

# Quickbrief\*

## Retail & Consumer

Timely news on industry accounting, operational and tax issues

### PCI Standard Evolves to Address Continued Security Threats

**In this issue:**

**New developments  
surrounding PCI standard**

Throughout 2009, Payment Card Industry (PCI) compliance has remained a challenge for many organizations. Adding to the complexity, there have been a number of recent developments surrounding PCI compliance programs that will affect merchants and other stakeholders. Based on our experience helping organizations with the forensics, containment, and remediation after a security breach, PricewaterhouseCoopers has observed increasingly sophisticated attacks that target payment card data directly. While some breaches occurred at organizations that had previously validated their PCI compliance, others occurred at companies that had not fully implemented PCI programs. The nature of these attacks means that risk levels are yet again on the rise. Organizations need to respond with security programs that not only meet minimum compliance standards, but also effectively mitigate the risk of breach and the high costs associated with such events.

Yet the recent breaches are just one reason for the new developments. Updates to the PCI standards are driven by the evolution of threats, introduction of new technologies, and input from stakeholders. Since June of 2005, the PCI Data Security Standard has matured as multiple constituents – including card brands, the PCI Security Standards Council, merchants, service providers, and card issuers – continue to work toward a common goal of further reducing the risk associated with the unauthorized disclosure of cardholder data. In this brief, we will outline how recent industry developments will affect merchants and the key areas that merchants should be aware of as the payment card landscape continues to evolve.

#### Development #1: Increasing Validation Requirements

When the PCI program was first launched in 2005, initial adoption was low. Once the card brands set explicit deadlines and fines for larger merchants, compliance efforts increased. Now the card brands are looking at the risks posed by smaller merchants and seeking to establish stronger methods for reducing the risk associated with non-compliance.

#### Increased focus on smaller merchants

Acquirers are focusing more attention on the merchants that process a smaller amount of transactions per year, but as a group they make up a large percentage of merchants. Not all merchants present the same level of risk, so some acquirers are

risk-ranking Level 4 merchants – those merchants that process the fewest transactions – through surveys or monitoring software. Based on the results of the assessment, acquirers are increasing validation requirements for certain Level 4 merchants. Recently, we have seen acquirers fine a portion of Level 4 merchants that had not validated their PCI compliance by completing a Self Assessment Questionnaire.

All merchants that accept credit card payments are required to be PCI compliant and all Level 4 merchants should already have a PCI Data Security Standard program in place – even if they have not been asked to validate compliance by their acquiring bank. This should include having the required PCI controls, completing the appropriate Self Assessment Questionnaire, and performing quarterly vulnerability scans with an Approved Scanning Vendor, if applicable.

### **Changes to the MasterCard Site Data Protection program**

MasterCard International recently introduced several changes to their PCI Site Data Protection program. The changes include a new requirement for Level 1 and 2 merchants to engage a Qualified Security Assessor to validate compliance through PCI Data Security Standard. Previously, Level 1 merchants were permitted to validate compliance by performing a self-assessment if an Officer of the merchant signed off on the Report on Compliance; Level 2 merchants could previously submit a Self Assessment Questionnaire without the need for an external third-party assessor to perform the compliance validation. **The change introduced in the Site Data Protection program requires that an assessment by a Qualified Security Assessor must occur for Level 1 and 2 merchants by December 31, 2010.** Merchants should work with their acquirers to determine what changes, if any, need to be made to their compliance validation program.

In addition, the MasterCard Site Data Protection now contains an updated fine structure for non-compliant merchants. The new structure contains higher initial fines which now start at \$25,000 and \$10,000 for Level 2 and Level 3 merchants, respectively. Additional violations will trigger escalating fines that cap out, per month, at \$200,000 for Level 1 and Level 2 merchants and \$80,000 for Level 3 merchants. Annually, the fines for Level 1 and Level 2 merchants are capped at \$375,000.

### **Development #2: New technologies**

Due to the increasing risks to payment card data, many stakeholders are working to develop and deploy solutions to reduce or eliminate the storage and handling of cardholder data by merchants and service providers. These solutions are designed to address some of the inherent risks in the current payment card processes and infrastructure.

