mcmillan

Privacy Law Bulletin

November 2018

Trick or…Breach? PIPEDA's Breach Reporting Requirements Come Into Force on November 1, 2018

After more than three years of consultation and anticipation, the big day has finally arrived. As of November 1, 2018, organizations subject to the Personal Information *Protection and Electronic Documents Act* ("PIPEDA") are, in certain circumstances, required to:

- report to the Office of the Privacy Commissioner of Canada (the "Commissioner's Office") a breach of the organization's security safeguards;
- notify affected individuals of a breach; and
- maintain particular records of all breaches.

The new reporting requirements arise from amendments to various sections of PIPEDA pursuant to the *Digital Privacy Act* ("DPA"). November 1, 2018 also marks the coming into force of the Breach of Security Safeguards Regulations (the "Regulations"), which are intended to reflect best practices established through the prior voluntary reporting initiative of the Commissioner's Office. The Commissioner's Office has released a Guidance Document[1] to assist organizations in understanding and complying with the new reporting, notification and recordkeeping requirements.

[1] What you need to know about mandatory reporting of breaches of security safeguards, Office of the Privacy Commission of Canada, click here

This bulletin provides an overview of the new breach reporting requirements.

Determining When to Report

PIPEDA now requires an organization to report any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

In order to trigger the reporting requirement, an organization must first determine whether a breach has in fact occurred. A breach of security safeguards includes the loss, unauthorized access to or unauthorized disclosure of personal information resulting from (i) a breach of an organization's security safeguards and/or (ii) the organization's failure to establish those safeguards.

For reporting to be necessary, the breach must also involve personal information under the organization's control. Neither PIPEDA nor the Regulations define "Control". The Guidance Document notes that, though the existence of "control" will be determined on a case-by-case basis, an organization will largely be responsible for reporting a breach that occurs with any third party processor to whom the organization has transferred personal information.

Finally, to invoke the reporting requirement, it must be reasonable to believe that the breach "creates a real risk of significant harm" to an individual. The number of individuals impacted does not matter. As long as there is a real risk of significant harm to even one individual, the organization is obliged to report the breach.

PIPEDA defines "significant harm" to broadly include bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on a credit record and damage to or loss of property.

In assessing whether there is a "real risk" of significant harm, the organization must consider:

a) the sensitivity of the information, including the context or circumstances of the breach; and

b) the probability that the personal information has been, is being, or will be misused, including factors such as how long and to whom the information was exposed, whether there was malicious intent behind the breach (such as theft or hacking), whether the information was adequately encrypted or anonymized, and whether harm has actually materialized.

An organization must report a breach as soon as feasible after the organization determines that a breach has occurred, even if some information with respect to the breach is still unknown.

What to Include in the Report

Once an organization determines that a reportable breach has occurred, the question becomes how to report the breach and how much information to include.

While not required, the Commissioner's Office is encouraging organizations to use the PIPEDA breach report form.[2] Whether the breach is reported using the PIPEDA breach report form or on a custom format, the report to the Commissioner's Office must include the following information:

- a description of the circumstances of the breach and, if known, the cause;
- the day on which, or period during which, the breach occurred or, if neither is known, the approximate time period;
- a description of the personal information that is the subject of the breach, to the extent that the information is known;
- the number of individuals affected by the breach or, if unknown, the approximate number;

[2] PIPEDA Breach Report Form

- a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach or to mitigate that harm;
- a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach; and
- the name and contact information of a person who can answer, on behalf of the organization, the Commissioner Office's questions about the breach.

An organization can also voluntarily include additional information should it assist in furthering the understanding of the Commissioner's Office. Importantly, an organization should base the initial report on the best information available to it at the time of reporting. An organization may later add information or correct its report if it becomes aware of any new pertinent information.

The Report is Made - What Happens Next?

When the Commissioner's Office becomes aware of a breach, it may:

- seek more information from the organization;
- work to identify and resolve any PIPEDA compliance issues;
- take steps to mitigate any of the damage that may flow from the breach; and/or
- initiate an investigation.

Though the Commissioner's Office has a general duty to maintain the confidentiality of breach reports, exceptions exist where:

- because of an information sharing agreement, disclosure to a domestic or international counterpart is required;
- the Commissioner's Office has reasonable grounds to believe that the information could be useful in the investigation of a contravention of Canada or a province's laws, in which case the breach report may be disclosed to a government institution; or

- the Commissioner's Office believes it is in the public interest to publicly disclose information related to a breach.

