Barbarians at the Firewall: Data Breaches, Cross-Border Commerce and Notification Requirements in Canada and the United States

The fallout for companies from data breaches is immense, as consumer trust and investor confidence is eroded and the financial costs run into millions of dollars

BY GEORGE J. POLLACK; DAVIES WARD PHILLIPS & VINEBERG LLP

CYBERCRIME, principally data breaches and the theft of personal and corporate information, now ranks as one of the top economic crimes worldwide. Cybercriminals do not discriminate. Hackers are truly equal-opportunity actors.

There is no area of the world, no company, no government agency and no sector of the economy that is immune from cyberattack. Iconic companies such as Target, Blue Cross Blue Shield, Anthem, Neiman Marcus, Home Depot, T.J. Maxx, Sony, J.P. Morgan and Heartland Payment Systems have suffered data breaches. Government offices, including, most recently, the Office of Personnel Management in the United States, have likewise been targeted. As *Fortune* magazine (July 1, 2015) put it, quoting an old line, in an article about the hacking of Sony Pictures ("The Hack of the Century"), there are two kinds of companies: "Those that have been hacked, and those that don't yet realize they've been hacked."

Retailers have been especially vulnerable to data breaches. According to the *2014 Trustwave Global Security Report*, retail was the top industry compromised by data breaches, accounting for 35 percent of attacks investigated. The food, beverage and hospitality industries accounted for 29 percent of total breaches. Finance and professional services accounted for a further 17 percent of intrusions.

The fallout from data breaches is enormous. The consequences of a hack can damage company performance for years. The financial costs alone – in terms of investigation, containment, remediation, credit card replacement expenses, credit-monitoring expenses, regulatory fines, penalties imposed by credit card brands and litigation – can be significant, running to the millions and even tens of millions of dollars. For example,

"Although the benefit of electronic-based business is undoubted, companies carrying on business through the Internet should adopt policies for dealing with data breaches, including notifying potential users and regulatory authorities."

The New York Times (August 5, 2014) reported that the data breach suffered by Target cost the company $148 million. Home Depot's quarterly SEC filing indicated that it incurred $43 million in data-breach-related expenses in the third quarter of 2014 alone. According to a report issued by IBM and the Ponemon Institute in May 2014, the average cost of a data breach for the companies it surveyed across all sectors of the economy was $3.5 million. And a study published in 2014 by McAfee (*Net Losses: Estimating the Global Cost of Cybercrime*) estimated the total cost of cybercrime to the global economy at more than $400 billion.

In addition to the direct economic cost of an intrusion, data breaches usually have serious reputational consequences for the breached entity. For example, intrusions can have a negative impact on how the company is viewed by consumers and investors alike. Data breaches erode consumer trust and investor confidence. The recent hacking of the Ashley Madison website is a graphic, if not unique, example of the way a data breach can call into question the long-term viability of an online company's business model.

In some instances, data breaches have led to the loss of shareholder value. For example, Heartland Payment Systems, one of the largest processors of credit card transactions in the United States, suffered a data breach in 2008 that resulted in the exposure of account data linked to over 100 million credit cards issued by more than 650 financial service companies. That intrusion is reported to have cost the company almost $40 million. Worse still, following the announcement of the breach, Heartland's stock price plummeted 77.6 percent.

Data breaches have also spawned class-action litigation on both sides of the 49th parallel, involving, among others, Sony Corporation, Home Depot and Target. Forty-four lawsuits were commenced against Home Depot in Canada and the United States. Jurisdictional considerations have placed some restrictions on class-action plaintiffs regarding their ability to file suit in a cross-border breach context. A class action commenced against Target before the Superior Court of Québec was dismissed on March 23, 2015, on the grounds that the court did not have jurisdiction over Target. In coming to this decision, the court noted that by the plaintiff's own admission, the breach occurred in the United States and affected only persons who shopped there. In fact, it was for this reason that Target's Canadian subsidiary – which had in the interim ceased its operations and sought creditor protection under the *Companies' Creditors Arrangement Act* – was not named as a defendant in the Québec proceedings.

Technology has turned the world into a highly connected place. In many ways, the Internet has dissolved the traditional boundaries of cross-border commerce. The Internet – and especially the e-commerce phenomenon – has given even the smallest of businesses a global reach. Although the benefit of electronic-based business is undoubted, companies carrying on business (in whole or in part) through the Internet should adopt policies for dealing with data breaches, including notifying potential users and regulatory authorities. These policies must take into account that an intrusion may require the organization to comply with many extraterritorial regulatory schemes dealing with data-breach notification.

Many European countries, and an increasing number of jurisdictions in the United States, require businesses and other organizations to report the unauthorized accessing of personal or financial information to the authorities. In Canada, legislation at the federal level (the *Personal Information Protection and Electronic Documents Act*, or PIPEDA) and some provincial jurisdictions establish obligations regarding the collection, use, disclosure and handling of personal information. For now, however, there are few mandatory reporting requirements in Canada following a data breach.

On June 18, 2015, the *Digital Privacy Act* (the Act) came into effect in Canada. It amended PIPEDA by introducing significant amendments to the private-sector privacy regime. The amendments include mandatory data-breach notification rules. However, those rules will only come into force once regulations are complete.

