

PAYMENT CARD SECURITY STANDARDS

BY PETER V. NGUYEN

Stand near the till and it seems as if paying by cash is a thing of the past. Instead, credit cards appear to be the payment method of choice, with point-of-sale terminals humming continuously during store hours. Similarly, paying for goods and services by way of credit card is almost the only option for e-commerce transactions.

According to the Canadian Bankers Association, Canada has more than 61 million Visa and MasterCard credit cards in circulation, accounting for more than \$214 billion in sales in 2006. While only 258,581—or less than 0.5 per cent—of credit cards were used fraudulently last year, Visa and MasterCard card issuers spent over \$185 million to reimburse customers for fraudulent activity thanks to the zero-liability policies on their cards. Further, a recent retail sector study commissioned by Visa Canada reports that 58 per cent of Canadian consumers fear that their credit card information might be intercepted at the point-of-sale (POS).

With so much payment card-handling activity combined with a lack of consumer confidence, it is imperative any business that processes credit card transactions—especially retailers—get serious about the data security standards imposed by payment card companies to protect cardholder data. While these standards are not regulated by government, non-compliance can lead to hefty fines or, in some circumstances, result in a shutdown of a business' entire credit card processing capability. Furthermore, when confidential data is compromised, it can also lead to wary customers and a subsequent decrease in sales.

It was three short years ago that Visa International and MasterCard Worldwide established the global Payment Card Industry Data Security Standard (PCI DSS) which sets out, among other things, the technical requirements for the secure storage, processing and transmission of cardholder data, as well as common auditing procedures, scanning procedures, and a security Self-Assessment Questionnaire. PCI DSS was quickly endorsed by American Express, Discover Financial Services, and JCB International. Last September, these three companies united with Visa and MasterCard to form the independent PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures for payment cards on a global basis.

The PCI DSS “house rules” take a common-sense approach to data security (as it relates to payment cards), calling on businesses to build and maintain secure networks, implement strong access control measures, keep up with maintenance, and monitor and test their IT systems and security processes and procedures regularly. For many small businesses, that could feel like a daunting task—especially when the owner is CEO, head of HR, and IT lead all rolled into one! Even a small busi-



ness with an IT department can feel overwhelmed given the lack of people, funds, and resources available. But it doesn't have to be that way if the right tools are in place and the right people are available to lend a hand.

So where to start? First stop is to check with the "merchant acquirer", the company that provides the hardware and services to facilitate the processing of credit card transactions. A merchant acquirer, such as Moneris Solutions, Chase Paymentech, Global Payments, or other organizations associated with certain banks, examines a business' total payment card processing activity. This would include credit card processing volumes and whether the merchant processes e-commerce transactions. If the merchant acquirer deems compliance necessary (in accordance with its rights under its contract with the business), a timeframe is given by which the merchant is to comply.

The next step is to fill out a lengthy PCI DSS self-assessment questionnaire, which asks important security-related questions, such as whether all Internet routers are secure, whether those employees accessing POS terminals have unique login IDs, and whether there is a formal IT security policy in place. Given the detail involved, many businesses—both big and small—may decide to hire a third-party Qualified Security Assessor (QSA) sanctioned by the PCI Security Standards Council. The QSA assesses the situation, assists the business in completing the survey, and can conduct a network scan (to determine if there are any vulnerabilities in the merchant's network).

The scan, conducted on a quarterly basis as required by the PCI DSS, ensures the computing environment is airtight and that confidential data is secure.

It is also beneficial to check whether the POS terminals

and PIN devices in use are PCI-compliant. Models purchased several years ago might not be and may need to be upgraded. That could prove expensive for a small business owner who may have spent hundreds or thousands of dollars a while back purchasing POS hardware only, to discover that it is not PCI-compliant. Again, while PCI standard compliance is not legally mandated, credit card process agreements typically require compliance with security procedures and processes determined by the merchant acquirer—so if a merchant doesn't comply, they could be in breach of its contract and could face penalties, including the imposition of fines.

Looking ahead, the next big security news related to payment processing set to hit merchants is "Chip and PIN"—chip-embedded credit or debit cards that replace a traditional "swipe and sign" transaction with a Chip and PIN transaction to complete a sale. Visa and MasterCard are already implementing Chip and PIN technology for payment cards in Canada, with full adoption expected by 2010. Small businesses about to replace their POS terminals should consider one that's chip-enabled if buying the terminals outright.

Storing and protecting sensitive information is an important aspect of doing business in today's market, and failing to put the proper security and compliance measures in place can be particularly risky. Remember the recent TJX/TJ Maxx/Winners/Home Sense debacle? Enough said. **E**

SOME DO'S AND DON'TS

There are some basic IT "do's and don'ts" to keep customer and corporate data safe from outside eyes. While they may seem obvious, they are, unfortunately, among the most overlooked areas. Here are some of them, many of which are PCI DSS house rules:

- ✓ When installing a wireless router, be sure to activate the security feature. The same goes for encryption technology—do not forget to turn it on and remember to change the manufacturer's default passwords. Install a firewall and test it regularly.
- ✓ Be sure to install software patches as soon as the vendor announces them. And do not forget to check regularly for new patches.
- ✓ Do not store all of the information that may be available on the credit card's magnetic stripe. As needed, keep only the account holder's name, credit card number and the expiration date, and then only for a limited amount of time. Never store the card-validation or card-verification code (those extra three digits on the back of the card), as the PCI standard requires organizations not store this data.
- ✓ Restrict access to the corporate database to only those individuals that have a "need-to-know" and ensure that access is by way of password-only access.
- ✓ Create strong passwords—not your dog's name or your son's birthday—that include both numbers and letters and uncommon words.
- ✓ Change passwords regularly, and be sure former employees have no access after they leave the company.
- ✓ Do not forget about physical security—use codes and passkeys for doors to restrict access to certain areas.
- ✓ Maintain a formal policy to address information security.

Peter V. Nguyen is an associate lawyer in the Toronto office of national business law firm Fraser Milner Casgrain LLP. He regularly

advises businesses on legal matters related to information technology, data security, privacy, and payment cards. He was previously in-house legal counsel to a leading Canadian merchant acquirer as well as an innovative stored-value payments company. He welcomes comments at peter.nguyen@fmc-law.com. For more information on the PCI DSS standard and a list of QSAs, visit www.pcisecuritystandards.org.