Cassels

PIPEDA's Draft *Breach of Security Safeguard Regulations* Provide Timely Guidance

Bernice Karn

September 14, 2017

Last Thursday, Equifax reported a data breach, which may have affected up to 143 million consumers in the United States. The credit reporting company announced that between mid-May and July of this year, hackers accessed and stole consumer names, social security numbers, and other personal information held by Equifax. Canadian consumers were also affected, though the scope of the Canadian breach is not yet known. Consumers are understandably concerned about the ramifications of the hack, particularly as this announcement comes almost two months after the breach occurred, though Equifax has stated it took prompt action and engaged a cybersecurity firm after discovering the breach.

The Equifax announcement follows closely on the heels of the draft *Breach of Security Safeguard Regulations* ("Breach Regulations") released by the Ministry of Innovation Science and Economic Development Canada (ISED) over the Labour Day long weekend. Organizations concerned about how to report a data breach in Canada now have some guidance as set out in these new Breach Regulations.

Background

The concept of data breach reporting was first introduced at the federal level in Canada by Bill s-4, the *Digital Privacy Act*, which came into force on June 18, 2015, and amended Canada's federal privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The revisions to PIPEDA mandated that organizations report data breaches that pose a "real risk of significant harm" to individuals and introduced record keeping requirements. The draft Breach Regulations specify the *minimum* requirements for reporting and notice, as well as the record-keeping requirements.

Following the 30-day comment period, the ISED may make further amendments or publish the final Breach Regulations. The ISED has stated that the coming into force of these Breach Regulations will be delayed to allow organizations sufficient time to establish processes and procedures for tracking and reporting data breaches.

Data Breach Reporting Requirements

1. Do all data breaches need to be reported?

The reporting regime mandates that data breaches that pose a "real risk of significant harm" must be

reported to the Office of the Privacy Commissioner of Canada (the “Commissioner”) and notification of the breach must be given to affected individuals. In assessing the risk of a data breach, organizations must consider the sensitivity of the information involved and the likelihood that such information will be misused. Other organizations, such as law enforcement agencies, must also be notified if they may be able to mitigate the harm to affected individuals. A data breach such as the one suffered by Equifax would likely qualify as the type of breach that must be reported under the new Breach Regulations, as the company held sensitive personal information such as social security/insurance numbers, and the probability of misuse in areas such as identity and credit theft is high.

Report to the Commissioner

When notifying the Commissioner, the organization must also provide a data breach report. The Breach Regulations set out the following minimum requirements for these types of reports:

(a) a description of the circumstances of the breach and, if known, the cause;

(b) the day on which, or the period during which, the breach occurred;

(c) a description of the personal information that is the subject of the breach;

(d) an estimate of the number of individuals in respect of whom the breach creates a real risk of significant harm;

(e) a description of the steps that the organization has taken to reduce the risk of harm to each affected individual resulting from the breach or to mitigate that harm;

(f) a description of the steps that the organization has taken or intends to take to notify each affected individual of the breach in accordance with subsection 10.1(3) of PIPEDA; and

(g) the name and contact information of a person who can answer, on behalf of the organization, the Commissioner’s questions about the breach.

These requirements do not preclude organizations from including additional information in their breach reports. While these new reporting requirements are generally in line with the regulations already in force under Alberta’s *Personal Information Protection Act*, one notable difference is that the proposed federal Breach Regulations do not require an assessment of risk of harm to individuals, which makes filing these reports significantly less onerous than in Alberta.

Notification to Affected Individuals

The proposed Breach Regulations also list the content of notifications to be provided to affected individuals. These requirements bear similarities to those in Alberta. Notifications to individuals should contain much of the same information as in the report to the Commissioner. Additionally, organizations must provide a toll-free number or email through which individuals can obtain more information, and must inform individuals of any internal complaint procedures and about their right to file a complaint with the Commissioner.

The manner of notification is also prescribed, and notably provides some flexibility for organizations, allowing organizations to communicate notifications via email (with consent), letter, telephone or in person. Indirect notification, through a posting on the organization's website or through an advertisement, is also an option in limited circumstances such as when direct notification would cause further harm to the individual or would be prohibitively expensive.

2. Record Keeping Requirements

The PIPEDA amendments also require organizations to maintain a record of every breach and there is no applicable minimum threshold. The Breach Regulations require that these records be retained for a period of 24 months from the date that the organization “determines” that a breach has occurred. (The implication is that, until a breach is confirmed, there may not be a requirement to keep a record of every possible incident.) These requirements may be of concern for larger organizations that deal with massive amounts of data and frequent security threats, but ISED has highlighted that mandatory record keeping will encourage organizations to maintain and implement tracking for data security incidents. Further, the definition of “record” allows for a broad interpretation, and organizations will be permitted to determine the form and content of the records so long as there is sufficient information to satisfy the data breach report requirements above. Implicitly, this means that a report meeting the data breach reporting requirements would be a sufficient record. The Commissioner may also request the data breach records for a two-year window; a time frame intended to align with the limitation period for civil action in most jurisdictions.

Impact on Businesses & Consumers

While the Breach Regulations, at first glance, appear to place an onerous administrative burden on organizations, they are generally flexible and provide a range of ways for organizations to comply. For example, for those organizations that have already implemented data security protocols and breach notification procedures (such as those mandated by privacy laws in other jurisdictions), compliance with the Breach Regulations may only nominally increase costs to the organization while reinforcing best practices for the industry.

Organizations that are familiar with data breach reporting obligations in the United States may find the current draft regulations disappointing. Unlike in the US, where reporting obligations are generally triggered if certain information is impacted (e.g., financial details, health information, social security numbers, government identification), the Breach Regulations only refer to data breaches resulting in a “real risk of

significant harm” as a threshold for requiring mandatory reporting. The lack of prescriptive notification triggers or further guidance on what types of breaches must be reported means that organizations will need to make their own determinations on what they believe to be “reportable” breaches. Without additional clarity from the regulator, or until precedents are established once the rules are in force, there is a possibility that organizations may inappropriately screen out data breaches based on their own internal assessments and industry-specific risk profiles – to the detriment of affected individuals.

Ultimately, although the Breach Regulations are a step in the right direction to protect personal information of Canadians, it remains to be seen if organizations will respond practically and effectively once they are in force. Interested parties may submit representations concerning the proposed regulations until October 2, 2017.

For the full text of the draft Breach Regulations and the Regulatory Impact Analysis Statement, please click here.

The contribution of Tegan O’Brien, articling student, in the preparation of this article is gratefully acknowledged.
