

Reducing PCI Compliance Scope: Take the Data Out

CyberSource Payment Security



With an average annual cost of \$225,000¹ for large merchants, a Payment Card Industry Data Security Standard (PCI DSS) audit is a resource intensive process that reaps few rewards. The scope of the audit is intrusive and requires an external auditor (Level 1 merchants²) or dedicated internal resources (Level 2, 3, 4 merchants²) to spend months analyzing and evaluating a merchant's environment and internal processes, to determine compliance without a guarantee of ongoing security. This brief will discuss a solution to limiting the PCI audit costs for a Card-Not-Present (CNP) merchant.

Solving the Problem

Limiting the cost of an audit while ensuring security measures are met on a continuous basis is no longer a pie-in-the-sky dream. While every merchant that processes credit cards will need to validate that they are PCI compliant, reducing the audit scope can directly result in a decline in associated expenditures.

The PCI standard mandates that every merchant device and system in the credit card environment be audited. According to a report by Gartner, large merchants with an average of 100,000 customer accounts would potentially store that data in 10 – 20 locations in-house³, resulting in millions of points of vulnerability and locations that will need to be audited. The amount of resources and time needed in this scenario results in an inflated expense with unquantifiable lost opportunity costs. Entirely eliminating the existence of card holder data from the environment is the only viable solution to reducing audit scope.

Revised PCI Scope

The removal of credit card data from the payment environment would render four out of the twelve PCI requirements obsolete (see Page 2, Requirements Removed from PCI Scope).

In using a third-party PCI compliant vendor to store and manage all credit card transactions, the merchant eliminates the number of critical systems from its PCI scope. As a result, the merchant has only to complete the PCI-DSS Self-Assessment Questionnaire (SAQ) A, which contains thirteen "yes" or "no" questions. In comparison, an average large merchant would be required to submit a fifty-page in-depth questionnaire as well as evidence of passing vulnerability scans completed by a PCI SSC Approved Scanning Vendor (ASV), a process that could take months to complete.

¹ \$225,000 does not include technological changes, operating and staff costs, and additional costs associated with bringing the merchant systems into compliance. Source: Ponemon Institute, "PCI DSS Trends 2010: QSA Insights Report," March 2010

² Merchant level definitions: http://usa.visa.com/merchants/risk_management/cisp_merchants.html

³ Source: Gartner, "Using Tokenization to Reduce PCI Compliance Requirements," August 5, 2009

PCI DSS Statistics:

- In the last five years, over 60% of merchants spent \$100,000 to \$1,000,000+ on PCI compliance

Cisco PCI DSS Survey,
January 2011

- \$204 = Average cost per breached customer record

Ponemon Institute,
March 2010

- Merchants can face fees of \$5,000 to \$100,000 per month for violating PCI compliance requirements

PCI Compliance Guide

CyberSource®

the power of payment

www.cybersource.com

Toll free: (888) 330-2300

Reducing PCI Compliance Scope: Take the Data Out



Requirements Removed from PCI Scope

- Requirement 1 – Install and maintain a firewall configuration to protect cardholder data
 - *Reason:* Firewalls will continue to be the dominant end-point security device. However, as cardholder data will no longer be stored in the environment, a dedicated firewall is not required to protect it.
- Requirement 3 – Protect stored cardholder data
 - *Reason:* The responsibility of protecting cardholder data would reside with the third-party vendor.
- Requirement 4 – Encrypt transmission of cardholder data across open, public networks
 - *Reason:* The third-party vendor would encrypt the data at the point of payment and be responsible for transmitting the data across a secure network.
- Requirement 9 – Restrict physical access to cardholder data
 - *Reason:* As cardholder data will be stored with a third-party vendor, merchant employees will no longer be able to physically access the data.

How it Works

Third-party vendors provide merchants with the means to store their entire valuable customer credit card information in a PCI-compliant environment, thereby becoming responsible for processing the data and protecting it from would-be hackers. Using a secure checkout page, which is actually hosted by the third-party vendor, transactions are captured and transmitted to the payment processor. On the vendor's side, the primary account number (PAN) is replaced with a masked number sequence (token), which is then provided to the merchant for record keeping and future transactions. Each token is unique and contains no valuable information, making it unattractive to hackers and reduces the potential impacts, should a security breach occur. Meanwhile, the PAN data is securely stored on the vendor's side. As with encryption, tokenization is viewed by the PCI council as a preferred method of managing data protection.

Merchants may be hesitant to trust a third-party vendor with its valuable customer credit card information, with the perception that data must be stored in-house in order to handle chargebacks, process recurring subscriptions, issue refunds, and provide other customer service activities. However, vetted vendors can assume the responsibility for processing chargebacks and provide recurring subscription features. Merchants can continue to provide customer service to their clients, as only PANs will be masked in the database. Regarding refunds, merchants would send the related token with a request to the vendor, who then processes the refund.

Results

What would a merchant expect to save from removing data from its environment and reducing its PCI scope? A definitive number is difficult to quantify as PCI scope differs by merchant depending on the complexity of their environment or the number of stored data records. However, in using a third-party source to securely capture, transmit and store its data, a merchant would expect significant savings from the following areas:

- Reducing the amount of resources dedicated to auditing the systems
- Repair/upgrade/replacement costs associated with bringing systems into compliance
- Reducing headcount dedicated to processing payments, chargebacks, refunds, etc.
- Minimizing the impact of a security breach (maintaining brand equity, avoiding customer lawsuits, retaining customers, eliminating public relations costs, etc.)

CyberSource®
the power of payment

www.cybersource.com

Toll free: (888) 330-2300