa provides other data security alerts, bulletins and webinars to payment system participants, all publicly available at *www.visa.com/cisp.*

Validating PCI DSS is a major milestone, but achieving and maintaining compliance requires companies to make an on-going commitment to keeping all consumers' data safe, including cardholder data—24 hours a day, 7 days a week, 365 days a year. For any standard to be effective, however, organizations must rigorously ensure that they comply with each of its requirements on an on-going basis. Verizon Business' 2009 Data Breach Investigations Report affirms similar findings, "The majority of breaches still occur because basic controls were not in place or because those that were present were not consistently implemented across the organization." Further, the report specifically attributes non-compliance to PCI DSS requirements as major factors contributing to breaches. Verizon cites PCI DSS Requirements 3 (protect stored cardholder data), 6 (develop and maintain secure systems and applications), and 10 (track and monitor access to network resources and cardholder data) as the least compliant across their caseload, saying, "This trio of deficiencies factored heavily into many of the largest breaches investigated by our team over the past five years."

Question 5. Mr. Russo of the PCI Council stated in his testimony that "in fact, we have never found a breached entity to have been in full compliance with the PCI standards at the time of a breach." Can you please explain the discrepancy between that statement and the statement of Ellen Richey, Chief Enterprise Risk Officer at Visa, that Heartland had validated PCI compliance "but it was a lack of on-going

compliance and on-going vigilance in maintaining security that left them vulnerable to attack". Can you please explain exactly how Heartland was not in full compliance with the PCI standards?

Answer. In all compromise cases within Visa's purview and as stated by Mr. Russo, despite any validation that may have been completed by a QSA, the breached entity was not found to have been in full compliance at the time of the breach. Based on compromise event findings, Visa removed Heartland from its list of PCI DSS compliant service providers. Information related to Heartland's PCI DSS compliance status was provided to Visa under the obligations of a confidentiality agreement. As such, Visa suggests contacting Heartland directly for specifics.

Question 6. You stated in your testimony that Visa looks forward to "working with all participants to continue to develop tools to minimize the risk and the impact of data-compromise events." Does Visa understand the committee's concern about a fraud prevention strategy that minimizes fraudulent charges only to the extent that card brands and issuing banks remain solvent when fraudulent charges finance criminal activities?

Answer. Visa's goal is to prevent both card data compromises and the subsequent potential for fraudulent transactions. Visa has been executing a multi-layered security strategy working with all payment system participants to prevent data compromises around the world as well as the fraud that may result there from. Visa invests substantial resources and leads innovation in the industry with measures to stay ahead of criminals and prevent them from obtaining financing through the payment system. This includes, for card-based solutions (e.g., EMV-chip, contactless), data-based measures (e.g., PCI DSS), and network-based technologies (e.g., Advanced Authorization, neural networks, Address Verification Service). In addition, participants in the Visa system should strictly adhere to the EFT Act and Reg. E, the Truth in Lending Act and Reg. Z, as well as numerous other Federal regulations that protect consumers from the consequences of data breaches and fraud. Additionally, Visa is currently working to empower cardholders to play a more active role in protecting their information through innovations such as transaction alerts. Armed with this kind of information, cardholders can help monitor usage on their accounts and identify potential fraud. All of these measures are designed to prevent criminals from obtaining card data, and to prevent them from using it to commit fraud.

Question 7. Merchants who have experienced data breaches also face significant class action lawsuits. What liability exists for the payment card industry and the assessors if a PCI-compliant company is breached?

Answer. Parties that experience data breaches may be subject to the liabilities determined through the court system. Visa is aware of a number of class action lawsuits related to major data breaches in the United States. However, Visa cannot speculate about facts and outcomes in potential or pending class action lawsuits. To our knowledge, no organization that has fully implemented and maintained compliance with the PCI DSS has been the victim of a data compromise event. These breaches damage consumer trust in the overall electronic payment system, including Visa and its brand.

Question 8. In response to the committee, JCB said that they expect the PCI standards will continue to "become even more stringent in future iterations of the PCI standards." Is this also your expectation? What changes will the next iteration likely have?

Answer. The PCI SSC is charged with reviewing and updating the PCI DSS to ensure that it remains effective to protect card data, by incorporating input from stakeholders as well as technological developments in the evolution of the standard over time. Since its creation, the PCI DSS has been formally updated three times, with considerable input from over 500 participating organizations, including merchants, banks, and service providers from around the world, in order to meet the evolving threats to the system, changing technologies and the increased sophistication of hackers. The updates introduced in version 1.1 and 1.2 of the PCI DSS have been relatively minor changes, most of which served as clarifications to help entities better understand the intent of a requirement. We expect the standard will continue to evolve to address new threats as they materialize and add further specificity where participating organizations, including many global merchants, provide feedback.

