internet.com

PCI Security: Small E-tailers Face Large Fines if Hacked

By **Kerry Watson**
September 1, 2009

Many small online merchants don't understand much about the powerful technology behind their e-commerce store or how vulnerable this technology is to being hacked. We rarely read about a small merchant's computer system being broken into, because the large ones are so much more spectacular. But some security experts now say it's not a question of if you will be hacked, it's when.

Small merchants...can be fined *$20 to $30 for each stolen card number* (up to a maximum of $500,000).

The Pain of PCI Non-compliance

Small merchants with on-site credit card processing who are hacked and have not put PCI standards in place can be fined $20 to $30 for each stolen card number (up to $500,000). If the breach is large, they may also be required to undergo a forensic audit (the cost of which starts at $10,000), be subject to more stringent standards than other stores of their size and may be sued. In addition to the horrors of dealing with the original breach, this is enough to effectively wipe out any small merchant.

Small Merchants Now in the PCI Spotlight

PCI (Payment Card Industry) Data Security Standards (DSS) are designed to be a baseline minimum standard for credit card security. The standard emerged in 2004 when five separate programs — Visa, Mastercard, Discover, American Express and JCB — were combined into a single standard. Last year the standards council began addressing the Level 4 Merchants who represent the vast majority of online payment. Small merchants are defined as those with fewer than 20,000 Visa transactions, and fewer than 1,000,000 total transactions per year. Most small vendors will fall into this category.

Beginning October 1, 2009, credit card processors and their agents who accept Visa will begin de-certifying all vulnerable payment applications. This means many small merchants will suddenly receive notices that they can no longer accept credit cards unless they have begun steps toward PCI security compliance. The de-certifications must be completed within one year. The time to take action is now, before your store is de-certified.

- The PCI DSS or Payment Card Industry Data Security Standard is a security process to help you identify all parts of your business that are vulnerable to theft. This ranges from how you dispose of and retain paper records, how your network is set up, and how you transmit and store credit card and other personally identifiable information online.
- Merchants who continue to use on-site credit card processing, must answer 195 additional questions on Questionnaire C or D each year, and begin quarterly or monthly security scans of their online store. They must also take active steps to fix any areas that are found to not be in compliance and specify dates by which their stores will be in compliance.
- Questionnaire C is for merchants who use a Point-of-Sale terminal connected to the Internet with a program such as Quickbooks POS. Most of these are small retailers with a bricks and mortar storefront in addition to their online store. Questionnaire D is for everyone else. These lengthy self-assessment questionnaires cover 12 security steps in great detail, including:
  - *Firewall password settings*
  - *Use of secure encryption*
  - *Quarterly scanning of wireless networks*
  - *Anti-virus, anti-spyware and anti-adware programs*
  - *Creation of a company Information Security Policy for employees and contractors*
  - *Shredding, cross-cutting or pulping of paper documents that contain credit card information*
- If any item on your questionnaire is not in compliance, you must specify a date that you expect to be in compliance, and explain what actions you plan to take to achieve compliance.

Article excerpt courtesy of internetnews.com's **ecommerce-guide.com**