Prepared testimony of
Robert Russo
General Manager
PCI Security Standards Council, LLC

Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
of the
House Committee on Homeland Security

"Do the Payment Card Industry Standards Reduce Cybercrime?"

311 Rayburn House Office Building
Tuesday, 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 U.S. 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 three 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 ongoing 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 ongoing 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 (P.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 ongoing 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 ongoing 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 two 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 two 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 touch screen 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 website 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 website 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 lifecycle 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 lifecycle process is important, it is equally important that the Council be responsive to emerging threats. As a result, we have several mechanisms for ongoing 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 online 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 ongoing 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.

# # #