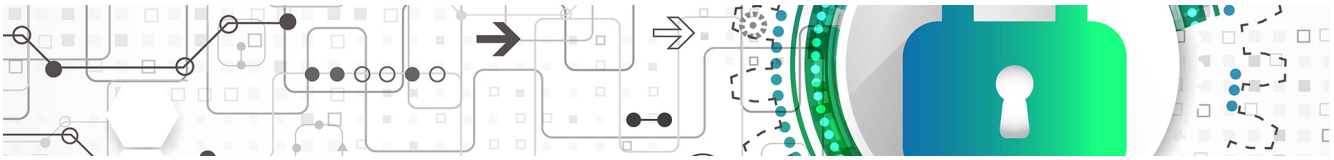

Oh, Hack! Canada's Mandatory Breach Notification Now in Force

November 23, 2018

By Amanda Branch

On November 1, 2018, the mandatory breach notification requirements came in to force.

Under the legislation, if an organization suffers a breach of security safeguards that gives rise to a "real risk of significant harm", the organization must (i) report the incident to the Office of the Privacy Commissioner of Canada (the "**OPC**"); (ii) notify affected individuals; and (iii) notify any other third party organizations or government institutions that are in a position to mitigate the risk of harm to affected individuals. These notifications must be made as soon as feasible after the organization determines that the breach has occurred.

The OPC recently released its breach guidance, "What you need to know about mandatory reporting of breaches of security safeguards" (the "**Guidelines**") which will help businesses better understand their obligations.

What should organizations know about breach reporting?

Penalties. Failure to report a breach or to maintain required records is an offence under PIPEDA and non-compliance is punishable by a fine of up to $100,000.

Who should report. Generally speaking, the organization that is in control of the personal information involved in the breach must report the breach to the OPC.

What to report. An organization must report to the OPC a breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe the breach creates a real risk of significant harm to the individual. Organizations are not expected to report all breaches (but recall, organizations are required to keep a record of all breaches).

What does a "real risk of significant harm" mean?

Determining whether there is a "real risk of significant harm" should be based on an assessment of the sensitivity of the personal information involved in the breach and the probability the personal information has been/is/will be misused. Under the legislation, "significant harm" is defined to include humiliation, damage to reputation or relationships, loss of employment or other opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

When to report. The breach should be reported to the OPC as soon as feasible after the organization determines a breach has occurred, even if not all information is known or confirmed. Organizations can update the form if/when they become aware of new information.

What about notifying individuals?

When to notify. Unless otherwise prohibited by law, if an organization determines that a breach poses a real risk of significant harm to an individual, the organization must notify the affected individual and must include:

- A description of the circumstances of the breach;
- The day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
- A description of the personal information that is the subject of the breach to the extent that the information is known;

- A description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;
- A description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
- Contact information that the affected individual can use to obtain further information about the breach.

The notification must be given as soon as feasible after the organization determines a breach has occurred.

How to notify. Generally speaking, the notification must be conspicuous and given directly to the individual (except in circumstances set out in the regulations where indirect notification is allowed).

What kind of records should be kept?

Businesses will also be required to maintain records of all data breach incidents for a minimum of 24 months (irrespective of whether the business concludes the breach gives rise to a real risk of significant harm to affected individuals). The Commissioner may request and review the history of breaches experienced by a particular business within the prior 24-month window. Records must contain sufficient information to permit the Commissioner to verify compliance with the breach reporting regime and the Guidelines state that, at a minimum, a record should include:

- Date or estimated date of the breach;
- General description of the circumstances of the breach;
- Nature of information involved in the breach;
- Whether or not the breach was reported to the Privacy Commissioner of Canada/individuals were notified; and
- If the breach was not reported to the Privacy Commissioner/individuals, a brief explanation of why the breach was determined not to pose a “real risk of significant harm.”

By way of background, in 2015 the *Digital Privacy Act* introduced significant amendments to PIPEDA, including the creation of mandatory data breach reporting and record keeping requirements. In April 2018, the federal government published the Breach of Security Safeguard Regulations which set out the requirements for the new mandatory reporting regime. These regulations came in to force on November 1, 2018.

This article was first published in the IICIE blog *https://www.iicie.com/users/blog.php?blgId=MTEx*