### **End-to-end encryption**

Currently, in most organizations, payment card data may be encrypted and decrypted multiple times before it is sent to a processor. Once received by the processor, the data may be further encrypted and decrypted before it's used for authorization and settlement. End-to-end encryption is designed to encrypt the payment card data as close to the point of entry as possible and to maintain the encryption until it's required for authorization and settlement. End-to-end encryption is deployed in various places around the world and there is currently a standardization effort underway in the US to promote interoperability. This approach promises to greatly reduce the risk held by merchants (and acquirers depending on the deployment), as the data would not be stored on systems and is transmitted to the acquiring bank in an encrypted format. End-to-end encryption requires new systems and technologies to perform the encryption, as well as modifications to payment card systems and other key management processes.

### **Tokenization**

While not a "new" technology, tokenization has matured considerably over the past few years. Tokenization allows a merchant to replace instances of payment card numbers with another number or "token" that has no value outside of the payment environment. As the technology has matured, a number of vendors now offer tokenization solutions as part of hosted services or as modules that can be integrated in a merchant's environment.

### **Magnetic stripe authentication**

Besides enhancing the security of payment card data, there are new technologies that reduce the usefulness of compromised payment card data. One approach is magnetic stripe authentication, which creates an electronic "fingerprint" of a card based on the unique characteristics contained within the card's magnetic stripe. During a purchase, the "fingerprint" is compared to a copy obtained by the issuer or a past transaction to determine if it is significantly different, accounting for minor variations. Consequently, merchants may experience reduced fraud from compromised track data. Implementing this solution typically involves new magnetic stripe readers and updates to point of sale systems.

### **Cardholder challenge and response**

Another approach – cardholder challenge and response – is designed to make compromised cardholder data less valuable unless combined with other personally identifiable information. This method requires customers to provide information at the checkout terminal such as the billing zip code, the last four digits of their home phone number, their home area code, and the last four digits of their cell phone number. Often, this data is not stored along with payment card data, so the risk of fraud associated with compromised

## PCI trends & developments

- Attacks against payment card data are rising in frequency and sophistication.
- Card brands are increasing focus on smaller merchants.
- New technologies are facilitating compliance and reducing risk to payment card data.
- MasterCard changed validation requirements for Level 1 and 2 merchants.
- Bank sues third party assessor of payment processor that experienced a large breach.
- Nevada passed the first law incorporating all of PCI as a state requirement.
- As of July 2009, less than five e-commerce applications have been certified to the Payment Application Data Security Standard.
- Participating Organizations are now able to provide formal feedback on PCI Data Security Standard v1.2.
- The US House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology conducted a hearing into the protection of confidential data.

payment card data is reduced. Depending on the environment, cardholder challenge and response can often be deployed with modifications to the point of sale systems.

## Evaluation of emerging technologies

The PCI Security Standards Council has engaged PricewaterhouseCoopers to assist in the evaluation of emerging technologies and approaches that may be available to help merchants, service providers, and processors more effectively secure cardholder data in accordance with the various standards.

We are currently working with some of the world's largest merchants, service providers, and processors to evaluate which technologies have the potential to facilitate compliance and reduce risk associated with payment card data. Findings and observations of this study will be presented by PricewaterhouseCoopers at the annual PCI Participating Organization Conference in September 2009.

## Development #3: Key Dates and Initiatives from the Standards Security Council

PCI compliance is continuously evolving alongside the associated standards, programs, and other requirements. Merchants need to be aware the impact these changes may have on their programs.

### Payment Application Data Security Standard deadlines

The Payment Application Data Security Standard defines controls that must be in place for commercial payment applications developed by third party vendors. **All merchants using commercial-off-the-shelf payment applications within their environments must use Payment Application Data Security Standard compliant products by July 31, 2010.** These requirements do not apply to third-party developed payment applications which have been modified and customized for the merchant's needs and environment; such applications will be assessed as part of the merchant's overall PCI Data Security Standard assessment scope. Merchants can find a list of Payment Application Data Security Standard compliant applications posted on the PCI Security Standards Council's website.

