WHY IS PCI IMPORTANT TO ME?

Joshua Knopp, CISSP MasterCard Worldwide

When people talk about "PCI" they are typically referring to the Payment Card Industry Security Standards Council (PCI SSC or "PCI Council"). The PCI SSC is an open, global forum founded in 2006 by MasterCard Worldwide and four other payment brands with the goal of creating and maintaining security standards to protect payment card data. The most prominent standard is the PCI Data Security Standard (DSS). When a merchant is asked if it is PCI compliant, it is generally understood that the merchant is being asked if it is compliant with the security processes and controls set forth in the PCI DSS.

The primary purpose of the PCI DSS is to reduce the risk of payment card (debit and credit) data loss by preventing, detecting, and reacting to potential breaches or hacks that could lead to an account data compromise (ADC) event. In other words, the goal of the PCI DSS is to protect payment card data from criminal threats and to minimize data breach risk to merchants of all sizes.

DO I NEED TO BE PCI COMPLIANT?

MasterCard rules require all entities that store, transmit, or process cardholder data, regardless of size, to comply with all PCI DSS requirements. Merchants with one million or fewer card-present transactions and 20,000 or fewer e-commerce transactions are classified by MasterCard as Level 4 merchants.

Level 4 merchants may be required to report the status of their PCI DSS compliance on a regular basis. A merchant should always check with its acquirer (or acquirer designee) to determine if and how it should report PCI DSS compliance. A merchant's acquirer may require the merchant to complete a Self-Assessment Questionnaire (SAQ) to report its compliance status. There are different SAQs for different types of merchants. For example, a merchant that only accepts payment cards via a dial-up terminal and does not store any card data would complete SAQ B. Currently, there are a total of five different SAQs; the merchant's acquirer will help the merchant to choose the appropriate SAQ. Visit https://www.pcisecuritystandards.org/merchants/self_assessment_form.php for more information.

WHY DOES PCI MATTER TO MY SMALL BUSINESS?

Small merchants are being targeted— Recently, attackers have been increasingly focused on small businesses. You might say to yourself, "Why would anyone want to break into my business? Wouldn't they target a bank instead?" In fact, attackers are focusing on any entity that processes or stores payment card data and may be vulnerable to compromise. Large financial institutions and large merchants tend to have expensive and substantial security to

protect against attacks, but this level of security may not be feasible for a small merchant. Consequently, when searching for vulnerable targets, attackers are discovering that many small merchants haven't implemented even the most basic security measures required by the PCI DSS. As a result, attackers increasingly are seeking to compromise small merchant environments through targeted "production line"-type attacks, which often go undetected for long periods of time due to a lack of monitoring by the small merchants.

Payment card data loss can be costly—If a merchant is compromised, such that an attacker was able to access payment card data, the merchant's acquirer may hold the merchant financially responsible for any resulting fraud loss and for other costs. If an ADC event is suspected, the merchant may be responsible for having a forensic examination performed by a PCI Forensic Investigator (PFI), which can be expensive.

Attackers may also compromise non-payment card data, such as financial and human resource records and proprietary or trade secrets that could seriously harm the ongoing operation and reputation of the merchant's business.

WHAT IS AN ACCOUNT DATA COMPROMISE?

Simply stated, an ADC event is an occurrence that results, either directly or indirectly, in the unauthorized access to or disclosure of MasterCard-branded payment account data. An ADC event can occur with physical receipts, but the most common attacks are targeted at electronic forms of payment card data storage, either internally by a dishonest employee skimming cards or externally through attackers gaining access to the merchant's/service provider's systems from remote locations and subsequently stealing the data.

HOW CAN I PROTECT MYSELF FROM ATTACKERS

There are currently two primary types of merchants that are typically the target of ADC events:

1) **Brick-and-Mortar/Card-Present Merchants with Physical Store Fronts**
In most cases of payment card data theft, merchants are compromised through improperly configured remote access technologies used in their point-of-sale (POS) applications.—Examples of these technologies include, but are not limited to, the following: PCAnywhere, VNC, GoToMyPC.com, and Windows Remote Access. **(Note: While these technologies offer security functionality, they are often implemented in an insecure manner.)** Often, these technologies are used by a solution provider or POS vendor that is authorized to remotely access the merchant's network in order to maintain and update the merchant environment. Remote access technologies may also be used by store managers, owners, or supervisors to perform tasks such as updating financial records, managing inventory, or creating staff schedules from home or elsewhere via an Internet connection. However, attackers can use incorrectly configured Internet-based remote access software applications to gain full access to the merchant's systems.

   These remote access tools allow for proper security configuration; therefore, all remote access should utilize two-factor authentication, in accordance with PCI DSS requirements. Two-factor authentication is commonly established by using two of the following identifiers:
   - Something you know (such as a password),
   - Something you have (such as a secure token), and/or
   - Something you are (such as a fingerprint).

