

# Out of the breach

---

## A Grant Thornton article

By Chris Anderson, CA(NZ), CISA, CMC, CISSP, Business Risk Services and Bashir Fancy, Special Adviser - Business Risk Services, Grant Thornton LLP

## There's "no compromise" when it comes to payment card data.

"It could happen to you." A caution we've all heard. And "it" has happened to most of us at one time or another: an accident, a theft, an injury—inconvenient and painful, perhaps, but usually regarded as an unpleasant glitch in life from which you happily move on. But when "you" are a company or organization whose business depends heavily on the secure processing of payment transaction card data, "it" can be disastrous and far-reaching.

The last several years have seen an increase in security breaches involving sensitive data: TJX companies, and payment card processors CardSystems Solutions and Heartland Payment Systems, for example. And while targeted attacks like these are serious enough, consider the Australian IT worker who discovered data for thousands



of active credit cards<sup>1</sup> on-line—accidentally—or the student researchers who purchased “recycled” hard drives in Ghana<sup>2</sup> that contained, not only the personal data of several families, but classified information pertaining to U.S. Department of Defense contracts. The implications of this apparent trend, given the relatively borderless nature of Internet commerce, are global in scope.

The costs associated with such breaches are considerable. While individuals whose data is compromised may be adversely impacted by identity theft and financial loss, breached organizations may also be affected, suffering damage to their income and reputation, as well as a loss of customer confidence that can be severe. Beyond that, such companies spend an estimated US\$202 per customer record<sup>3</sup> to manage the cleanup (fines, card replacement, goodwill retention, credit counselling), a material cost that can add up rather quickly when the financial records in question number in the tens of thousands—or millions.

**From the obvious players—payment card service providers and retail businesses—to entities as disparate as universities, municipalities and charities, the threats the payment card industry (PCI) is currently experiencing are a genuine concern.**

### **The foundation is solid**

A great deal of work is being done to reduce data security breaches. The PCI Security Standards Council, created in 2006 by the five major payment card companies (Visa, MasterCard, American Express, JCB and Discover), has developed a set of 12 comprehensive security requirements—the Data Security Standard (DSS)—with which organizations involved in the PCI must comply. Every aspect of the industry is impacted by these regulations, from processes to enabling technologies. In an attempt to achieve industry-wide compliance—and consequently industry-wide security—the council has undertaken to train and certify a global network of Qualified Security Assessors (QSAs) to determine whether organizations are in full compliance with the DSS. Companies who are not can face penalties and are, of course, required to become compliant. Moreover, these efforts have attracted regulatory attention. Three US states have put key elements of the PCI standards into law, and recently in Canada, with the introduction of Bill S-4 into law (which amends the Criminal Code with respect to identity theft), there is growing pressure on businesses to comply.

The formation of the PCI Security Standards Council and the work done by the card companies have been extremely beneficial. First of all, the companies have created an independent governing body to manage the PCI standards and keep them updated. Secondly, they provide oversight for an industry that is facing



major issues as its technological capabilities grow as fast as—but no faster than—those of the criminal element that assaults it. The card companies are responsible for the enforcement of the standards. They've brought these issues to the forefront of the industry and into the public eye, responding quickly to security issues and showing true commitment to continued vigilance and ongoing improvement. Most importantly, the converging of security standards by the five major card companies has led to the content of the DSS, an extensive and inclusive set of requirements against which the security of individual card processing organizations can be effectively measured. In short, they've made huge strides in enhancing the security of individuals and businesses alike. The question is, what can be done to enhance the ability of businesses to achieve and maintain compliance with the DSS?

### Fortifying the walls

The standards developed and embodied in the PCI DSS are strongly designed, but there may well be a way to increase their practical application while achieving efficiencies in meeting a broader range of assurance needs. Your external auditor may have the ideal combination of experience and qualification in both information security and information systems assurance to help. External auditors have been determining compliance, building credibility and perfecting an audit-infrastructure for more than 100 years, and certain audit practitioners have extensive training and experience in reporting to third parties on the adequacy of internal controls and security.

### Taking the next step

The advantages of using professional auditors for PCI DSS compliance reports are numerous. Audit firms bring to the table not only vast experience, but the advantage of working within an audit structure that clients already understand. For example, Canadian companies that have outsourced significant parts of their financial processes and/or underlying IT, as well as companies that provide those services, will no doubt have experience with a CICA Section 5970 audit, which provides clients and their financial auditors with independent assurance on the design and operation of relevant internal controls over financial information. Any company with a head of internal audit or audit committee will be familiar with the approach, processes and documentation that audit firms apply—and which they also apply to PCI DSS compliance reports. Moreover, audit firms can provide a separate audit report, under Canadian Institute of Chartered Accountants (CICA) standards, that can be supplied to the client's own customers, attesting to such compliance under the high assurance standards already in place for professional audit firms.