Notifying Affected Individuals

An organization must also notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual, provided that such notification is not prohibited by law.

As is the case with reporting a breach to the Commissioner's Office, notification to an individual must occur as soon as feasible after the organization has determined that a breach of security safeguards involving a real risk of significant harm as occurred.

Notifications must be conspicuous, easy to understand, and include the following information:

- 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 time period;
- a description of the personal information that is the subject of the breach, to the extent 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 Regulations require that notice be made directly to each individual by way of email, letter, telephone, or in person, unless:

- direct notification would likely cause further harm to the affected individual;
- direct notification would be likely to cause undue hardship for the organization; or
- the organization does not have contact information for the affected individual or the information it has is out of date.

In circumstances where an organization does not have current contact information for an affected organization, the Regulations permit indirect notification through public announcements or advertising, such as advertisements in print or online newspapers.

Whenever an organization notifies an individual of a breach, it must also notify any government institutions or organizations that it believes can reduce or mitigate the risk of harm. For example, an organization might notify a bank or payment processing service following a breach of payment information.

Recordkeeping

Organizations are now be required to keep and maintain for a period of at least two (2) years records of all breaches of security safeguards involving personal information under their control, whether or not there is a real risk of significant harm.

The Guidance Document provides that, at minimum, records must include:

- the date or estimated date of the breach;
- a general description of the circumstances of the breach;
- the nature of the information involved in the breach; and
- whether or not the breach was reported to the Commissioner's Office and/or whether affected individuals were notified.

An organization's records should also contain sufficient details for the Commissioner's Office to assess whether the organization has correctly applied the real risk of significant harm standard and

otherwise satisfied its obligations to report and notify affected individuals. To this end, organizations may wish to include a note in their records indicating why a breach of security safeguards did not trigger the obligation to report or notify.

Penalties for Failure to Comply

PIPEDA provides that it is an offence to knowingly contravene the reporting, notification and record-keeping provisions. In the event of a failure to comply with the provisions, the Commissioner may refer the information to the Attorney General of Canada, who may then prosecute the organization. Knowingly failing to report to the Commissioner, notify affected individuals, or maintain records could attract a fine of up to $100,000.

Next Steps for Organizations

Given the new mandatory privacy breach reporting, notification and record-keeping requirements, organizations should conduct a thorough review of their policies, procedures and safeguards to prevent, uncover and respond to breaches and other privacy incidents. Organizations should also update their existing privacy policy to reflect these new obligations.

Organizations should carefully review PIPEDA, the Regulations and the Guidance Document with relevant stakeholders, including senior leadership. Employees should be trained at the earliest opportunity, with an emphasis placed on the need to identify and escalate any breaches to the appropriate person(s) within the organization as soon as possible. Consider hosting a "lunch and learn" to work through the new obligations and discuss how they may affect employees in their daily roles.

The need to establish a breach or incident response team and plan is more critical than ever given the time-sensitive nature of the reporting and notification requirements. In the event of a suspected breach, organizations will have to make a number of decisions very quickly, including engaging in a particularly nuanced analysis of whether a given situation triggers the mandatory reporting and notice requirements. Organizations should take the opportunity to think through and assign roles and responsibilities prior to any

potential breach, when the circumstances are significantly less rushed and stressful.

Members of the breach or incident response team ought to familiarize themselves with the PIPEDA breach report form (or any other template reporting document decided upon by the organization, provided it complies with the Regulations) to better understand the types of information that the organization may need to collect quickly in the event of a breach and where to access this information.

If an organization uses a third party service provider to process or store personal information, it is important to review existing and new contracts with third parties to ensure adequate provision for compliance with the breach reporting, including notification and recordkeeping obligations. This further underscores the importance of vendor selection and being diligent about third parties that the organization entrusts with personal information. Organizations should do their due diligence and understand how a third party will be storing, handling and disposing of personal information to mitigate the risk of being liable to report due to a third party's breach.

Organizations that experience a suspected or actual breach of their security safeguards are encouraged to immediately contact privacy professionals to determine whether a particular breach requires reporting and notification, and to avoid incurring significant penalties for non-compliance.

by Kristen Pennington and Mitch Koczerginski

For more information on this topic, please contact:

Toronto	Kristen Pennington	416.865.7943	kristen.pennington@mcmillan.ca
Toronto	Mitch Koczerginski	416.865.7262	mitch.koczerginski@mcmillan.ca