Federal breach notification law now in effect in Canada

Christine N. Czuprynski, Dominic A. Paluzzi | Wednesday, November 7, 2018

The breach notification provisions of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) went into effect Nov. 1, 2018. PIPEDA places requirements and restrictions on an entity's collection and use of "personal information," defined as information about an identifiable individual, in the course of a commercial activity. All organizations that collect and use personal information belonging to Canadians must comply with PIPEDA's requirements. This includes consumer/customer data, as well as employee data. The law has been in force since 2001 and was amended in 2015 to include breach notification requirements, though the 2015 breach notification amendments made as a result of the Digital Privacy Act were not immediately effective. Those amendments are now effective.

PIPEDA requires personal information to be protected by security safeguards appropriate to the sensitivity of the information. An organization's security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. The safeguards should include: physical measures, organizational measures, and technological measures. A "breach of security safeguards" is defined in PIPEDA as the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards, or from a failure to establish those safeguards.

Here's what you need to know about breach notification in Canada:

Under what circumstances is breach notification required in Canada?

The law requires notification to both the Office of the Privacy Commissioner of Canada (OPC) and impacted individuals in the event the breach results in a risk of harm to the impacted individual(s). PIPEDA calls this a "real risk of significant harm (RROSH) to an individual." The OPC provides guidance 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. Factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm include the sensitivity of the personal information involved in the breach of security safeguards and the probability the personal information has been/is/will be misused."

Who is responsible for notifying?

The law follows the format of many of the U.S. state data breach notification laws in that the obligation to notify rests with the entity/organization in control of the personal information implicated in the breach (here, referred to as the "controlling entity").

- If the controlling entity has transferred the personal information to a third party for processing, and the third party suffers the breach, the controlling entity still has the obligation to notify. As such, the OPC recommends including strong provisions in contracts with third parties that require those third parties to notify the controlling entity in the event of a breach.

How quickly should notice be made?

The law requires that notification to individuals be given as soon as feasible after an entity has determined that a breach of security safeguards involving a real risk of significant harm has occurred.

What should the notice include?

The notification must 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 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.
- Contact information that the affected individual can use to obtain further information about the breach.

How should notice be provided?

The law requires direct notice (in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances) unless direct notice would cause more harm to the individuals, is not feasible for the breached entity, or is not possible given a lack of contact information available to the breached entity.

Are there any other notification obligations?

An entity that notifies an individual of a breach involving a RROSH must also notify any government

institutions or organizations that the entity believes can reduce the risk of harm that could result from the breach or mitigate the harm.

Are there any record-keeping requirements?

The law requires that an organization has to keep and maintain a record of every breach of security safeguards involving personal information under its control.

How is the law enforced?

Under PIPEDA, it is an offense to knowingly violate PIPEDA's reporting, notification and record-keeping requirements relating to breaches of security safeguards, and doing so could lead to fines. The OPC will refer possible violations to the Attorney General of Canada, who will be responsible for investigation and prosecution. OPC had provided a form that it encourages entities to use to report breaches of security safeguards.

How your business should respond to new federal data breach notification law in Canada

Organizations' Incident Response Plans need to be updated to account for this new federal data breach notification law in Canada. We expect the OPC and Attorney General of Canada to increase investigations of breached entities both inside and outside of Canada. As such, it is critical that PIPEDA is closely complied with and that policies and training are in place and updated.

Christine N. Czuprynski

Dominic A. Paluzzi