Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

Statement of Stephen W. Orfei
General Manager
PCI Security Standards Council

Before the Committee on Financial Services,
United States House of Representatives
Protecting Consumers: Financial Data Security in the Age of Computer Hackers
May 14, 2015
2129 Rayburn House Office Building

Introduction

Chairman Hensarling, Ranking Member Waters, members of the committee, on behalf of the PCI Security Standards Council, thank you for inviting us to testify today.

My name is Stephen Orfei and I am the General Manager of the Payment Card Industry (PCI) Security Standards Council (SSC), a global industry initiative and membership organization, focused on securing payment card data. Working with a global community of industry players, our organization has created data security standards—notably the PCI Data Security Standard (PCI DSS)—certification programs, training courses and best practice guidelines to help improve payment card security.

Together with our community of over one thousand of the world’s leading businesses, we’re tackling data security challenges from password complexity to proper protection of EMV Chip Terminals. Our work is broad because there is no silver bullet to securing payment card data. No single technology is a panacea; security technology is constantly evolving and requires a multi-layered approach across the payment chain.

Work by the PCI Security Standards Council demonstrates effective industry collaboration to develop private sector standards. Simply put, the PCI Standards are the best line of defense against the criminals who threaten our way of life by seeking to steal and utilize payment card data. And while recent high profile breaches have captured the nation's attention, the PCI Council has stimulated great progress over the past eight years in securing payment card data through a collaborative cross-industry approach, and we continue to build upon the way we protect this data.

We understand that consumers are upset when their payment card data is put at risk of misuse and—while the PCI Security Standards Council is not a name most consumers know—we are sensitive to the impact that breaches cause for consumers. Consumers can take comfort from the fact that many of the organizations they do business with have joined with the PCI Council to collaborate in an effort to better protect their payment card data.

Payment card security: a dynamic environment

Since the threat landscape is constantly evolving, the PCI Council expects its standards will do the same. Confidence that businesses are protecting payment card data is paramount to a healthy economy and payment process—both in person and online. That's why to date, more than one thousand of the world's leading retailers, airlines, banks, hotels, payment processors, government agencies, universities, and technology companies have joined with the PCI Council as Participating Organizations and as part of our community to develop security standards that apply across the spectrum of today's global multi-channel and online businesses.

Our Board of Advisors is a global, active, cross-industry group that includes merchants such as Starbucks, Wal-Mart, British Airways; financial institutions such as Citi and Barclaycard; technology companies such as Cisco, RSA; and service providers such as First Data.

Our community members are living on the front lines of this battle and are therefore well placed, through the unique forum of the PCI Council, to provide input about threats they are seeing and ideas for how to tackle these threats through the PCI Standards. The Council and the PCI community have the resources to continually monitor and provide updates through standards, published FAQs, Special Interest Group work, and guidance papers on emerging threats and new ways to improve payment security. Examples include updated wireless guidance and security guidelines for merchants wishing to accept mobile payments.

Now in version 3.1, the PCI Data Security Standard (PCI DSS) is our overarching data security standard, built on 12 principles that cover everything from implementing strong access control, monitoring and testing networks, to having an information security policy. During updates to this standard, we receive hundreds of pieces of feedback from our community. This is almost evenly split between feedback from domestic and international organizations, highlighting the global nature of participation in the PCI Council and the need to provide standards and resources that can be adopted globally to support the international nature of the payment system.

This feedback has enabled us to be directly responsive to challenges that organizations are facing every day in securing cardholder data. For example, in this latest round of PCI DSS revisions, community feedback indicated changes were needed to secure password recommendations. Password strength remains a challenge—as "123456" and "password" are still the most common passwords used by global businesses—and is highlighted in industry reports as a common failure leading to data compromise. Small merchants in particular often do not change passwords on point of sale (POS) applications and devices. With the help of the PCI community, the Council has updated requirements to make clear that default passwords should never be used, all passwords must be regularly changed and not continually repeated, should never be shared, and must always be of appropriate strength. Beyond promulgating appropriate standards, we have taken steps through training and public outreach to educate the merchant community on the importance of following proper password protocols.

Recognizing the need for a multi-layered approach, in addition to the PCI DSS, the Council and community have developed standards that cover payment applications, card production, PIN security, EMV Chip Terminals and other PIN entry devices. In other areas, based on community feedback, we have produced standards and guidance on other technologies such as tokenization and point-to-point encryption. These technologies can dramatically increase data security at vulnerable points along the transactional chain. Tokenization and point-to-point encryption remove or render payment card information useless to cyber criminals, and work in concert with other PCI Standards to offer additional protection to payment card data. Going forward, "de-valuing" payment card data is a key strategy for erasing the monetary incentive for cyber criminals to commit data breaches.

In addition to developing and updating standards, every year the PCI community votes on which topics they would like to explore with the Council and provide related guidance. Over the last few years the working groups formed by the Council to address these concerns have drawn hundreds of organizations to collaborate together to produce resources on third party security assurance, cloud computing, best practices for maintaining compliance, e-commerce guidelines, virtualization, and wireless security. Other recent Council initiatives have addressed promoting security awareness by employees, ATM security, PIN security, and mobile payment acceptance security for developers and merchants. A key topic this year is daily log monitoring—a PCI DSS requirement that is critical for detecting (and stopping) early stages of a data breach in progress.

