Prepared testimony of
Troy Leach
Chief Technology Officer
PCI Security Standards Council, LLC

Before the Subcommittee on Financial Institutions and Consumer Credit

“The Future of Money: How Mobile Payments Could Change Financial Services”

Room 2128 Rayburn House Office Building
Thursday, March 22, 2012

Introduction

Chairman Capito, Ranking Member Maloney, members of the Subcommittee, thank you for the opportunity to testify on the important issue of mobile payment security.

My name is Troy Leach and I am the chief technology officer of the PCI (Payment Card Industry) Security Standards Council. The Council is a global industry standards body focused on securing payment card data that is processed, stored, or transmitted regardless of the form factor, device or channel used to initiate payment. Formed in 2006 by the payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. to guide the development of open industry standards for global payment security, the Council has an active base of more than 600 global participating organizations representing leading industry players from the around the world.

As the payments environment changes, new technologies are introduced which must be evaluated to determine what new threats may also emerge. It is increasingly important to have a strong framework, driven by cross-industry collaboration to secure payment transactions to contain and reduce fraud for consumers and businesses globally.

Mobile technology offers many opportunities to grow consumer payments and also presents many challenges to secure sensitive payment information. As with any technology being considered for use in a payments environment, the Council's goal is to foster standards that help to minimize this risk to cardholder data. To this end, we have taken a leadership role by actively engaging with industry and other standards groups to proactively address the security of mobile payment acceptance. The Council's work is ongoing, and we have made significant progress.

My testimony today will outline the Council's focus on securing cardholder data, specifically in environments where mobile devices are being used as a new type of payment acceptance tool, and how we're applying our expertise to address the fast-paced evolution and adoption of mobile technology in the payments space. Currently, we are not addressing consumer-facing mobile payment technologies or solutions.

About The PCI Security Standards Council

The Council's Mission

The Council was formed in 2006 by global payment card brands to work with industry stakeholders in guiding the development of open industry standards for global payment security.

Very simply, this means that the Council's goal is to foster standards to protect not just consumers, but also industry players such as merchants (retailers, transportation companies, hotels, etc), banks, government, academia and all other organizations that store, process and transmit cardholder data. It's this wide range of stakeholders that make up the Council's global base of more than 600 leading national, regional and global participating organizations.

The Council's Work

The growth and improvement in payment card security over the past 5 years has everything to do with global industry involvement in the work of the Council.

It's through the voluntary and active participation of this global community that the Council sets and develops technical standards and other resources that comprise the essential tools needed help to protect cardholder data against breaches and reduce payment card fraud. Protecting payment card data is a shared responsibility across the payments ecosystem. Together with our industry participants we drive education and awareness of payment security globally.

Today global adoption of the Council's standards and industry participation in the Council's process for standards development are at an all-time high. As a result of our collective efforts, we are seeing fewer large-scale card data breaches in the marketplace.[1] And when breaches do occur, organizations that have applied the Council's PCI Security Standards are in a better position to mitigate the impact of the compromise.[2] Together these industry standards provide the best baseline available for protecting payment card data. Indeed, other sensitive industries are modeling their own security standards on those developed by the Council.

The Council's Role in Mobile Payments

Our Focus

The Council's focus is the protection of cardholder data through implementation of its standards. Absent such safeguards, that data can be too easily accessed, and then used to commit fraud. It's through this lens that we evaluate mobile payments technology.

[1] Verizon Business 2011. "2011 Data Breach Investigations Report."

[2] The Ponemon Institute. 2011. "2011 PCI DSS Compliance Trends Study."

When discussing mobile payment security, it's important to differentiate between two different environments for the use of mobile devices:

1) Merchant acceptance applications where phones, tablets and other mobile devices are used by merchants as point-of-sale terminals in place of traditional hardware terminals, and

2) Consumer facing applications where the phone is used in place of a traditional payment card by a consumer to initiate payment. Several standards groups have been involved and have focused on securing different parts of the mobile payments ecosystem with the aim to protect payment data.