Question 9. Currently, requirements of notification of breaches vary from State to State. Given that the Department of Justice stressed the importance of notification, both of law enforcement and consumers, has or will the Council consider mandating notification as part of its standards? How would or could that be enforced?

Answer. PCI DSS Requirement 12.9.1 addresses incident response and requires entities to have a communication and contact strategy in the event of data com-

promise. Additionally, in the event of a compromise Visa advises entities to follow all State and Federal disclosure requirements. Visa also works closely with the Federal Bureau of Investigation's Cyber Division, United States Secret Service, United States Postal Inspection Service, State attorneys general and the Department of Justice Cybercrime and Intellectual Properties Unit in criminal cases of data compromises.

Question 10. You stated that "security must be a shared responsibility among all relative parties—law enforcement, payment companies, regulatory agencies, retailers and others." How is the financial risk and liability shared between these parties?

Answer. Financial institutions have the direct responsibility and relationship with cardholders, and because of Federal law and Visa's zero liability policy for cardholders, bear most of the financial loss if fraud occurs. Visa's Account Data Compromise Recovery program allows issuing financial institutions to receive reimbursement for counterfeit fraud losses and a portion of their operating expenses incurred as a result of data compromise events from the financial institution responsible for the compromised entity in the Visa system.

Question 11. Mr. Jones of Michaels Stores stated in his testimony that "credit card companies' financial institutions do not accept encrypted transaction." The committee is concerned that the PCI Council is not applying the same standards to its members that it applies to merchants and processors. Is Visa planning to move forward with securing the communications channel between merchants and financial institutions?

Answer. Visa accepts encrypted data transmissions from its processing endpoints and many processors also accept encrypted data transmissions for merchant transaction submissions. Visa is also mandating use of stronger encryption for protection of PINs at every point of sale globally, specifying use of Triple Data Encryption Standard (TDES) for PIN accepting entities. While the PCI DSS requires encryption over public networks including the internet, it does not require the use of encryption over private networks, such as a merchant's internal network or a private connection between a merchant and processor. Encrypting cardholder data in-transit over private networks is encouraged. It should be noted, however, that while encryption can add an additional layer of security, the data is still at risk if transactions must be decrypted at any point within the private network—for example, for transaction processing—and must still be properly protected. As such, many organizations have determined that the costs and number of system and software modifications needed outweigh any incremental security benefit. The requirements outlined currently in the PCI DSS, when implemented properly, should effectively prevent a criminal from obtaining access to a business' private network and detect any unauthorized access.

Question 12. The basic design and security model of credit cards has not changed since the 1950s. What major investments would be required for a large-scale migration to a different payment technology? Who would make those investments? For example, if we were move to a chip and PIN system?

Answer. In the 50 years since the beginning of the card industry, Visa has evolved from credit card roots to become one of the world's leading global retail electronic payments networks. Today, the Visa network connects cardholders, merchants, and financial institutions around the world with products and services that are designed to make payments faster, more convenient, more reliable, and more secure. At the heart of Visa's business is VisaNet, our centralized processing platform and one of the world's largest transaction and information processing networks. Nearly 92 billion authorization, clearing, and settlement transactions were processed through VisaNet in calendar year 2008. On this platform, Visa has been able to build capabilities that provide secure, reliable, and scalable processing, including innovations such as Advanced Authorization to risk-score transactions in real time. Other examples of technological improvements include the introduction of magnetic stripe technology, CVV2 (three-digit code on the back of a Visa card), address verification service and contactless cards with dynamic data technology. There have also been anti-counterfeit measures such as holograms, ultra-violet marks, and micro text, to name a few. Fraud rates today are at historic lows, much lower than they were decades ago when we did not fully benefit from the power of the Visa network to be able to analyze and authorize transactions in real time.

Visa supports chip technologies around the world, including in the United States where we are beginning to see adoption in mobile and contactless payments. Chip technology—both contact and contactless—can add an important security layer, introducing dynamic data into transactions which can reduce the incidence of fraud. However, we recognize that there are different needs, threats, and infrastructures in different parts of the world, and there is no one-size-fits-all chip solution. In some

other countries around the world, the market has driven the adoption of chip technology based on these factors. To the extent chip adoption can meet the needs of the payments industry in the United States, Visa is ready to support migration as it has in other markets. Where chip technology has been implemented broadly in a market, it should be noted that migration takes time. The costs have been shared by all parties—payment networks, financial institutions, and merchants. Generally, the card brands make investments in the network upgrades and consistent standards and financial institutions and merchants typically bear the increased cost of card technology and the upgraded payment terminals.

Question 13. A large part of the data theft problem is the amount of valuable data stored in the system. What requirements exist for merchants to store credit card data in their systems? Please explain how the chargeback/retrieval process affects what kinds of data can or should be stored on a merchant's system.

