Blaney McMurtry LLP

PUBLICATION

Variety of Protections Open To Businesses Exposed To "Panama Papers" — Type Data Breaches

Date: June 01, 2016

Original Newsletter(s) this article was published in: Blaneys on Business: June 2016

The recent “Panama Papers” scandal is a timely example of the impact that a data breach can have on high net worth individuals, businesses and law firms.

The scandal, which involved the leak of more than 11.5 million documents from the Panamanian law firm Mossack Fonseca, has implicated numerous lawyers, accountants, financial professionals and individual clients, through the involuntary disclosure of confidential information, in alleged efforts to escape income tax obligations.

The information leaked included emails, contracts, transcripts, scanned documents, PDFs and photos. These documents publicly disclosed thousands of transactions, many legal, but also many which revealed ties to offshore accounts used for tax evasion, fraud or financial misconduct. The data cover almost 40 years and nearly 214,000 offshore entities in 21 jurisdictions around the world.[1] The data breach highlights the significant risks that exist for companies in possession of sensitive client information.

Regulators around the world, including the US Department of Justice and various European financial watchdogs, are investigating certain individuals and companies now that such information has come to light. The breach has implicated business people, athletes, celebrities, and political leaders, including UK Prime Minister David Cameron, certain Bollywood film stars, and the Prime Minister of Iceland, who stepped aside as a result of the scandal. Closer to home, the Canada Revenue Agency recently sought a court order to obtain information from the Royal Bank of Canada regarding its clients that have a connection to Mossack Fonseca. RBC or its affiliates registered 429 offshore corporations through the Panamanian law firm.[2]

Although many of the stories in the media surrounding the scandal have focused on the tax evasion implications of the data breach at Mossack Fonseca, it is important that Canadian

businesses re-examine their information security practices in order to reduce the associated liabilities that can occur when private information is disclosed involuntarily.

Data breaches

A data breach occurs when data is stolen or taken from a system without the knowledge or permission of the system's owner,[3] or when the holder of information accidentally loses control of it. This type of data can include personal identifying information such as banking information, social insurance numbers, addresses, phone numbers, medical records, email addresses, usernames and passwords.

There are various ways that businesses can be targeted. Hackers commonly exploit outdated software or insecure systems, or trick employees, often by phony emails, into revealing usernames and passwords (known as spear-phishing). According to a leading security software producer, Symantec, spear-phishing campaigns targeting employees increased by 55 per cent in 2015.[4]

Other causes of a data breach include lost, stolen or improperly disposed-of devices; malware (malicious software designed to damage a computer, such as viruses, worms, spy ware, and Trojan horse programs); or disgruntled employees releasing information. In the case of Mossack Fonseca, there is a suspicion that the data breach was made possible by the failure to update outdated software on the firm's web server.

A data breach can be very costly to a business (or, in situations like that facing Mossack Fonseca, potentially catastrophic). Expenses associated with responding to the breach and repairing weaknesses in computer systems can be significant. Other costs that are more difficult to quantify are also likely to result, including reputational damage, loss of business, and loss of goodwill.

Lawsuits, particularly class actions, related to damages for the disclosure of information or breach of privacy are becoming much more frequent. Ontario courts have thus far recognized two privacy-related torts: intrusion upon seclusion and, more recently, public disclosure of private facts. There may also be costs incurred related to client notification, investigation of the breach, identity theft and credit monitoring, and disruptions to normal business operations.

Other major data breaches have occurred across different industries including healthcare, banking, financial services, technology, education, government, and retail.

In 2014, approximately 56 million debit and credit cards and 53 million email addresses were stolen from Home Depot via malware after the company's network was initially breached using a third party's username and password.[5]

Home Depot reported a cost of $232 million for its data breach, with insurance covering $100 million. Insurance Business America has anticipated, however, that the cost could reach into the billions.[6]

A data breach at Target in 2013 compromised 40 million credit and debit cards which affected 70 million customers after a third party's login credentials were again stolen and malware infected the point of sale system.[7] By August 2015, Target estimated that the data breach could cost $264 million, with approximately $90 million covered by insurance.[8]

Law firms, accounting firms and other companies offering professional services may suffer more severe ramifications than other types of businesses because of the high degree of trust that clients place in them. These businesses possess sensitive client information and confidentiality is critical to the services they offer. The release of client information could have a large impact on a firm's credibility and impair its business significantly. Although it is too soon to know what effect the data breach will have on Mossack Fonseca, the firm has acknowledged that its image has been damaged.[9]

Protection against breaches

There are various ways in which a business can guard against data breaches. Cyber insurance, which provides third and first party coverage, can be purchased. This coverage could include investigation and remediation of the breach, business interruption, notification expenses, public relations and network security.

