



ON GUARD!

THE ONLY THING YOU CAN'T DO IS NOTHING

**The payment card landscape is changing,
and retailers need to be ready.**

By **Chris Anderson**, CA (NZ), CISA, CMC, CISSP, PCI DSS QSA, National Leader of Information Security Services, and **Bashir Fancy**, Special Adviser, Business Risk, Grant Thornton LLP

On guard! In fencing, it's the position of complete preparation. It means you're ready to both take action and defend yourself, and merchants conducting payment card transactions in today's business environment definitely need to be "on guard." By taking action to address new compliance requirements in the upgraded Payment Card Industry Data Security Standard (PCI DSS), you can defend yourself against the current proliferation of payment card crime while avoiding the potential negative consequences of non-compliance.

Changes to the PCI DSS may have a substantial impact on some retail merchants. If you're not in compliance or at least able to show you're moving towards it, consequences begin at serious and end at catastrophic. Reputation damage, increased transaction fees, loss of revenue, disruptive forensic investiga-

tions (at your cost), potentially crippling fines: the risk of non-compliance is one no retailer can afford.

Action—get compliant

The good news is that the new standard is not designed to punish retailers, but to help them and the consumers they serve. Yes, those who do not comply face increasingly stiff punishment, but those who do will see a number of benefits, such as increased consumer confidence and financial security, as well as a substantial reduction in their own liability. Whether you do it internally or engage the PCI compliance services of a QSA (Qualified Security Assessor)-certified audit firm, you must report on the extent to which you are compliant with the PCI DSS by October, 2010; if you are not fully compliant, you must have a plan to address remaining gaps.

PCI transaction compliance levels for merchants

Level 1: \$6M +/-year (also anyone with a previous data security breach)

Level 2: \$1M to \$6M.

Level 3: \$20k to \$1M.

Level 4: Up to \$20k.

There are several specific actions retailers can take right away to get the PCI DSS compliance ball rolling:

Find out the extent of your responsibilities

If you're conducting payment card transactions under the umbrella of a franchise where credit card processing functions are being provided by head office or a franchise management company, examine your agreements to verify the level of your obligations and liabilities. What are your obligations to the acquiring bank? Are you considered the merchant or is the franchisor the merchant? If there is a master merchant agreement in place, individual franchises may have a higher PCI DSS compliance level than they suspect, as well as the corresponding increased responsibilities and liabilities.

Get your Chip and PIN terminal

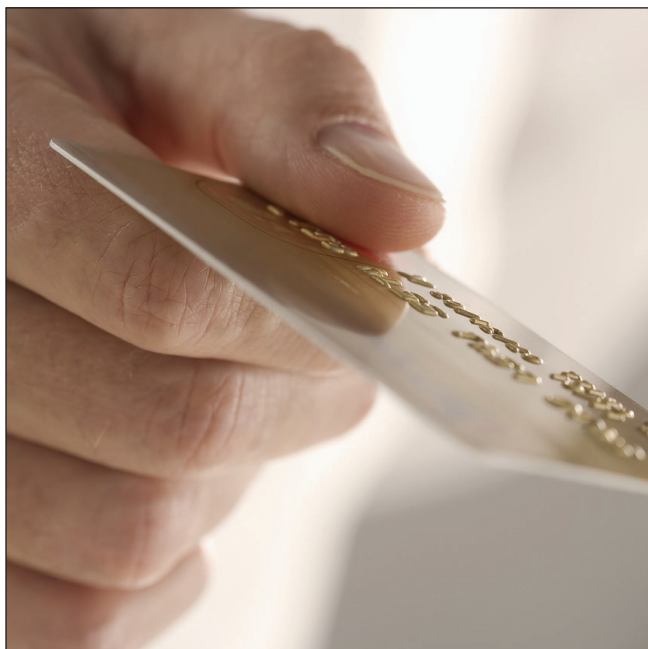
Your Chip and PIN point-of-sale systems must be in place by October 2010. This is to your benefit. If you are Chip and PIN compliant by October, 2010, you will not be liable for fraud that occurs after that date involving magnetic stripe cards used at your terminal. Criminals will be increasingly targeting these individuals since magnetic stripe cards are much easier to compromise, but the liability will revert to the customer who has chosen not to take advantage of your compliant payment and security technology.

Discard unnecessary data

What data is being collected during payment card transactions by your Customer Relationship Management (CRM) system? Get rid of any names, expiry dates and payment authorization data, and try to ensure such data is not collected in the future. Also, do not keep "merchant copy" transaction receipts in the till.

Make sure quarterly scans are done (e-commerce)

If you conduct any payment card transactions via your website, you must ensure your e-commerce systems are secure by having a quarterly scan conducted by an Approved Scanning Vendor, even if you have outsourced the hosting and management of your website to a third party. (You should also consider whether



you're breaching the privacy of Canadian customers if you outsource to vendors who store information on servers located in the U.S.).

Defence—you are the target

The criminals behind payment card crime are highly sophisticated and expert at recycling schemes and shifting to the easiest target. With the recent focus on tightening e-commerce security for merchants at PCI Compliance Level 1, criminals are now concentrating on Level 3 and 4 businesses who are not yet up to full speed in terms of security oversight. For criminals who have honed their skills on larger corporations, smaller merchants with minimal security are now easier and cheaper to target. If this applies to you, the best defence really is a good offense. Review your current information security measures against the 12 PCI DSS requirements, and make the right information security improvements to manage your risk and achieve full compliance as soon as possible. Make the PCI DSS work for you. **HM**



Chris Anderson leads an expert Grant Thornton team who provide creative and innovative solutions to complex technology risk management challenges faced by organizations today.



Bashir Fancy has successfully assisted clients globally in understanding and applying a risk-based approach to achieving sustainable compliance, governance and fraud prevention as it relates to the payment card industry.