



Credit Card Security for Clients and Vendors

It's a question on the minds of consumers everywhere, especially as they make their way through crowded malls or to online shopping carts this busy holiday season: "Do you take credit cards?" If you're like most businesses and associations, your answer is "Yes." Just keep in mind that there are many new credit card security requirements you should know about to ensure a safe and secure environment for your in-store and online customers. Even if you answered "No," read up on these latest requirements. They will provide you with the information you need to know, as a consumer, before booking your holiday travel or making any other online purchases.

The Facts

Identity theft results from non-secure business transactions every minute of every day. Whether collecting credit card data from customers online or in a physical store, companies must take steps to ensure the security of consumers' private information to prevent identity theft and fraudulent transactions.

- The U.S. Federal Trade Commission's Consumer Sentinel reports that, in 2005, credit card fraud was the most commonly reported form of identity theft, accounting for 26% of all cases of identity theft.
- In a January 31, 2006 study, the Better Business Bureau (BBB) estimates that the identities of 8.9 million U.S. adults would be stolen in 2006, costing \$56.6 billion. In the same study, the BBB found that approximately 43% of victims' identities were stolen through business or online transactions.
- In one incident in July 2005, approximately 40 million credit card accounts were exposed to potential fraud because of a security breach at a third-party processor of payment transactions. In a matter of hours, hackers exported the names, card numbers, and card security codes for nearly 200,000 accounts.

Tougher Standards

Due to a long line of data security breaches in 2005, the main credit card companies—American Express®, Discover®Card, MasterCard®, and Visa® U.S.A.—created a series of stringent requirements designed to protect cardholders and the businesses that accept credit cards. Together, these requirements, released in January 2006, form the Payment Card Industry (PCI) Data Security Standard and govern the safekeeping and destruction of account information, as

well as the use of agents or third parties in maintaining this information and reporting any security incidents.

The PCI requirements are categorized into four distinct levels of online merchants, such that requirements and compliance mechanisms escalate with the merchant's number of annual transactions.

- **Level 1 merchants process more than 6 million credit card transactions each year—online or otherwise—or have suffered a hack or other security breach that caused data to be compromised.** These merchants are required to undergo an annual onsite security audit and to complete a quarterly network scan. The company audit must be performed by a certified auditor. The network scan must be conducted by a qualified independent scan vendor.
- **Level 2 merchants process between 1 million and 6 million transactions online per year.** These merchants must complete an annual PCI self-assessment questionnaire and complete a quarterly network scan. Compliance must be validated by a qualified independent scan vendor and by the merchant.
- **Level 3 merchants process between 20,000 and 1 million transactions online per year.** These merchants must meet the same set of criteria as the Level 2 merchants. They must complete an annual PCI self-assessment questionnaire and complete a quarterly network scan. Compliance must be validated by a qualified independent scan vendor and by the merchant.
- **Level 4 includes all other merchants, regardless of the quantity of their online or in-store transactions.** It is strongly recommended that these merchants complete an annual PCI self-assessment questionnaire, as well as an annual network scan, but validation is not required by a certified party.

Why Comply?

Failure to comply with PCI regulations can result in significant fines from the PCI Data Security Standard (as much as \$50,000 for a first offense and \$100,000 thereafter), as well as the cancellation of payment processing capabilities. But, at the heart of the PCI standards are basic tenets that should govern the behavior of any quality corporation—make sure your internal network and system components are secure and intact; protect your consumers and your employees; guard your credibility.


“As more and more of the general public uses credit cards for auto payments, business-to-business payments and more, it is crucial that consumers have a sense of security,” says Katherine Novikov, CEO of Diamond Mind, Inc., a niche credit card processing company. “These new regulations provide that security, and they are here to stay.”

“Complying,” Novikov continues, “is a form of superior customer service. To fail to do so would be to risk great embarrassment, as well as a loss of consumer confidence should a problem arise.”

Getting Started

As an online or store-based merchant, there are a couple of things you can do to gauge your security status. First, take a system security self-assessment to ensure that you are evaluating the

right items. An information technology survey that will help you to assess the overall security of your network can be found at www.optimalnetworks.com/assessment . While this self-assessment is not a substitute for the questionnaire required by the PCI standards, it is a proactive tool that will help you to identify and suppress security problems before they occur. Next, conduct an external security analysis. Allow an outside company to perform a scan of your systems to see if they have been compromised in any way. A free, external scan can be performed by Diamond Mind Business Services by going to www.diamondmindinc.com . If, after the self-assessment and external scan, you find that your organization has cause for concern, contact an external IT services provider to comprehensively secure your systems—and your customers' transactions.

Heinan Landa is President of Optimal Networks, Inc., a network support and technology management company. He can be reached at 240.499.7900 or hlanda@optimalnetworks.com This email address is being protected from spam bots, you need Javascript enabled to view it .