EMV Chip & PCI Standards—a strong combination

One technology that has garnered a great deal of recent attention is EMV chip—a technology that has widespread use in Europe and other regions. EMV chip is an extremely effective method of reducing counterfeit and lost/stolen card fraud in a face-to-face payments environment. That's why the PCI Security Standards Council supports the deployment of EMV chip technology.

However, global adoption of EMV chip, including broad deployment in the United States, does not preclude the need for a strong data security posture to prevent the loss of cardholder data from intrusions and data breaches. We must continue to strengthen data security protections that are designed to prevent the unauthorized access and exfiltration of cardholder data.

Payment cards are used in a variety of remote channels—such as electronic commerce—where today's EMV chip technology is not typically an option for securing payment transactions. Security innovation continues to occur for online payments beyond existing fraud detection and prevention systems. Technologies such as authentication, tokenization, and other frameworks are being developed, including some solutions that may involve EMV chip—yet broad adoption of these solutions is not on the short-term horizon. Consequently, the industry needs to continue to protect cardholder data across all payment channels to minimize the ongoing risks of data loss and resulting cross-channel fraud, such as may be experienced in the online channel.

Nor does EMV chip negate the need for secure passwords, patching systems, monitoring for intrusions, using firewalls, managing access, developing secure software, educating employees, and having clear processes for the handling of sensitive payment card data. These processes are critical for all businesses—both large retailers and small businesses—who themselves have become a target for cyber criminals. At smaller businesses, EMV chip technology will have a strong positive impact. But if small businesses are not aware of the need to secure other parts of their systems, or if they purchase services and products that are not capable of doing that for them, then they will still be subject to the ongoing exposure of the compromise of cardholder data and resulting financial or reputational risk.

Similarly, protection from malware-based attacks requires more than just EMV chip technology. Reports in the press and subsequent forensic analyses regarding recent breaches point to insertion of complex malware into vulnerable back-office computers, which were used by attackers as a gateway to POS systems containing unprotected cardholder data. EMV chip technology could not have prevented the unauthorized access, introduction of malware, and subsequent exfiltration of cardholder data. Failure of other security protocols required under PCI Standards is necessary for malware to be inserted.

Finally, EMV chip technology does not prevent memory scraping, a technique that has been highlighted in press reports of recent breaches. Other safeguards are needed to do so. In our latest versions of security standards for point of sale devices, (PCI PIN Transaction Security Requirements, or "PTS"), the Council includes requirements to further counter this threat. These include improved tamper responsiveness so that devices will cease to operate if they are opened or tampered with and the creation of electronic signatures that prevent applications that have not been "whitelisted" from being installed. Our newest version of the standard, PTS 4.0, requires a default reset every 24 hours that would remove malware from memory and reduce the risk of data being obtained in this way. By responding to the Council's PTS requirements, POS manufacturers are bringing more secure products to market that reflect a standards development process that incorporates feedback from a broad base of diverse stakeholders.

Used together, EMV chip, PCI Standards, complementary technologies and solutions such as tokenization and encryption, along with many other tools can provide strong protections for payment card data. I want to take this opportunity to encourage all parties in the payment chain—whether they are EMV chip ready or not—to take a multi-layered approach to protect consumers' payment card data. There are no easy answers and no shortcuts to security.

Global adoption of EMV chip is necessary and important. Indeed, when EMV chip technology does become broadly deployed in the US marketplace and fraud migrates to less secure transaction environments, PCI Standards will remain critical.

Beyond PCI Standards – building a support infrastructure

An effective security program through PCI is not focused on technology alone; it includes people and process as key parts of payment card data protection. PCI Standards highlight the need for secure software development processes, regularly updated security policies, clear access controls, and security awareness education for employees. Employees have to know not to click on suspicious links, why it is important to have secure passwords, and to question suspicious activity at the point of sale. For example, "Many [retail data breach] incidents involved direct social engineering of store employees (often via a simple phone call) in order to trick them into providing the password needed for remote access to the POS," according to the *Verizon 2015 Data Breach Investigations Report*.

Most standards' organizations create standards, and no more. PCI Security Standards Council, however, recognizes that standards, without more, are only tools, and not solutions. And standards alone do not address the critical challenges of training people and improving processes.

Consequently, the Council is actively distinguishing between "point-in-time compliance" with PCI Standards and "security." Achieving an ongoing state of payment security requires continuous effort in deploying security controls, monitoring their effective use, and diligently applying daily processes and best practices. This is a challenge, as noted by the *Verizon 2015 PCI Compliance Report*: "Compliance with the Payment Card Industry Data Security Standard (PCI DSS) continues to improve, but four out of five companies still fail at interim assessment. This indicates that they've failed to sustain the security controls they put in place." And, "But for most companies the DSS provides a useful baseline. While validation is no assurance of security, not being compliant is pretty much a guarantee that you're not secure."