User IDs do not qualify as a factor in two-factor authentication.

2) **E-commerce or Internet-based Merchants**

Structured Query Language (SQL) injection attacks are the most prevalent form of successful attack against e-commerce based merchants.—A SQL injection attack occurs when an attacker inserts database code into a field on a website, which is subsequently executed by the database. This form of attack can give an attacker full access to a database, which can potentially be used to further compromise the rest of the network.

E-commerce merchants may utilize their own resources to host and manage their Internet presence, or they may hire a third party to host their site for them. (Visit www.mastercard.com/pci360 for a white paper on Hosted Payment Pages.) Internet-based merchants should be aware of their responsibilities with respect to accepting payment cards and protecting payment card data from criminals looking to target these sites. For example, the PCI DSS requires the implementation of secure coding to help ensure that systems are not vulnerable to SQL injection attacks. Also, PCI DSS requirements provide the option of installing web application firewalls, which can help protect merchant websites from such attacks.

WHAT ABOUT MY HARDWARE POINT-OF-SALE TERMINALS AND MY POINT-OF-SALE PAYEMENT APPLICATIONS?

Compliance with the PCI DSS is required, because small merchants accept payment cards (credit or debit) via a hardware POS terminal or a payment application. If a merchant does not have any other business processes that collect or store payment card data, then the focus of its security and compliance efforts should be on its hardware POS terminal and/or POS payment applications.

Hardware POS Terminals—Hardware POS terminals are predominantly utilized by brick-and-mortar merchants. This type of small merchant should work directly with its hardware vendor and/or acquirer on at least an annual basis to be sure it is receiving the information needed to secure its hardware terminals in alignment with PCI DSS requirements. In most cases, the merchant's acquirer can assist the merchant in communicating with its hardware terminal vendors.

The PCI SSC manages a list of devices validated as compliant with PCI PIN Transaction Security (PTS) requirements that can be used to securely accept PIN entry data. MasterCard requires that merchants utilize a PTS-validated PIN entry device to accept PINs.

A list of PCI SSC-approved PIN entry devices can be found on its website: https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

POS Payment Applications—Both e-commerce and brick-and-mortar-based small merchants may use a hardware POS terminal in conjunction with a personal computer-based payment application to process payment transactions, manage consumer accounts, maintain inventory, etc. The PCI SSC's *Payment Application Data Security Standard* (PA-DSS) requires payment application vendors to build their solutions securely in order to mitigate the risk of compromise for merchants using commercially available ("off-the-shelf") payment applications. Starting July 1, 2012, MasterCard will require all merchants using an off-the-shelf payment application to utilize a PA-DSS validated payment application.

The PCI Council has over 1,200 currently validated payment applications listed on its website:

https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php?agree=true

Please refer to this list or verify with your vendor or your acquirer/processor as to whether your payment application has been validated as PA-DSS compliant.

FOR MORE INFORMATION

Your acquirer can provide you with more information regarding the applicability of the PCI DSS requirements. In addition, the following resources are available to you:

MasterCard

The MasterCard PCI 360 website contains complimentary information including white papers and over two dozen webinars on cardholder data security. This site offers beginner to expert level training curricula suitable for merchants of all sizes and complexity.

MasterCard PCI 360 Education Portal: http://www.mastercard.com/pci360

The Payment Card Industry Security Standards Council

The PCI SSC provides a wide array of documentation on its website as well as a "micro-site" dedicated to small merchants.

PCI Security Standards Council Site: https://www.pcisecuritystandards.org
PCI SSC Small Merchants Site: https://www.pcisecuritystandards.org/smb

Qualified Security Assessors (QSAs)

The PCI SSC manages a program for Qualified Security Assessors (QSAs) that qualifies security assessors as being properly trained in evaluating merchant compliance with PCI DSS requirements. QSAs are thoroughly educated on PCI DSS requirements, have solid experience regarding information security, and are regularly subject to a vigorous Quality Assurance program. A QSA can act as both a consultant and an auditor specifically focused on PCI DSS requirements.

A list of validated QSAs are located on the PCI Council's website:
https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

Approved Scanning Vendors

The PCI Council manages Approved Scanning Vendors (ASVs). ASVs are organizations that validate merchant and service provider adherence to certain PCI DSS requirements by performing vulnerability scans of their online environments. For those merchants using Internet technologies for their business processes in tandem with their payment card systems, use of an ASV is needed to help ensure that hackers are not taking advantage of open access through the Internet to any of the merchant's systems containing cardholder data. The PCI SSC has approved more than 130 ASVs; however, small merchants should check with their acquirer or processor for recommended ASVs.

A list of currently validated ASVs is available on the PCI Council's website:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php