The Council's security efforts to date in this area have been concentrated on work related to securing the use of mobile devices as a point of sale acceptance tool.

In line with the Council's focus on working with stakeholders to secure the entire payment card transaction– from point of entry of payment data to how it's processed through secure payment applications - the Council's efforts in the mobile area are centered around the impact of mobile payment solutions on merchant acceptance and processing channels. Specifically, the Council is focused on mitigating the risk of mobile devices used to take payments from being tampered with; addressing the security of applications running on mobile devices that include or require card data; and the integrity of third-party services. In the midst of an evolving payments landscape and threat environment, maintaining the security of cardholder data remains critical and an ongoing challenge. To address this fast-changing technology and continue to drive payment security forward, the payments industry needs to look to advancements in secure payment technology (e.g., through encryption) to reduce these risks by minimizing the value and exposure of cardholder data, and develop strong effective security practices and controls for mobile payments. The payments industry must take a nimble and proactive approach, while continually evolving our strategies for risk management to adapt quickly to these ongoing changes.

As an open, global cross-industry organization focused on providing baseline standards for stakeholders to increase the security of payment transactions, the Council is well positioned to spearhead this effort. We recognize that payment security is a shared responsibility and requires active involvement from participants across the payment chain. The Council is currently working with stakeholders from all sectors of the emerging mobile payment acceptance environment to collectively and effectively develop the standards and other tools necessary to help secure cardholder data in this manner.

Challenges and Risks

The ability to use mobile technology to accept and process payments undoubtedly offers great potential to the marketplace. However, the rapid innovation and complexity of the environment, present a number of challenges, including managing potential risks to payment information. In the midst of growing deployment of mobile technologies in payments, worries over security may potentially be a barrier to adoption.

While technologies that promise real solutions for securing mobile acceptance are quickly evolving, a number of security risks remain. These include: rapid and potentially insecure development of mobile applications; lack of traditional security controls such as effective software patch management and monitoring; potentially unauthorized access or too wide-spread privileges of third parties to access financial applications; and to the potential for the abuse protective measures such as data encryption or administrative controls. A failure to adequately address any of these valid concerns can put payment card data at risk.

Our Approach

The Council is applying its expertise to examine these risks within the context of the existing industry security framework that its PCI Security Standards provide – one that's built around the fundamental element of trust essential to enable mobile commerce to flourish.

For mobile technology to be adopted in the same way that traditional forms of payment are accepted, consumers and businesses alike need to be able to trust the ability of the technology to protect their payment data. It's also critical that they trust the service providers and other entities involved.

Trust is even more significant in the mobile payments environment because the environment is fragmented across manufacturers of devices, developers of Operating Systems, application designers, network carriers and the use of various protocols used to connect these different entities. Payment security is a shared responsibility. Ensuring mobile acceptance solutions are deployed securely requires that all parties in the payment chain work together in this effort.

To tackle this issue of trust the Council is working with a variety of stakeholders around the world. The goal is to identify and mitigate the risks that may arise when consumer and merchant roles converge to protect the device, the manufacturing of the device, the secure coding practices for software within those environments and the standards required to test and validate third-party entities that are involved in processing, storing and transmitting transaction data.

Securing Mobile Payments: Payment Acceptance Devices

Mobile phones have not traditionally been built to function as payment acceptance devices. Today, new capabilities are being added to these mobile devices to enable them to accept payment transactions. The integrity of the device that is being used to initiate a payment or access payment card-related information has to be trusted, and this trust must be based on real and robust security. Given this potential risk area to cardholder data, the integrity of the acceptance device is one of the Council's key focus areas in its work to address the mobile payment acceptance security.

The Council's existing standards include the PCI PIN Transaction Security (PTS) requirements[3] to provide security for physical devices accepting payments, such as point-of-sale terminals at the grocery checkout, gas pumps and airline ticket kiosks. The standard aims to ensure that the device is tamper-proof and if compromised, the data will be "zeroized", rendering it useless. At the end of 2011, the Council expanded the PTS requirements for protecting traditional swipe card terminals against tampering, to apply to mobile payment acceptance devices.[4]

The Council maintains a list on its website of approved devices that have been successfully tested in Council-approved laboratories to assist merchants in assessing the security of their currently deployed terminal devices, and in making informed future purchasing decisions.[5] This list is now expanding to include mobile, as well as traditional, acceptance devices.

