THOMPSON DORFMAN SWEATMAN

Mandatory Federal Security Breach Reporting Requirements in Effect

As of November 1, 2018, an organization subject to the Personal Information Protection and Electronic Documents Act (PIPEDA) is, in certain circumstances, required to give notice of a breach of security safeguards involving personal information under its control to both the Office of the Privacy Commissioner of Canada (the "OPC") and affected individuals.

PIPEDA defines "breach of security safeguards" as either 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.

Failure to respond to and report, where required, a breach of security safeguards may result in significant fines to an organization.

Below are critical questions and answers to help you understand and implement within your organization the breach reporting and record keeping requirements.

Reporting to the OPC

Do I need to report all "breach of security safeguards" to the OPC?

No. An organization only has to report a privacy breach involving personal information under its control if the breach creates a "real risk of significant harm" to an individual. "Significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, identity theft, and/or financial loss.

In order to determine whether a breach of security safeguards creates a real risk of significant harm, an organization needs to consider, among other factors, the sensitivity of the personal information and probability of misuse.

Does it matter how many individuals are affected by a breach of security safeguards?

Mandatory Federal Security Breach Reporting Requirements in Effect

No. Whether a breach of security safeguards affects one person or a 100,000, it must still be reported if it is determined that there is a real risk of significant harm to an individual.

What is the time within which I have to report a breach to the OPC?

Notification to the OPC must be given as soon as feasible after an organization determines that a breach has occurred.

What do I have to include in a report to the OPC?

You must submit a report to the OPC that includes the following information:

- a description of the circumstances of the breach and, if known, the cause;
- the day on which, or the 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;
- the number of individuals affected by the breach or, if unknown, the approximate number;
- a description of the steps that the organization has taken to reduce the risk of harm to affected individuals 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 OPC's questions about the breach.

Can I submit new information to the OPC?

Yes. An organization should submit any new information that it becomes aware of after having made the report.

Do I still need to report to the OPC if the personal information of my customers, employees, etc. is in the hands of a third party for processing?

You are still in control of the personal information and have to report to the OPC.

Notifying an Affected Individual

Do I need to report all "breach of security safeguards" to an affected individual?

No. The standard is the same as reporting to the OPC, i.e. when there is a "real risk of

significant harm" to the affected individual or individuals.

When do I have to report to an affected individual?

As soon as feasible after an organization determines that a security breach has occurred, unless giving notice is otherwise prohibited by law.

How do I tell an affected individual?

An organization may provide direct or indirect notification to an affected individual.

Direct notification must be visible and easy to understand and may be given by telephone, mail, e-mail or any other form of communication a reasonable person would consider appropriate in the circumstances.

Indirect notification may be allowed in the following circumstances: (1) direct notification would likely cause further harm to the affected individual; (2) direct notification would likely cause undue hardship for the organization; or (3) the organization does not have contact information for the individual.

Examples of indirect notification may include public communication such as in advertisements or announcements in online or offline newspapers.

What do I tell an affected individual?

- Notification to an affected individual must contain:
- 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.

Record Keeping Obligations

THOMPSON DORFMAN SWEATMAN

Mandatory Federal Security Breach Reporting Requirements in Effect

What are my record keeping obligations?

An organization must keep a record of "every breach of security safeguards involving personal information under its control" regardless of whether there is a "real risk of significant harm."

What do I need to include in my records?

Records should contain sufficient information to enable the OPC to verify compliance with breach of security safeguards reporting and notification requirements, including how the organization assessed whether there was a real risk of significant harm.

At a minimum, the OPC expects the following information to be included in each breach record:

- date or estimated date of the breach;
- general description of the circumstances of the breach;
- nature of information involved in the breach; and
- whether or not the breach was reported to the OPC/individuals were notified.

How long do I keep records?

An organization must maintain a record of each breach for 2 years. There may also be other legal requirements that may require you to keep records for a longer period of time.

Financial Penalties for Non-Compliance

Are there any financial penalties?

Yes. Under PIPEDA, it is an offence to knowingly contravene the breach reporting, notification and record-keeping requirements and an organization can be liable to a fine of up to $100,000.

An affected individual may also apply to the Federal Court for an award of damages, which includes damages for humiliation.

What next steps should I take?

- An organization should do the following:

Mandatory Federal Security Breach Reporting Requirements in Effect

- Review privacy policies and amend as needed;
- Develop a breach reporting and incident response plan;
- Ensure a record keeping system is in place to record all breaches;
- Do an assessment of where your data is located and with which third parties.