Answer. Visa does not require merchants to store complete card numbers. To the contrary, Visa encourages merchants to limit retention to truncated account numbers and has executed a "drop the data" educational campaign in partnership with the U.S. Chamber of Commerce over the past 3 years to encourage merchants to reduce data storage *(www.dropthedata.com).* A merchant may work with their acquiring financial institution to implement the necessary chargeback processes that do not rely upon the merchant's storage of the account number. For example, a signed point-of-sale terminal receipt with a truncated account number and the accompanying authorization log is valid fulfillment and will remedy a fraud chargeback. As such, a merchant may mitigate their risk by storing only truncated account numbers. In many cases, merchants decide to store cardholder data for marketing, loyalty programs, or customer service purposes. In those instances, Visa requires that stored data is protected in accordance with the PCI DSS.

Question 14. In responses to the committee, Discover stated that it is currently making changes to processes to provide merchants with the option of receiving masked data for disputes (like retrievals and chargebacks) as well as settlement reports. Is Visa doing something similar? Would this cut back on the amount of data stored that could be subject to breach?

Answer. Visa does not require merchants to store complete card numbers. Visa continues to work with those financial institution clients that may be requesting card numbers for dispute resolution to eliminate this practice and adopt the use of truncated account numbers. While Visa strives to eliminate any practices that may lead to the storage of cardholder data, there are likely many other reasons merchants have made a business decision to store this data, including processing returns and loyalty programs. In addition to our efforts to limit retention of complete account numbers, Visa has made considerable strides toward eliminating the storage by merchants and processors of authorization data, which criminals covet to perpetrate fraud. This "prohibited" data includes full magnetic stripe data, the CVV2 or "Card Verification Value 2" and PIN.

Question 15. Visa asserts that consumers bear zero legal liability for fraudulent use of credit cards. How is this policy financed?

Answer. Visa card-issuing financial institutions are responsible for complying with Federal law and honoring Visa's zero liability policy for cardholders and, as a result, bear most of the financial loss if fraud occurs.

In closing, Visa is acutely focused on ensuring that payment products are not used to perpetrate criminal activity and has taken a leading role in promoting cardholder information security and innovation within the payments industry. I appreciate the opportunity to assist the committee in this matter.

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE OF NEW YORK FOR MICHAEL JONES, SENIOR VICE PRESIDENT AND CHIEF INFORMATION OFFICER, MICHAELS STORES, INC.

Question 1. How much does it cost you to comply with the PCI standards, and are they effective in keeping out intruders?

Answer. Response was not received at the time of publication.

Question 2. Are retailers bearing a disproportionate burden of costs in data security?

Answer. Response was not received at the time of publication.

Question 3. Do you agree that the effectiveness of data security standards is inherently limited by the technology base of U.S. credit and signature debit card processing networks? How could this technology base be improved, and what obstacles exist that would prevent this from happening?

Answer. Response was not received at the time of publication.

Question 4. Have you ever notified the Council of assessors trying to sell their own products or services?

Answer. Response was not received at the time of publication.

Question 5. The basic design and security model of credit cards has not changed since the 1950s. What major investments would be required for a large-scale migration to a different payment technology? Who would make those investments? For example, if we were move to a chip and PIN system?

Answer. Response was not received at the time of publication.

Question 6. A large part of the data theft problem is the amount of valuable data stored in the system. What requirements exist for merchants to store credit card data in their systems? Please explain how the chargeback/retrieval process affects what kinds of data can or should be stored on a merchant's system.

Answer. Response was not received at the time of publication.

Question 7. Visa asserts that consumers bear zero legal liability for fraudulent use of credit cards. How is this policy financed?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE OF NEW YORK FOR DAVID HOGAN, SENIOR VICE PRESIDENT, RETAIL OPERATIONS, AND CHIEF INFORMATION OFFICER, NATIONAL RETAIL FEDERATION

Question 1. Are retailers bearing a disproportionate burden of costs in data security?

Answer. Response was not received at the time of publication.

Question 2. Do you agree that the effectiveness of data security standards is inherently limited by the technology base of U.S. credit and signature debit card processing networks? How could this technology base be improved, and what obstacles exist that would prevent this from happening?

Answer. Response was not received at the time of publication.

Question 3. Have you ever notified the Council of assessors trying to sell their own products or services?

Answer. Response was not received at the time of publication.

Question 4. The basic design and security model of credit cards has not changed since the 1950s. What major investments would be required for a large-scale migration to a different payment technology? Who would make those investments? For example, if we were move to a chip and PIN system?

Answer. Response was not received at the time of publication.

Question 5. A large part of the data theft problem is the amount of valuable data stored in the system. What requirements exist for merchants to store credit card data in their systems? Please explain how the chargeback/retrieval process affects what kinds of data can or should be stored on a merchant's system.

Answer. Response was not received at the time of publication.

Question 6. Visa asserts that consumers bear zero legal liability for fraudulent use of credit cards. How is this policy financed?

Answer. Response was not received at the time of publication.