Compliance by device vendors with the PCI PTS requirements allows merchants to use plug in devices with mobile phones to swipe cards securely by first encrypting the data at the point that the card is swiped to minimize risk by making it unreadable. The mobile device acts as a conduit and has no ability to decrypt the encrypted data.

Later this year, the Council plans to release specific guidance for merchants on how to effectively use these security requirements in conjunction with encryption technology to more easily and securely accept payments using mobile technology.

Securing Mobile Payments: Payment Software Applications

Today the entire shopping experience, from creating a grocery list to paying for the items on that list, can be realized using mobile technology. Retailers can get more customers through their store during a busy holiday season using payment software applications installed on a phone or tablet that transform these devices into a mobile cash register for quick and easy checkout. Consumers and

[3] PIN Transaction Security (PTS) requirements contain a single set of requirements for all personal identification number (PIN) terminals, including POS devices, encrypting PIN pads and unattended payment terminals.
https://www.pcisecuritystandards.org/security_standards/documents.php?association=PTS

[4] PCI Security Standards Council. 2011. "PCI Council Updates PTS Program for PTS, Mobile." Press Release, November. https://www.pcisecuritystandards.org/pdfs/pr_111014_pts_v3-1.pdf

[5] Approved PIN Transaction Security Devices
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

businesses alike are benefiting from the convenience of mobile payments technology.

The potential for mobile technology to make things faster, easier and cheaper, both at home and in the workplace, domestically and around the world, means there is a growing market demand for businesses to use mobile applications to accept and process payments.

The security of software applications is one of the leading issues in securing mobile acceptance. Applications and acceptance devices must work together to realize a mobile payment transaction. Just as the integrity of the device has to be trusted, so does the integrity of the payment software application. As noted earlier, one of the key roles of the Council is not only to create the standards necessary to enable security, but also to educate the marketplace to the benefit of implementing these standards.

The PCI Payment Application Data Security Standard (PA-DSS) is the Council's standard for addressing the security of software applications.[6] It supports the Council's foundational standard for securing cardholder data, the PCI Data Security Standard (PCI DSS).[7]

Traditional 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. Some of these payment applications may be designed to store cardholder data, putting this information at risk. Once again, the Council maintains a list of PA- DSS compliant applications. In this case, that list includes those applications that have been tested by Council-trained security assessors in laboratories and validated as secure. This list is available on the Council website for merchants to use in assessing their own applications and making informed purchasing decisions.[8]

[6] To help software vendors and others develop secure payment applications, the Council maintains the Payment Application Data Security Standard (PA-DSS).
https://www.pcisecuritystandards.org/security_standards/documents.php?association=PA-DSS

[7] The PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.
https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0

[8] List of Validated Payment Applications
https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php

It's against this standard that mobile payment acceptance applications are evaluated, recognizing that the strong technical requirements in this standard should be the baseline for any application accepting or processing payments – whether traditional or mobile.

As part of this evaluation, in 2011 the Council issued guidance on the types of mobile payment acceptance applications that can allow businesses to accept and process payments securely.[9] The Council published a checklist resource to help explain simply and succinctly to anyone currently considering mobile payment acceptance solutions which types of application support PCI Standards.[10] This resource, like all Council tools and resources, is available for download from the Council website free of charge.

The Council also identified the types of applications that fall short of security standards for secure mobile payment transactions. In collaboration with industry subject matters experts, including software application developers, the Council is continuing to examine this area to determine whether the inherent risk of card data exposure in these applications can be addressed by existing PCI requirements, or whether additional guidance or requirements must be developed.

