Protect Yourself From Credit Card Data Liability

The risks for compromised credit card information are huge, but the responsibility to protect against it is not all on your shoulders.

Integrated Solutions for Retailers, September 2005

Written by Khristen Chapin

You're probably aware of the negative effect a credit card security breach could have on your reputation. But, did you know it could have similarly severe financial repercussions? For example, when a payment processor's network was breached this June, more than 40 million credit card numbers were stolen. That payment processor has contracts with 100,000 retailers. In situations like this, retailers — even though a credit card data compromise occurred outside their operations — could face two potentially damaging consequences.

"The costs card associations face in a credit card data security breach can end up at the retailer," says Bill Pittman, president of TPI Software. "That's part of retailers' merchant agreements, usually in fine print." In the case of the June payment processor breach, more than 14 million of the 40 million compromised card numbers were MasterCard accounts. MasterCard will now contact its cardholders and reissue most, if not all, of those cards, which can cost the card association $39 per account. MasterCard typically works through acquiring banks to establish merchant accounts, and those agreements often pass the liability for those re-issue costs to acquiring banks, who can then pass liability on to retailers.

Other consequences include fines assessed by card associations for noncompliance with the associations' security standards, which can be more than $250,000. An association can even impose restrictions on you or a merchant service provider and prohibit you from processing its transactions.

Credit Card Data Security Responsibility Extends To Your Technology Providers

Pittman's statement makes clear this point: retailers are liable for credit card information security breaches beyond their operational environments. When it comes to compromised security, your technology partners (e.g. payment processors, online shopping cart providers, and even POS software providers) are extensions of your enterprise. With that many opportunities for hackers and information thieves to get into data, how can you protect yourself?

While liability may come back to you, the responsibility of preventing security breaches is not all yours. You've heard of Visa's CISP (cardholder information security program) and MasterCard's SDP (site data protection) program. Those card associations, as well as Discover, American Express, and others, have now streamlined their efforts to spell out security requirements in one set of standards: the PCI (payment card industry) data security standard. "This new standard requires a third party to measure the current data security protocols of a retailer's environment versus the PCI requirements," says Conan Lane, general manager of PNC Merchant Services. "Retailers can find these third parties, called Qualified Security Assessors [QSAs] on Visa's and MasterCard's Web sites."

According to the PCI standard, the requirements apply to all members, merchants, and service providers that store, process, or transmit cardholder data. The standard details 12 key steps that can reduce risks of data breaches and protect liabilities should a breach occur. The 12 steps are as follows:

1. Install and maintain a firewall configuration to protect data.

2. Do not use vendor-supplied defaults for system passwords and other security parameters.

3. Protect stored data.

4. Encrypt transmission of cardholder data and sensitive information across public networks.

5. Use and regularly update antivirus software.

6. Develop and maintain secure systems and applications.

7. Restrict access to data by business need-to-know.

8. Assign a unique ID to each person with computer access.

9. Restrict physical access to cardholder data.

10. Track and monitor all access to network resources and cardholder data.

11. Regularly test security systems and processes.

12. Maintain a policy that addresses information security.

The PCI standard goes into much more detail on each of these 12 points, but many of the requirements are most likely already in place in your operation. “A lot of the standards are basic common sense,” says Kevin Pannebecker, SVP of alliances for Mosaic Software. “All of your systems and data should be behind a firewall. Your systems should be password protected with unique, not default, passwords. All the card associations are trying to do is say, ‘Prove to us this is being done and we’ll feel more comfortable with you.’”

Is Your Payment Processor On The PCI-Certified List?
You are not the only entity in the retail financial chain that stores and processes data. Your technology partners must also provide those security measures. Like retailers, these vendors must also be certified as compliant with the PCI standards through a third party assessor. Visa maintains a list of compliant vendors on its Web site (including when the vendor was certified). Vendors are realizing that, to get business and survive, they must adjust their technology so they’re in compliance. “Concerns reach beyond a cardholder swiping a card,” says Susan Kohl, director of compliance administration for RBS Lynk. “Retailers need to work directly with their payment application provider, e-commerce shopping cart hosts and gateway providers, and payment processors to ensure everyone along the payment processing chain is compliant.”

POS Software And Hardware Providers Should Meet Security Requirements
While the PCI requirements focus on payment processing and stored data security, Visa has established additional guidelines for POS systems, both software and hardware. These guidelines, which are a subset of CISP, are called Payment Application Best Practices (PABP). According to Visa, establishing secure payment applications (when implemented in a PCI-compliant environment) will minimize the potential for security breaches leading to compromises of full magnetic stripe data or CVV2 information. The PABP recommendation consists of 13 points (with details regarding the points listed) similar to the items found in the PCI standard, arranged in a self-assessment form.

However, these guidelines are simply that — guidelines, not requirements. Visa does not have relationships with POS-level technology providers, and therefore cannot require compliance. But, your payment processors can. “The payment processor First Data has required that its POS software partners are in compliance with the PABP guidelines, and others are following suit, which Visa wants to happen — its members should become the enforcers,” says Marco Mabante, VP of compliance and integration for payment technology provider VeriFone. “We have a relationship with First Data that we want to maintain, so First Data can demand that we prove we’re compliant. And we will.”