As a further asset, clients can access integrated audit advice that delivers a genuine advantage. Instead of coming in, doing a one-off compliance report and moving on, auditors can do audit work on payment card technology and processing; customer service controls; internal controls for financial reporting; privacy controls for sensitive data—work that's common to, and linked to, a broader range of governance and compliance requirements. In other words, audit once, assure many times—

with a Sarbanes-Oxley Section 404 report; a privacy controls report; a report in support of the issuance of a Web Trust seal for Internet-based commerce; or a report in accordance with CICA Handbook Section 5815 (Special Reports: Audit Reports on Compliance with Agreements, Statutes and Regulations)—all in addition to the PCI Report on Compliance and all performed under generally accepted audit standards and procedures.

Essentially, auditors draw on a quality-of-service commitment that is hard to match in its breadth or background, and it's an industry whose own integrity and compliance are highly regulated. Audit professionals understand and respect the expectation of a completely independent assessment of PCI DSS compliance. Fulfilling this expectation is, and has always been, at the heart of the audit engagement process. The industry at large is committed to the spirit of independence and to a long tradition of upholding rigorous assurance standards.



The upside to consulting a QSA-certified professional audit firm is clear for larger businesses that must have an independent audit report completed, but all businesses that conduct payment card transactions are expected to be compliant. With Visa and MasterCard, for example, businesses with lower credit card transaction volumes are allowed to complete a self-assessment questionnaire (SAQ) that must, in Canada, be signed off on by a QSA to verify accuracy. If you're a smaller business, there may be an advantage to using the services of an audit firm that can thoroughly evaluate your processes as well as provide sign-off on audit compliance.

### Building our credentials

The audit profession has continuously adapted to meet the evolving needs of clients and the economies in which they operate. From simple fraud-detection objectives through broader assessments of corporate financial well-being to contemporary risk-based approaches, the audit profession itself has evolved with the times. More audit professionals becoming credentialed QSAs and offering PCI DSS compliance assurance could mean significant advantages to their clients.

With the work already done by the card companies and, subsequently, the PCI Council—Visa is taking a leadership role in setting firm deadlines for PCI compliance, and MasterCard is now

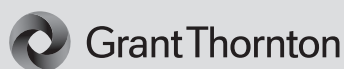
publishing fines for PCI DSS non-compliance—the system is getting better all the time. And the increased involvement of audit professionals in delivering relevant compliance and audit services would be an excellent addition.

For more information, visit [www.GrantThornton.ca](http://www.GrantThornton.ca).

<sup>1</sup> Source: "Several thousand credit card accounts exposed in cache search." *The Tech Herald*, March 24, 2009, <http://www.thetechherald.com/article.php/200913/3291/Several-thousand-credit-card-accounts-exposed-in-cache-search> (accessed September 19, 2009).

<sup>2</sup> Source: "B.C. students buy sensitive U.S. defence data for \$40 in Africa." *CBC*, June 24, 2009, <http://www.cbc.ca/technology/story/2009/06/23/teche-waste-ghana-data-british-columbia-journalism-students.html> (accessed September 19, 2009).

<sup>3</sup> Source: Ponemon, Dr. Larry, "Fourth Annual US Cost of Data Breach Study, Benchmark Study of Companies." *Ponemon Institute*, January 2009, <http://www.ponemon.org/local/upload/tckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf> (accessed September 19, 2009).



[www.GrantThornton.ca](http://www.GrantThornton.ca)

Audit • Tax • Advisory  
Grant Thornton LLP. A Canadian Member of Grant Thornton International Ltd. Some of the defined services may be provided by an associated entity of Grant Thornton LLP.

#### About Grant Thornton in Canada

Grant Thornton LLP is a leading Canadian accounting and advisory firm providing audit, tax and advisory services to private and public organizations. Together with the Quebec firm Raymond Chabot Grant Thornton LLP, Grant Thornton in Canada has more than 3,100 people in offices across Canada. Grant Thornton LLP is a Canadian member of Grant Thornton International Ltd, whose member and correspondent firms operate in over 100 countries worldwide.

© 2010 Grant Thornton LLP. We have made every effort to ensure information in this publication is accurate as of its issue date. Nevertheless, information or views expressed herein are neither official statements of position, nor should they be considered technical advice for you or your organization without consulting a professional business adviser. For more information about this topic, please contact your Grant Thornton adviser. If you do not have an adviser, please contact us. We are happy to help.