Securing Mobile Payments: The Way Forward

The technology is here to make mobile payments a reality, and the possibilities are infinite. The Council's charter is to provide a forum for collaboration across the payments space to determine how the potential of mobile payment acceptance technology can be realized securely. The more pervasive mobile technology becomes the more we will see new threats and attack vectors that put data at risk. In tandem, other technologies for securing payments will emerge. It is, and for the future will certainly remain, a dynamic space.

As with all unchartered territory, trust must be established to make a way forward. In the case of mobile technology, this means establishing mechanisms and resources to build consumer and marketplace confidence that mobile payments are just as secure as credit or debit card payments. The Council will continue its consideration of extensions to its existing standards and the development of new standards to help ensure the trusted security of mobile payments and the devices that enable them. Additionally, this will mean working to enhance the security of entities across the payment chain who are involved in mobile acceptance, to ensure the existence of an industry standards framework

[9] PCI Security Standards Council. 2011. "PCI Security Standards Council Update on PA-DSS and Mobile Payment Acceptance Applications." Statement, June. https://www.pcisecuritystandards.org/documents/statement_110624_pcissc.pdf

[10] PCI Security Standards Council. 2011. "Which Applications are Eligible for PA-DSS Validation? A Guiding Checklist." Factsheet, June. https://www.pcisecuritystandards.org/documents/which_applications_eligible_for_pa-dss_validation.pdf

to validate these entities, and to establish trust in the services these entities provide. This is an area that the Council will continue to examine moving forward.

In the meantime, great work is being done through the advancement of technologies in payments. The mobile phone will introduce new innovation but also may introduce new risks to payments. Our strategy for minimizing risk that can be added to a payment transaction by a mobile acceptance device is, where possible, to help eliminate card data from potentially insecure mobile environments. Technologies continue to emerge that offer the potential to both leverage the power of mobile computing and effectively reduce security risks by making payment data inaccessible or devaluing the data rendering it useless for committing fraud. The Council has already harnessed some of these technologies to address this dynamic environment and we will continue to assess and develop standards and guidance around them moving forward.

Payment security is a shared responsibility. The Council has engaged a wide range of industry participants in a collaborative effort to apply continued focus to the area of mobile payment acceptance security, including members across the mobile payments spectrum – from those who develop the applications and the phones themselves to those who are providing voice and data services. We are also working appropriately with other standards groups on this issue – such as EMVCo and BITS - and others across the board to address this multi-faceted challenge as an industry. Our outreach efforts to engage new players with whom we can work together to enable security in payments are ongoing.

The mobile payments environment, like other new and complex environments demands an understanding of many different perspectives. As a global industry group with members who represent the payment chain around the world, the Council is positioned to spearhead efforts to help ensure that payment security standards are addressing the mobile payments environment.

Conclusion

Once again, I want to thank Chairman Capito, Ranking Member Maloney, and the members of the Subcommittee for providing me the opportunity to testify on this important issue of mobile payment security. The PCI Security Standards Council's mission is securing payment data, including mobile acceptance. As the payments system changes and new technologies evolve, we will continue to work with our global stakeholders to develop the industry standards and provide the resources necessary for the protection of cardholder data across all payments channels and for the reduction of fraud for consumers and businesses globally.

# # #

United States House of Representatives
Committee on Financial Services

"TRUTH IN TESTIMONY" DISCLOSURE FORM

Clause 2(g) of rule XI of the Rules of the House of Representatives and the Rules of the Committee on Financial Services require the disclosure of the following information. A copy of this form should be attached to your written testimony.

1. Name:	**2. Organization or organizations you are representing:**
Troy Leach	PCI Security Standards Council, LLC
3. Business Address and telephone number:	
[redacted]	
4. Have you received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify?	**5. Have any of the organizations you are representing received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify?**
□ Yes ☑ No	□ Yes ☑ No
6. If you answered .yes. to either item 4 or 5, please list the source and amount of each grant or contract, and indicate whether the recipient of such grant was you or the organization(s) you are representing. You may list additional grants or contracts on additional sheets.	
7. Signature:	

Please attach a copy of this form to your written testimony.