Due to the potential impact of upgrading key payment systems, merchants should already be determining whether their environments contain any non-Payment Application Data Security Standard compliant applications. Merchants with e-commerce operations need to be aware there are very few Payment Applications Data Security Standard compliant e-commerce applications currently available. Merchants may need to exert pressure on application vendors to provide compliant versions of applications prior to the deadline. **Merchants should further consider alternative options such as migrating to a compliant payment application in order to meet this requirement by July 1, 2010.**

### PCI Security Standards Council Quality Assurance Program

One of the first major payment card data compromises occurred in 2004 when a large processor was breached and 40 million card numbers were compromised. Three months prior to the breach, the processor was certified as compliant with the Cardholder Information Security Program (predecessor to PCI) by an assessor. This bears strong resemblance to a number of recent breaches of merchants and service providers that were certified as PCI compliant by their assessor. Incidents like these have driven the new Quality Assurance program. As part of the Quality Assurance program, the PCI Security Standards Council is currently reviewing assessors' workpapers and feedback. Merchants can play a role in the continuous improvement of the PCI compliance program by leaving comments about their assessors on the PCI Security Standards Council website. Merchants should be aware of the potential impact that the Quality Assurance program and a recent lawsuit

filed by a bank against the assessor in the 2004 breach may have on them. Based on conversations with many of the constituents involved, Qualified Security Assessors are enacting changes to manage their own exposure and risk – including increasing their diligence during assessments and becoming less receptive to compensating controls that address the risk to the payment card environment. In addition, merchants should be aware that Qualified Security Assessor contracts now contain a clause that allows their workpapers to be shared with the PCI Security Standards Council.

### **PCI feedback program**

Beginning July 1, 2009, the PCI Security Standards Council began the feedback and comment period for version 1.2 of the PCI Data Security Standard. Feedback provided will be evaluated by the PCI Security Standards Council Technical Working Group and will help shape the next version of the PCI Standards (PCI Data Security Standards, Payment Application Data Security Standard and Pin Entry Device Standard). Merchants who are Participating Organizations are encouraged to provide detailed and actionable feedback to the PCI Security Standards Council. Merchants that are not Participating Organizations should work with their payment processors, acquiring banks or Qualified Security Assessors to provide feedback. The feedback period will be open through October 31, 2009.

### **New Wireless Guidance**

The PCI Security Standards Council Wireless Special Interest Group released new guidelines for 802.11 wireless networks. It is required that all organizations – even those without authorized wireless networks – have processes in place to detect unauthorized or rogue wireless devices, performed with a wireless analyzer or wireless intrusion detection system. The new guidelines explicitly prohibit sampling locations, so organizations need to have a plan in place for checking all locations at least quarterly. Organizations that have authorized wireless networks that are not used to transmit payment card data are required to be separated by a firewall with appropriate rules in place in order to be excluded from the PCI wireless control requirement.

### **PIN Key Management Requirements**

**Merchants are required to transition their point of sale devices to Triple-Data Encryption Standard encryption keys by July 1, 2010.** Per MasterCard guidance, remote key injection can only be done if the systems are PCI compliant. Merchants need to make sure their environment is PCI compliant before implementing new keys, as manual key injection can be a burdensome process.

## **Development #4: Government Involvement**

The publicity surrounding recent breaches has led to increased concern from US states and an inquiry by the US House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology on the effectiveness of industry efforts to secure sensitive payment card data. The purpose of the hearing was to determine if the PCI Security Standards Council has been successful in reducing payment card data compromises and who benefits from the fraudulent transactions. One key observation was that the US lags behind the rest of the developed world with respect to a comprehensive data protection and privacy law.

### **Potential Federal Laws for the Protection of Cardholder Data**

As a result of the House hearing and several high-profile cardholder data compromises, observers are closely monitoring the US Federal government to determine if it will take a more active role in mandating a data security standard for cardholder data similar to HIPAA (developed to protect the privacy of individually-identifiable health information). Based on currently proposed legislation, a federal data security breach notification law may be passed first. In addition, US federal agencies like the Federal Trade Commission already investigate and enact sanctions for organizations involved in a data breach regarding personally identifiable information.

