INTO THE BREACH: EFFECTIVE LOSS CONTROL

By. Jessie Bellam, Associate & Alex Robineau, Summer Law Student
McCague Borlack LLP

1. INTRODUCTION

Recent advances in technology have brought about a new age in which commercial enterprises have unprecedented access to the information of private individuals. The positive aspects of these advances are noteworthy; from one-click purchasing online, to targeted marketing and metric analysis, data collection has become an indispensable tool in 21st century commerce. However, enhanced efficiency and practicality come with their own set of costs, the most notable being the risk of data breach. Private entities entrusted with confidential information are becoming increasingly scrutinized, and one mishap with this valuable data can have devastating consequences, both for company and consumer.

Despite significant efforts to develop comprehensive *ex-ante* measures to prevent and diminish the impact of data breaches, there is industry consensus that some manifestation of a breach is inevitable. Accordingly, it is critical for corporations to understand their legal responsibilities relating to this issue and to develop strategies to manage data breaches *ex-post*. The following paper will begin by summarizing the types of breaches and their effects. It will then consider legislative requirements for private organizations. Finally, the paper will provide a series of practical steps a company can take to mitigate losses a breach materialize.

2. TYPES OF DATA BREACH

Regardless of size, specialization or location of the organization collecting data, when it comes to a security breach the question is often "when" rather than "if" one will occur. An initial step to limiting the impact of a data breach is to gain a better understanding of the different types of possible breaches and how they can occur.

(a) MALICIOUS VS NON-MALICIOUS BREACHES

The term "data breach" is often associated with an entity having succeeded in forcefully breaking into an organization's network to extricate information. However, data breaches tend to be more frequently associated with human error, such as employee or contractor negligence, or system

error or malfunctions, while breaches caused by malicious insiders or external attacks remain less common.[1]

The former can be characterized as non-malicious breaches and can be more appropriately described as a loss of confidential information. An examples of a non-malicious breach would include an employee or contractor charged with supervising records of personal information misplaces them, resulting in the risk of these being accessed by an unauthorized party. The risk of harm in non-malicious breaches is typically minimal but the fact that personal information has been compromised nevertheless exposes an organization to potential exposure and necessitates post-breach procedures.

In the case of malicious breaches, where a criminal insider or outsider steals information assets, the express purpose of the breach is to gain illicit profits from the information resulting in the potential for more significant damages.

(b) NATURE OF THE DATA LOSS

Another element to consider when reviewing a data breach is the type of information that is lost or stolen. Although breaches relating to confidential employee information or business information are serious, the most damaging breaches involve the loss or theft of confidential customer information.[2] Referred to in Canadian privacy legislation as "personal information," this sensitive data is generally thought of as any information that can be used to identify an individual. Therefore, corporate information is generally not considered personal information. The scope of personal information, absent specific statutory definition to the contrary, has been held by the Supreme Court of Canada to be deliberately broad encompassing an ever changing landscape of information.[3]

3. LEGISLATIVE REQUIREMENTS

In Canada, there exists a legislative framework in place which establishes legal guidelines and obligations for private organizations who deal with personal information.

(c) FEDERAL AND PROVINCIAL FRAMEWORK

[1] Ponemon Insitute LLC, *The Post Breach Boom*, February 2013, p 1.
[2] Ponemon Institute LLC, *Reputation Impact of a Data Breach: Executive Summary*, October 2011, p 2.
[3] *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403.

The governing legislation at the national level is the *Personal Information Protection and Electronic Documents Act*[4] ("PIPEDA"), which was enacted in 2005. This statute regulates the collection, use and disclosure of personal information, which as previously noted is generally defines as "information about an identifiable individual […]".[5] PIPEDA applies to private entities who handle personal information in the course of their commercial activities nationwide. Noteworthy exceptions to this rule are the provinces of British Columbia, Alberta, Québec, and Ontario, though of note Ontario's legislation applies only to personal health information.[6] The Act remains the governing authority for federal businesses even when they are operating in these particular provinces.

The standard of reasonableness is the principal rule governing Canadian privacy legislation. In this sense, organizations may only collect, use and disclose personal information for purposes that would be qualified as acceptable by the reasonable person. Consent is irrelevant with regard to this rule, meaning that an organization will be found to have violated the Act when it handles data in an unreasonable manner, regardless of the position of the individual whose information is in question.