Once in effect, the mandatory notification rules introduced by the Act will require an organization to report a data breach to the Privacy Commissioner if the organization reasonably believes that the intrusion creates "a real risk of significant harm to an individual." The assessment of what constitutes a real risk of significant harm will be based on a number of factors, including the sensitivity of the information compromised and the probability that the information in question has been, is being or will be misused. "Significant harm" is broadly defined and includes bodily harm; damage to reputation or relationships; humiliation; loss of employment; financial loss such as the impact on a person's credit record; identity theft; and damage to or loss of property. In these cases, the breached entity must do the following:

- Report the breach to the Privacy Commissioner as soon as feasible.
- Notify the individuals affected (unless prohibited by law from doing so). Such notification must be conspicuous and must, if possible, be given directly to the individuals affected.

The notice must be sufficiently explicit to allow the individuals to understand the significance of the breach and take whatever remedial steps may be required.

- Notify other organizations, including the government, if notification can mitigate the risk resulting from the breach.

Failure to comply with the Act's data-breach rules can result in fines of up to C$100,000.

PIPEDA's reporting requirements will apply to any organization that collects, uses or discloses personal information in the course of commercial activities, including federal works, undertakings and businesses.

Although Ontario, Newfoundland, New Brunswick and Nova Scotia have enacted legislation requiring notification in the event of the compromise of health-related personal information, only Alberta currently has a private sector-wide data-breach notification requirement. In that province, the *Personal Information Protection Act* (PIPA) requires organizations to notify the Alberta Privacy Commissioner if personal information under their control is accessed without authorization in circumstances in which a reasonable person would consider that there exists a real risk of significant harm to an individual.

The Alberta Privacy Commissioner may in turn require the breached entity to notify the affected individuals if he or she determines that there is a real risk of significant harm as a result of unauthorized access or disclosure. Factors to be considered under PIPA in order to determine whether a real risk of significant harm exists include the number of individuals affected, the maliciousness of the breach, the sensitivity of the information, whether there are indications that personal information was misappropriated for nefarious purposes and the harm that could result.

Manitoba passed the *Personal Information Protection and Identity Theft Protection Act* (PIPITPA). PIPITPA contains a broad breach-notification obligation that will, once in force, require an organization that collects or uses personal information to notify an individual if personal information in its control or custody is accessed, stolen or lost in an authorized manner. Unlike PIPEDA or PIPA, there is no "real risk of significant harm" threshold. Nor is there any obligation to notify the Privacy Commissioner of a data breach.

Although the United States does not currently have a broad-based data breach notification law, on January 12, 2015, President Obama proposed the *Personal Data Notification & Protection Act*. This legislation would create a federal standard for data-breach notification. It would apply to a wide variety of "sensitive personally identifiable information." It would also require notification directly to the individuals concerned and through the media if a security breach creates a risk of harm. If a breached entity determines that a risk of harm exists, it must notify the Federal Trade Commission within 30 days of discovering the breach. Businesses would also be required to notify federal law enforcement and national security authorities of a data breach if the sensitive personally identifiable information of more than 5,000 individuals was accessed or acquired or if the intrusion involved a data system containing sensitive personally identifiable information of more than 500,000 persons across the United States.

The majority of states have enacted data-breach notification laws applicable to affected individuals resident in such jurisdictions (a complete list of the relevant state laws may be found at www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx). The various state laws are similar, but they do have significant variations, including what constitutes a breach that triggers the obligation to notify. In many jurisdictions within the United States, time is of the essence when reporting data breaches.

In addition, companies in industries such as banking and financial services, insurance and healthcare may be subject to certain state and federal industry-specific breach notification requirements.

Regulatory authorities at both state and federal levels in the United States can impose significant fines and penalties for non-compliance with notification requirements, including late notification. In some cases, a breached entity's exposure to fines and penalties will increase if it is found not to have complied with applicable data privacy and security standards. For example, companies subject to regulatory scrutiny by the Federal Trade Commission may be subject to enforcement for unfair or deceptive acts or practices under the *Federal Trade Commission Act*. The FTC has interpreted "unfair acts or practices" to include the failure to adopt appropriate data-security measures to protect personal information and has brought enforcement actions against companies that have suffered data breaches.

The application of various state laws is typically based on the place where the person whose data was compromised resides. In many cases, state laws will apply irrespective of where the breached entity's place of business is located or where the compromised information was held. This means that Canadian companies could be subject to US state data-breach legislation requiring them to give notice to United States-based customers in the event of a data breach. It is critical, therefore, that Canadian companies with customers located in the United States be aware of potential reporting requirements when faced with a data breach.

George J. Pollack

Davies Ward Phillips & Vineberg LLP

Tel: (514) 841-6420
Fax: (514) 841-6499

gpollack@dwpv.com

George J. Pollack is a partner in Davies' Litigation practice. He regularly acts on behalf of public and private companies on a wide variety of complex commercial litigation matters, including investigations and litigation arising out of data breaches and other cybersecurity-related matters, extraordinary remedies, debt recovery, the enforcement of foreign arbitration awards and judgments and specialty insurance and contractual disputes.

George has represented clients before the courts at all levels of the Province of Québec and throughout the country, including the Supreme Court of Canada. He also advises clients in their dealings and appearances before various administrative tribunals. In addition to his litigation practice, George acts as an arbitrator and a mediator. He is a member of the Québec and Ontario Bars.