### **Nevada State Law – SB 227**

Nevada passed the first state law in the US that mandates PCI compliance. According to the law, any organization that does business in the state must "comply with the current version" of the PCI Data Security Standard as adopted by the PCI Security Standards Council, and comply by the deadlines established by the council. The law also covers entities that accept other types of personally identifiable information; these entities are required to encrypt data when transmitted and provide logical and physical controls for data storage.

While Nevada is the first state to incorporate PCI compliance into a law, history has shown other states often enact similar legislation to protect residents. For example, California's SB 1386 was considered a groundbreaking privacy law in the US. Other states saw the benefit of Data Breach Notification Laws and 45 states passed similar regulations. Minnesota incorporated parts of PCI into a law, but did not mandate compliance with the standard. Given the recent PCI data breaches, other states may follow Nevada's lead and pass similar laws.

The Nevada law mandates PCI compliance but does not outline penalties for non-compliance or explicit enforcement mechanisms. Instead, the law appears to provide a safe harbor for organizations that comply with the requirements. **The law goes into effect January 1, 2010 and merchants should consult with their legal council to determine implications this law may have on their organization.**

## Conclusion

The changes in the PCI landscape during 2009 are an indication of the continued maturing of the PCI compliance program towards a more inclusive and risk-based compliance program. The developments described in this overview also highlight the need for merchants to stay apprised of developments and make the relevant updates to their PCI programs. Based on these developments, key actions for merchants and service providers include:

- **Respond to increased validation requirements** by continuing to work with their third party assessors, payment processors and acquiring banks to evaluate how the recent compliance validation changes will impact current and future PCI efforts.
- **Evaluate new technologies** to see how they can play a role in the reduction of risks and costs associated with PCI compliance during the evaluation of new payment card systems and upgrades. In addition, companies should watch for the results of the emerging technology review presented by PwC at the 2009 Participating Organization meetings.
- **Be aware of key dates and initiatives from the security standards council.** Merchants should determine whether they use non-Payment Application Security Standards Council compliant applications or should transition to these applications, and should be prepared for more in-depth assessments of their PCI programs.
- **Remain alert for potential federal or state legislation and other government intervention** and consult with legal counsel to determine the potential impact.

To minimize the need to react to enhanced control requirements and reduce the chance of a breach, merchants should not approach PCI compliance as a checklist activity, but instead address the protection of payment card and other personally identifiable data through a risk-based approach. PCI compliance is not a one time event, but an ongoing activity that needs to be incorporated into how an organization secures their environment.

## Key PCI Dates

### September 30, 2009

Prohibited Data Storage Deadline for Global Level 1 and 2 Merchants (Visa).

### October 1, 2009

VisaNet Processors and agents must decertify all vulnerable payment applications (Visa).

### June 30, 2010

Use of Wired Equivalent Privacy (WEP) in current wireless implementations prohibited (PCI Data Security Standard).

### July 1, 2010

Triple - Data Encryption Standard (TDES) mandate; all point of sale Pin-Entry Devices must be encrypting PINs using TDES end-to-end (Visa and MasterCard).

### July 1, 2010

Acquirers must ensure their merchants, Visa Net Processors and agents use only Payment Application Data Security Standard compliant applications (Visa).

### September 30, 2010

Global PCI Data Security Standard Compliance Validation Deadline for Level 1 Merchants (Visa).

### December 31, 2010

All Level 1 and Level 2 merchants must validate compliance and complete an annual onsite assessment conducted by a PCI Security Standards Council certified Qualified Security Assessor (MasterCard).

**For more information, please contact:**

#### Ron Kinghorn

(617) 530-5938  
ron.kinghorn@us.pwc.com

#### Gary Loveland

(949) 437-5380  
gary.loveland@us.pwc.com

#### Mark Lobel

(646) 471-5731  
mark.a.lobel@us.pwc.com

pwc.com

The information contained in this document is provided 'as is', for general guidance on matters of interest only. Although we believe that the information contained in this document has been obtained from reliable sources, PricewaterhouseCoopers is not responsible for any errors or omissions contained herein or for the results obtained from the use of this information. PricewaterhouseCoopers is not herein engaged in rendering legal, accounting, tax, or other professional advice and services. Before making any decision or taking any action, you should consult a competent professional adviser.

© 2009 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP, a Delaware limited liability partnership, or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity. This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.