The Green Sheet
The Financial Services Industry Source for Education, Inspiration and Actionable Advice

What PCI Data Security Regulations Mean to Your Merchants

By Peter Scharnell

Recently I attended the MasterCard Acquirers conference in Atlanta and noticed that what is typically a conference devoted to sales, marketing and operational announcements was now dominated by one topic in particular – security. Over half of this years agenda was focused on cardholder security issues, primarily with regards to the Visa / MasterCard PCI security standards. The attendees witnessed a live Website hack and compromise by SecurityMetrics, a Payment Card Industry Security firm. They revealed to the audience online tools and resources – that anyone can easily access - that exposed common hacking practices and protocols. They went on to show us that any computer that is connected to the Internet is a target and that the easiest systems could be hacked and compromised in on only 7 minutes. At the end of their presentation, they revealed to us all how we can prevent the likelihood of being targeted by hackers and fraudsters by implementing some basic changes to our systems. Preventative measures like installing firewalls and utilizing intrusion detection technologies and they emphasized the importance of the PCI security policies. SecurityMetrics really drove home the point that industry-wide security policies and procedures are essential for all computers that are connected to the Internet but most importantly, they're required for the majority of the Websites and software applications that are conducting e-commerce transactions.

What are PCI Security standards?

The Cardholder Information Security Program (CISP) is a set of rules established by Visa for securing your computer systems and data from unauthorized access and loss of credit card information. These rules have been in place for several years and were required of large credit card processors, but were only recommendations for most merchants accepting credit cards. The Payment Card Industry (PCI) data security standard is an industry-wide standard that incorporates many of the CISP standards and includes additional requirements. These are now referred to as the PCI data security standard. Visa, MasterCard, American Express, Discover, and other card issuers now all recognize and adhere to the new unified PCI standard as a part of their data security programs.

The PCI regulations require that merchants encrypt credit card numbers however, they also specify rules related to CVV (card security) codes and other security related fields. These rules require that merchants do not store card security codes on their systems.

Who is subject to PCI Rules?

According to Visa, any merchant processing over 500,000 transactions a year must comply with PCI rules. For MasterCard, any merchant accepting $125,000 in transactions in a month must comply with PCI rules. Other card issuers have different rules however; most are adopting or recognizing Visa's. Almost all card issuers reserve the right to require any merchant to meet the rules, and any loss of data will certainly result in audit and rules requirements. You should consult with your bank or card-processing vendor to determine if any of your merchants must meet PCI rules.

Visa also states that acquirers are responsible for determining the compliance validation levels of their merchants. All merchants will fall into one of the four merchant levels and prioritized based on the volume of transactions, the potential risk, and exposure introduced into the Visa system. The transaction volume is based on the aggregate number of Visa transactions from a Doing Business As (DBA) or a chain of stores (not of a corporation that has several chains).
Merchant levels are defined as:

Merchant Level	Description
1	Any merchant-regardless of acceptance channel-processing over 6,000,000 Visa transactions per year. Any merchant that has suffered a hack or an attack that resulted in an account data compromise. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system. Any merchant identified by any other payment card brand as Level 1.
2	Any merchant processing 150,000 to 6,000,000 Visa e-commerce transactions per year.
3	Any merchant processing 20,000 to 150,000 Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 6,000,000 Visa transactions per year.

Source: Visa

In addition to adhering to the twelve security requirements and sub-requirements detailed in the PCI Security Audit Procedures, compliance validation is required for Level 1, Level 2, and Level 3 merchants, and strongly recommended for Level 4 merchants.

Level	Validation Action	Validated By	Due Date
1	• Annual On-Site Security Audit and • Quarterly Network Scan	• Independent Security Assessor or Internal Audit if signed by Officer of the company • Qualified Independent Scan Vendor	9/30/04
2 and 3	• Annual Self-Assessment Questionnaire and • Quarterly Network Scan	• Merchant • Qualified Independent Scan Vendor	6/30/05
4*	• Annual Self-Assessment Questionnaire (Recommended) and • Network Scan (Recommended)	• Merchant • Qualified Independent Scan Vendor	TBD

Source: Visa

Even if the majority of your merchants do not meet the minimum requirements for PCI compliance, there are other good reasons to get them to adhere to these rules. Complying with the PCI standards will help in meeting other state and federal regulations for data security such as, Gramm Leach Bliley (GLBA), Sarbanes-Oxley, HIPAA, just to name a few.

It's safe to say that the card associations are serious about the PCI Data Security Standards. Both Visa and MasterCard impose stiff fines of up to $500,000 to non-compliant merchants. It's also clear that the card associations are also trying to send a strong message to the federal government conveying that they can regulate the payment processing industry without intervention from Capitol Hill.

For more information on the Visa / MasterCard PCI Rules and Regulations, please contact your acquirer or processor and visit the following Websites:

Visa Cardholder Information Security Program:
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_merchants.html

MasterCard Site Protection Program:
https://sdp.mastercardintl.com/

SecurityMetrics:
http://www.securitymetrics.com/

Peter Scharnell is VP Marketing for Electronic Exchange Systems (EXS), a national provider of merchant processing solutions. Founded in 1991, EXS offers ISO partner programs, innovative pricing, a complete product line, monthly phone/web training, integration services, and most of all credibility.

For more information, please visit our website at www.exsprocessing.com or email Peter at peter.scharnell@exsprocessing.com

Electronic Exchange Systems is a registered ISO/MSP for HSBC Bank USA, National Association.