Although cyber insurance can shield businesses against some of the financial risks of a data breach, a strong information security and risk management policy is crucial to protect a company's sensitive information. Strong information security, such as up-to-date systems with robust security software, encrypted databases, and malware detection, generally is a requirement for insurance. Good information security and risk management policies should also focus on preventing inadvertent disclosure by employees. For example, staff should be trained so that they do not reveal passwords to people over the phone and are able to identify phishing emails. Procedures should also be in place to destroy data, where possible, when it is no longer needed.

Businesses should have a data breach response plan in place to mitigate damage if a breach occurs. A plan may include assembling data breach response team members, which could include IT staff, upper management, human resources, public relations as well as privacy lawyers. The team could help develop data security policies, train employees, and implement a response plan in the event of a breach.

According to federal legislation that applies to the collection, use and disclosure of personal information by organizations in the course of commercial activities, organizations will soon have to notify the Privacy Commissioner of Canada and individuals whose personal information has been breached if the breach creates a "real risk of significant harm".[10]

A data breach may be unavoidable in certain circumstances, however, having and implementing a data protection plan will go a long way to minimizing risk exposure. Of course, a business experiencing a significant breach should enlist professional assistance at the outset to help navigate the risk.

Blaney McMurtry LLP helps clients manage data breach risks by taking into account the particular circumstances of a given business. The firm's skilled lawyers in the areas of cyber, information and privacy risk can advise and help clients navigate the risks associated with advances in technology. Its practice areas include privacy, crisis and reputation management, fraud investigation recovery and enforcement, e-commerce, technology contracts and transactions, litigation dispute and resolution, information and technology insurance coverage, and employment & labour. Please contact us for more information.

Laina Smith is an associate in Blaney McMurtry's Corporate & Commercial Practice Group. She holds a law degree from the University of Windsor and a master of arts degree from the University of Toronto.

---

[1] ICIJ, "Giant Leak of Offshore Financial Records Exposes Global Array of Crime and Corruption" (3 April 2016), online: ICIJ <https://panamapapers.icij.org>.

[2] Robert Cribb and Marco Chown Oved, "Taxman wants Royal Bank's Panama Papers client list", *Toronto Star* (5 May 2016), online: Toronto Star <https://www.thestar.com/>.

[3] Trend Micro, "Data Breach", online: Trend Micro <http://www.trendmicro.com/>.

[4] Symantec, "Internet Security Threat Report" (Volume 21, April 2016), online: Symantec <https://symantec.com/>.

[5] The Home Depot, "The Home Depot Reports Findings in Payment Data Breach Investigation" (6 November 2014), online: The Home Depot <https://corporate.homedepot.com>.

[6] The Home Depot, "Home Depot Inc filed this Form 10-Q on 08/25/2015" (25 August 2015), online: The Home Depot <http://ir.homedepot.com/>; Caitlin Bronson, "Home Depot cyber attack costs could reach into the billions" (1 October 2015), online: Insurance Business America <http://www.ibamag.com/>.

[7] Jim Finkle and Mark Hosenball, "Target says criminals attacked with stolen vendor credentials" (30 January 2014), online: Reuters <http://uk.reuters.com/>; Becky Quick, "Target CEO defends 4-day wait to disclose massive data hack" (12 January 2014), online: CNBC <http://www.cnbc.com/>.

[8] United States Securities and Exchange Commission, "Target Form 10-Q Quarterly Report", (25 August 2015), online: Securities and Exchange Commission <http://www.sec.gov/>.

[9] Mossack Fonseca, Statement, "Mossack Fonseca & Co. rejects the recent dissemination of false information" (10 May 2016), online: Mossack Fonseca <http://mossfonmedia.com/>.

[10] Innovation, Science and Economic Development Canada, “For Discussion - Data Breach Notification and Reporting Regulations” (4 March 2016), online: Innovation, Science and Economic Development Canada <https://www.ic.gc.ca>.