Implied or express consent is required in most cases where an individual's data is collected, used or disclosed.[7] This requirement, by which knowledge and consent of the individual is required for collection, use or disclosure of personal information, except where inappropriate, is one of ten principles listed in *Schedule 1* of the Act[8]. The others revolve around the overarching principles of reasonableness and diligence on behalf of organizations. Notably, organizations should designate individual(s) in charge of compliance and establish safeguards to protect the information. The level of these safeguards depends on the sensitivity of the information, meaning that highly sensitive information requires additional security. Organizations should also identify the purposes for which the information is collected, used or disclosed, while strictly limiting the handling of the information for these particular purposes. Collection of the information should be collected by fair and lawful means and organizations should ensure their accuracy. Finally, their policies should be readily available to individuals, who should have access to their information and be able to challenge compliance when necessary.[9]

One notable aspect of this legislation is that it is often voluntary. As stated in section 5(2) of the Act: "The word "should", when used in Schedule 1, indicates a recommendation and does not

[4] SC 2005, c 5.
[5] *Ibid.*, s 2. (1), "personal information".
[6] BC: Personal Information Protection Act, , SBC 2003, c 63; AB: Personal Information Protection Act, SA 2003, c P-6.5; QC: Respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1; ON: Personal Health Information Protection Act, 2004, S.O., c. 3.
[7] *Ibid.*, p 105.
[8] *PIPEDA*, *supra* note 7, Schedule 1.
[9] *Ibid.*

impose an obligation".[10] This provision signifies that adherence to the Act and its regulations is in many cases voluntary for private organizations. From a post-breach perspective, organizations are not obligated by law to notify individuals, or to take any other measures for that matter, in the event of a data breach pursuant to PIPEDA. However, guidelines and checklists that have been issued by the Office of the Privacy Commissioner of Canada regarding response to data breaches are recommendations that cannot result in penalties if not respected. Nevertheless, they remain extremely insightful for organizations and should be followed in order to minimize exposure to legal exposure and reputational damage.

(d) FUTURE CONSIDERATIONS

The rapid evolution of data handling has prompted the federal commissioner to become increasingly proactive in bringing reform to PIPEA. In a report entitled "*The Case for Reforming the Personal Information and Electronic Documents Act*"[11], the current commissioner Jennifer Stoddart affirms that "the days of soft recommendations with few consequences for non-compliance are no longer effective in a rapidly changing environment where privacy risks are on the rise."[12]

In its recommendations for changes to the Act, the report suggests instituting new enforcement powers such as statutory damages administered by the Federal Court, authority for the Commissioner to make orders and granting him or her power to impose administrative monetary penalties. Most importantly, the report advocates the introduction of mandatory breach notification and reporting. This measure would compel organizations to report any security breaches to the Commissioner and would oblige them to notify the affected individuals, ensuring that remediating action would be taken without delay.

Such a reform reflects the legislative changes that have already been enacted in Alberta, which is the only jurisdiction in the country with a mandatory breach notification and reporting legislative scheme in place for the private sector.[13] Under Alberta's privacy legislation, organizations must notify the province's information and privacy commissioner in the event that personal information is lost, accessed or disclosed without authorization, or if the organization has suffered a privacy breach. The threshold for this notification requirement is triggered when a real risk of significant harm to an individual materializes and this risk would be qualified as so by a

[10] *PIPEDA, supra* note , 5(2)

[11] Office of the Privacy Commissioner of Canada, *The Case for Reforming the Personal Information Protection and Electronic Documents Act*, May 2013.

[12] Éloïse Gratton, *reforming PIPEDA with stronger enforcement powers, mandatory breach notification and accountability obligations*, McMillan Privacy Law Bulletin, May 2013, p 2.

[13] *Ibid.*

reasonable, objective person. Organizations who fail to notify the commissioner during such an occurrence are guilty of an offence under the provincial legislation. When the reporting is properly conducted, the commissioner is charged with reviewing the information provided and determines if the affected individuals require notification of the data breach, which he or she can order if necessary.

The federal government has already sought to amend the Act numerous times to impose reforms such as these mentioned above. Although these changes have not yet ensued, the evolution of personal data use and collection increases their likelihood and private organizations must be made aware of this very real possibility. Based on the findings of its most recent business survey, the Office of the Privacy Commissioner has concluded that mandatory breach notification provisions will entice organizations to develop preventive data protection strategies.[14] Therefore, though the majority of Canadian organizations must only adhere to the voluntary legislative scheme today, it is recommended that they establish strategies such as incidence response plans going forward to comply with the regulations of tomorrow.

4. STEPS POST-BREACH

An organization's reaction to a data breach can prove to be the difference between inconvenience and loss of reputation and decreased revenues. The following is an overview of some of the important steps to be taken after becoming aware of a data breach.

a. POST-BREACH

In the event of a breach, an organization must adopt measures in order to mitigate their losses, limit reputational damage, and protect client personal information. Some of these steps can be executed independently, while others require pre-breach planning beyond the scope of this paper.

