Information Protection

What you need to know about the new Breach Notification Rules under PIPEDA

By Kelsey M. Yakimoski and Paul K. Grower, Fillmore Riley LLP

On Nov. 1, 2018, the new mandatory breach notification rules under the *Personal Information and Protection and Electronic Documents Act* (PIPEDA) and the related Breaches of Security Safeguards Regulation came into force. PIPEDA applies to organizations that are either: 1) federally regulated; 2) move personal information across provincial or international borders; or 3) located in provinces who have failed to adopt similar legislation to PIPEDA – which, at present, is every province except Alberta, British Columbia and Québec. The Alberta legislation contains breach notification rules – outlined below – whereas the legislation in B.C. and Québec does not. The Breach Rules will apply to all personal information that is caught by PIPEDA in B.C. and Québec, but does not apply to personal information caught only by the B.C. or Québec privacy legislation.

As of Nov. 1, 2018, organizations subject to PIPEDA are required to report to the Office of the Privacy Commissioner of Canada (OPCC), as well as the affected individuals, any breach of security safeguards involving 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 affected individuals.

PIPEDA requires that personal information must be protected by security safeguards appropriate to the sensitivity

NULINUKAS / 123RF

of the information and should protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. A "breach of security safeguards" occurs where loss of, unauthorized access to or unauthorized disclosure of personal information results from a breach of an organization's security safeguards or from the failure to establish a security safeguard.

It is important to note that the new Breach Rules under PIPEDA apply to the organization which is in control of the personal information involved in a breach. The OPCC has confirmed that it is reasonable to interpret the principal organization as having "control" over the information in such circumstances and therefore bearing the responsibility for reporting the breach. For example, if a breach occurs at an arm's length storage facility hired by the organization to store personal information, it will be the organization's responsibility to comply with the Breach Rules as further outlined below.

The Breach Rules outline that if it is reasonable in the circumstances to believe that the breach creates *a real risk of significant harm* to an individual, the organization – and if applicable, any other third party – is then obligated, as soon as it is feasible to do so, to:

- File a report with the OPCC;
- Notify the individual(s) whose personal information was breached; and,
- Notify any other organization or government entity that may be able to assist in reducing or lessening any harm to individuals (e.g. the police, credit reporting agencies, etc.).

In the report filed with the OPCC, the organization must (to the extent that the organization knows):

- Describe the circumstances of the breach and the cause;
- Identify the period when the breach occurred;
- Describe the personal information that is the subject of the breach;
- Identify the number of individuals affected;
- Describe the steps undertaken to reduce or lessen the risk of harm to the affected individuals;
- Describe the steps undertaken to notify the affected individuals; and,
- Identify the contact person at the organization who will be able to answer any further questions from the OPCC about the breach.

It is expected that the organization will update this report as further information is gathered/determined.

In the notification provided to the individual, the organization must (to the extent that the organization knows):

- Describe the circumstances of the breach;
- Identify the period when the breach occurred;
- Describe the personal information that is the subject of the breach;
- Describe the steps undertaken to reduce or lessen the risk of harm to the individual;
- Describe the steps that the individual could take to reduce their risk of harm (e.g. changing passwords, monitoring financial account activity, etc.); and,
- Identify the contact person at the organization who will be able to answer any further questions from the individual about the breach.

The goal of the notification to the individual is to provide sufficient information to allow the individual to understand the significance to *them* of the breach, such that they can take steps, if any are possible, to reduce the risk of or mitigate the harm.

Also, it is expected that the individuals affected will be directly contacted by the organization (phone, email, mail, etc.), subject to exceptions of harm to the individual and/or hardship to the organization and/or lack of contact information. If any of the exceptions apply, indirect notification – via public communications (e.g. media, website, etc.) – will need to be utilized.

PIPEDA specifies that "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

In determining whether there is a "real risk" of "significant harm," the sensitivity of the information and the probability that it will be misused need to be considered. When considering the sensitivity of the information, the organization

LEAF / 123RF

Medical records and income records are almost always considered to be sensitive but any information can be sensitive depending on the context

NIRATPIX / 123RF

It is important to note that the new Breach Rules under PIPEDA apply to the organization which is in control of the personal information involved in a breach.

must look at the context and the circumstances of the breach to determine the extent to which the information is sensitive. PIPEDA notes that although some information (for example, medical records and income records) are almost always considered to be sensitive, any information can be sensitive depending on the context.

When considering the probability that the personal information will be misused, the organization should look at who actually accessed or could have accessed the personal information, the length of time the information was exposed and the presence of any evidence of malicious intent.

Alberta has had similar breach notification rules in place since 2010 under its *Personal Information Protection Act*, which also require notification if there is a real risk of significant harm. The Alberta Office of the Information and Privacy Commissioner (AOIPC) has stated that to meet the significant harm test the harm must be important, meaningful and have non-trivial consequences or effects. The AOIPC further noted in 2011 that:

> "…This standard does not require that significant harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. Further, there must be a cause and effect relationship between the incident and the possible harm."

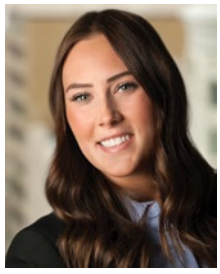
The AOPIC has provided some guidance based on past decisions on what constitutes a real risk of significant harm as a result of a breach. For example, highly sensitive personal information (such as social insurance numbers, drivers' license numbers and credit card numbers in combination with personal identifiers such as name and address) coupled with circumstances where information was stolen for nefarious purposes, where the recipients of the information could not be determined or where the device containing the personal information had no encryption – making access possible and unknown – have led to a finding that a real risk of significant harm exists as a result of a breach.

It is important to note that if a breach occurs – and it is determined by the organization that it does not create a real risk of significant harm to an individual – the organization must still maintain a record of the breach for at least two years thereafter. The record must include a description of the incident (including when it happened and what information was involved) and must also document whether notification was made, and if not, why it was determined that there was not a real risk of harm. The purpose for retaining these records is to allow the OPCC to verify an organization's compliance with the Breach Rules. Therefore, if a breach is not reported to the OPCC, the information that would have been provided to the OPCC, if it had been reported, must be maintained.

Most importantly, these Breach Rules provide for fines of up to $100,000 if an organization knowingly fails to report to the OPCC, notify the affected individuals or fails to maintain a record for all breaches.

This article provides a brief summary of what these Breach Rules entail and should not be construed as legal advice. Readers are encouraged to speak with legal counsel to better understand how the Breach Rules will affect their organization.

Kelsey M. Yakimoski is an associate with Fillmore Riley LLP who practises primarily in the area of civil litigation. You may reach her at 204-957-8397 or kyakimoski@fillmoreriley.com.



Paul K. Grower is a partner with Fillmore Riley LLP who practises primarily in the areas of taxation litigation, general commercial litigation and privacy law. You may reach him at 204-957 8369 or pgrower@fillmoreriley.com.