To help organizations improve continuous payment data security, the Council takes a holistic approach to securing payment card data, and its work encompasses both PCI Standards development and maintenance of programs that support standards implementation across the payment chain. The Council believes that providing a full suite of tools to support implementation and ongoing sustainment is the most effective way to ensure the protection of payment card data. To support successful implementation of PCI Standards, the Council maintains programs that certify and validate certain hardware and software products to support payment security. For example, the Council wants to make it easy for merchants and financial institutions to deploy the latest and most secure terminals and so maintains a public listing on its website for them to consult before purchasing products. We realize it takes time and money to upgrade POS terminals and we encourage businesses that are looking to upgrade for EMV chip to consider other necessary security measures by choosing a POS terminal from this list. Similarly, we are supporting the adoption of point-to-point encryption, and listing appropriate solutions on our website to take a solutions-oriented approach to helping retailers more readily implement security in line with the PCI standards.

Additionally, the Council runs a program that develops and maintains a pool of global assessment personnel to help work with organizations that deploy PCI Standards to assess and sustain their performance in using PCI Standards. The Council also focuses on creating education and training opportunities to build expertise in protecting payment card data in different environments and from the various viewpoints of stakeholders in the payment chain. Since our inception, we have trained tens of thousands of individuals, including staff from large merchants, leading technology companies and government agencies. Finally, we devote substantial resources to creating public campaigns to raise awareness of these resources and the issue of protecting payment card data.

The PCI community and large organizations that accept, store, or transmit payment card data worldwide have made important strides in adopting globally consistent security protocols. However, the Council recognizes that small organizations remain vulnerable. Smaller businesses lack IT staff and budgets to devote resources to following or participating in the development of industry standards. But they can take simple steps like updating passwords, firewalls, and ensuring they are configured to accept automatic security updates. Additionally, to help this population, the Council promotes its listings of validated products, and recently launched a program, the Qualified Integrator and Reseller program (QIR) to provide a pool of personnel able to help small businesses ensure high quality and secure installation of their payment systems.

The work of the Council covers the entire payment security environment with the goal of providing or facilitating access to all the tools necessary—standards, products, assessors, educational resources, and training—for stakeholders to successfully secure payment card data. We do this because we believe that no one technology is a panacea and effective security requires a multi-layered approach.

Public – private collaboration

The Council welcomes this hearing and the government’s attention on this critical issue. The recent data breaches underscore the importance of constant vigilance in the face of threats to payment card data. We are hopeful that this hearing will help raise awareness of the importance of a multi-layered approach to payment card security.

There are very clear ways in which the government can help improve the payment data security environment. For example, government can champion stronger law enforcement efforts worldwide, particularly due to the global nature of these threats. It can also encourage stiff penalties for cybercrimes to act as a deterrent. Also, there is much public discussion about simplifying data breach notification laws and promoting information sharing between public and private sectors. These are all opportunities for the government to help tackle this challenge.

The Council is an active participant in government research in this area: we have provided resources, expertise and ideas to FS-ISAC, NIST, DHS, and the Secret Service, as well as global agencies such as Interpol and Europol. We remain ready and willing to do more.

Twenty years ago, through its passage of the Technology Transfer and Advancement Act of 1995, Congress recognized that government should rely on the private sector to develop standards rather than to develop them itself. The substantial benefits of the unique, U.S. “bottom up” standards development process have been well recognized. They include the more rapid development and adoption of standards that are more responsive to market needs, representing an enormous savings in time to government and in cost to taxpayers.

The Council believes that the development of standards to protect payment card data is something the private sector, and PCI specifically, is uniquely qualified to do. It is unlikely any government agency could duplicate the expansive global reach, expertise, and decisiveness of the PCI Council. High profile events such as the recent breaches are a legitimate area of inquiry for the Congress, but should not serve as a justification to impose new government regulations. Any government standard in this area would likely be significantly less effective in addressing current threats, and less nimble in protecting consumers from future threats, than the constantly evolving PCI Standards.

Conclusion

In March, the *Verizon 2015 PCI Compliance Report* said: “Of all the data breaches that our forensics team has investigated over the last 10 years, not a single company has been found to be compliant at the time of the breach—this underscores the importance of PCI DSS compliance.”

But we recognize that compliance is not the endgame. Security is.   That’s why it’s so critical that companies maintain this effort through ongoing vigilance.

Recent breaches at retailers underscore the complex nature of payment card security and the need for ongoing vigilance. A complex problem cannot be solved by any single technology, standard, mandate, or regulation. It cannot be solved by a single sector of society—business, standards-setting bodies, policymakers, and law enforcement—must work together to protect the financial and privacy interests of consumers. Today as this committee addresses the issue of data breaches, we know that there are criminals intent on inventing the next threat.

There is no time to waste. The PCI Security Standards Council and business must commit to promoting stronger security protections and continuous effort of their effective use while Congress leads efforts to combat global cyber-crimes that threaten us all.

We thank the Committee for taking an important leadership role in seeking solutions to one of the largest security concerns of our time. Our conversation should not end today. We embrace the opportunity to work with you to develop the most practical and feasible solution to addressing cyber and data security threats.

# # #