5. **Identify the origin and extent of the breach, contain it and close the vulnerability.** The first step upon notification of a breach is to immediately contain the situation. Containment, while highly fact specific, can include stopping the unauthorized practice, physically removing accessed records, shutting down the breached system, revoking access, etc.

   To the extent possible a preliminary assessment of the extent of the breach should be undertaken. This includes determining the extent of unauthorized access and sensitivity of information at risk.

[14] Gratton, *supra* note 15.

6. **Engage the relevant personnel.** Appropriate individuals from each part of the business should be organized as a unit under one leader possessing the necessary credentials to navigate within the organization and make initial recommendations. While some organizations have in place the necessary human resources to complete this task, it is advised upon notification of a breach to immediately contact counsel and/or a technical consultant to coordinate remediation efforts.

7. **Ensure document retention and proper care of the evidence.** From the moment a breach is reported, it is important that all relevant documentation is conserved to avoid the spoliation of evidence should future litigation arise and, further, to assist in the investigation of the breach.

8. **Assess the risks associated with the breach.** In order to determine the proper course of action it is important to find out what information is involved and who the breach is likely to affect. What is the sensitivity of the information, is it protected and, if accessed, can this information be used to harm individuals? How many individuals have or can be affected by the breach? Is there a possibility of foreseeable harm to these individuals, to the organization and/or to the public? The answer to this question will assist the organization in deciding what level of notification is appropriate.[15]

9. **Notify the appropriate individuals.** Notification, while currently voluntary in the majority of Canada from a legislative perspective, remains an important mitigation strategy that has the potential to benefit both the organization and individuals affected by the breach. As an initial step, an organization must consider whether notification is warranted in order to avoid or limit harm to an individual whose information has been illegally accessed, used, collected or disclosed. If there is a reasonable risk of harm such as identity theft, fraud or physical harm, the affected individuals should be contacted as soon as reasonably possible and preferably by direct notification. Each incident needs to be considered on a case-by-case basis to determine whether notification is required.

The content of notifications will vary depending on the nature of the organization and the data affected. However, notifications should typically include: a broad outline of the breach and its timing; a description of the personal information affected; a general account of the steps taken to mitigate the harm *ex-post*; what the organization is doing to assist individuals that are adversely affected and what individuals can do on their own to mitigate loss; links to third party sources of information to assist individuals (e.g. the Office of the Privacy Commissioner); and, contact

[15] Office of the Privacy Commissioner of Canada, *Key Steps for Organizations in Responding to Privacy Breaches*, 28-08-2007, p 5.

information of a designated individual or department within the organization who can respond to inquiries.

10. **Notify other relevant entities.** It can be beneficial for an organization to notify public or private bodies that can assist with or be affected by the breach. Most importantly, organizations are recommended to notify designated privacy commissioner(s) of breaches as this can assist them in responding to public inquiries and complaints.[16] These offices can also provide guidance with regard to responding to the breach. The police authorities should be contacted if the breach involves theft or another crime. An organization might be contractually obliged to contact their insurance company. Third parties such as credit card companies, financial institutions or credit reporting agencies should be contacted if notification of individuals will have repercussions on their operations.

11. **Consider offering services to affected individuals**. If the breach is in relation to financial information, offering a free service such as credit monitoring can help limit an organization's exposure. In fact, experts have concluded that an organization is 3.5 times more likely to be sued when financial harm is caused to individuals, but 6 times less likely to face litigation if it provides free credit monitoring.[17]

12. **Prevent future breaches.** After the short-term requirements have been met, organization should apply the knowledge gained from the breach and update their prevention plan. Vulnerabilities should be assessed and corrected. Policies and procedures should be reviewed and ameliorated to prevent similar incidents. Finally, an audit should be conducted at the end of the process to ensure implementation of new measures.

These general steps offer guidance for the procedures and strategies that should be adopted before, during and after a breach. The circumstances of each breach are different and organizations should conduct a pragmatic analysis of the situation to ensure that individuals, as well as the business itself, are protected. It is nevertheless important to note that breaches can have important consequences, regardless of response or fault: "The unfortunate reality is that notification can lead to litigation, whether meritorious or not, because even fear of potential harm is enough to persuade some plaintiffs to sue."[18]

5. CONCLUSION

The age of Big Data has brought about many significant advantages for organizations. However, access to such large amounts of sensitive information imposes a new set of risks. In order to

[16] *Ibid.*, p 6.
[17] Sasha Romanosky, *Empirical Analysis of Data Breach Litigation*, Carnegie Mellon University Cylab, June 1, 2012, p. 4.
[18] Flaherty, *supra* note 25, p 50.

help mitigate the prospective losses in a data breach scenario, it is essential, from both a litigation risk and regulatory perspective, that all data handlers take affirmative action to prevent and be prepared to respond to data breach.