How to Handle Mandatory Breach Notifications Under Canadian Privacy Law

By John Sanche, Mardi McNaughton & Peter Ciechanowski

The privacy law regime in Canada is unified in some respects, but with notable nuances and gaps. There are privacy laws with federal application and ones that apply provincially, as well as laws that apply to private sector organizations versus public bodies. There are also laws that apply specifically to health information as opposed to general personal information. The scope of this article is limited to private sector organizations dealing with personal information, generally.

The following provides a brief overview of the process of determining whether notification is required after a privacy breach in Canada, including as a result of a cyber incident, and the notification process. The following also assumes a privacy breach has occurred, meaning the loss of, unauthorized access to or unauthorized disclosure of personal information.

1. Is privacy breach notification required under applicable privacy laws?

Canadian privacy laws applicable to private sector organizations are:

- the federal *Personal Information Protection and Electronic Documents Act* (***PIPEDA***);[1]
- in certain provinces (for organizations that are not a federal work, undertaking or business), provincial privacy legislation that is substantially similar to PIPEDA, namely:
    - British Columbia's *Personal Information Protection Act* (**BC *PIPA***);[2]
    - Alberta's *Personal Information Protection Act* (**AB *PIPA***);[3] and
    - Quebec's Act respecting personal information in the private sector (***Law 25***).[4]

Under *PIPEDA*, AB *PIPA*, and *Law 25*, organizations must notify the applicable Privacy Commissioner's office—the Office of the Privacy Commissioner of Canada (**OPC**), Alberta's Office of the Information and Privacy Commissioner (**AB OIPC**), or Commission d'accès à l'information du Québec, respectively—as well as affected individuals, where a privacy breach that meets the threshold for notification has occurred.

[1] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.
[2] *Personal Information Protection Act*, SBC 2003, c 63.
[3] *Personal Information Protection Act*, SA 2003, c P-6.5.
[4] *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1.

The BC *PIPA* does not currently have mandatory breach notification requirements for private organizations, although BC's Office of the Information and Privacy Commissioner (**BC OIPC**) recommends voluntary notification.

None of the Canadian privacy laws have a specific deadline for notification; rather, they all have language requiring a degree of urgency, but no firm timeline. Under *PIPEDA*, organizations must notify the OPC and affected individuals "as soon as feasible",[5] the AB *PIPA* requires notification "without unreasonable delay",[6] and *Law 25* requires organizations to "promptly notify"[7] its commission and affected individuals if a privacy breach meets the notification threshold.

2. What is the threshold for notification?

Not all privacy breaches require notification to the applicable Privacy Commissioner or affected individuals. The threshold for notification applies where it is reasonable to believe the breach creates a real risk of significant harm to the affected individuals (the **RROSH test**).[8]

The Canadian federal and Alberta governments provide guidance on how to determine whether the RROSH test is met for a privacy breach.[9] Some of the factors considered include the sensitivity of the personal information involved in the breach and the likelihood that the information has been or will be misused, which could result in harms such as identity theft or fraud, humiliation, reputational harm or embarrassment.

3. Process for notification

If an organization has determined that a privacy breach has occurred and it meets the RROSH test, then it must notify the applicable Privacy Commissioner and the affected individuals. The federal and Alberta governments provide template documents with the information required to be included in the notices to the Privacy Commissioner and affected individuals, and other related guidance.[10] The organization may ask the Privacy Commissioner to decide whether the RROSH test has been met before notifying the affected individuals; however, unless an organization believes the RROSH test is definitely not met in the circumstances, it is almost always better to notify affected individuals either before or concurrently with the notice to the Privacy Commissioner.

---

[5] *PIPEDA*, s. 10.1(2).
[6] AB *PIPA*, s. 34.1(1).
[7] *Law 25*, s. 3.5.
[8] *PIPEDA*, s. 10.1(1); AB *PIPA*, s. 34.1(1); Law 25, s. 3.5 (note that the language in *Law 25* is "if the incident presents a risk of serious injury").
[9] See: OPC, *Assess if a privacy breach poses a real risk of significant harm to an individual* (26 March 2025), online: <priv.gc.ca/en/privacy-topics/business-privacy/breaches-and-safeguards/privacy-breaches-at-your-business/rrosh-tool/>; and AB OIPC, *Guidance for Notifying the Commissioner about a Privacy Breach under PIPA* (1 April 2024), online: <oipc.ab.ca/wp-content/uploads/2024/04/Guidance-for-Notifying-the-OIPC-about-a-Privacy-Breach-Under-PIPA-April-2024.pdf>.
[10] See: OPC, *Report a privacy breach at your business* (23 June 2025), online: <priv.gc.ca/en/report-a-concern/report-a-privacy-breach-at-your-organization/report-a-privacy-breach-at-your-business/>; and AB OIPC, *How to Notify the OIPC of a Privacy Breach* (June 2025), online: <oipc.ab.ca/breach-notification/>.

4. Advantages to proactive notification

Although there are no fixed deadlines for reporting privacy breaches in Canada, the Canadian and Alberta Privacy Commissioners advise that organizations should provide notice as soon as is reasonably possible. They understand that often the facts of a privacy breach situation are not immediately clear and may not become fully known for some time. It is not necessary to wait until all the facts are known and, in fact, the Privacy Commissioners prefer to be notified early, with whatever information is available at the time; the organization may then update its notice document to provide additional information if and when it becomes available.

In the past, the AB OIPC published all breach notification decisions (**BND**s) of whether a breach met the RROSH test; however, since April 1, 2024,[11] the AB OIPC only issues a BND where an organization has suffered a privacy breach and has not notified affected individuals or when its notice to individuals does not meet the requirements of the AB PIPA regulations. So, notifying affected individuals in compliance with the AB PIPA regulations' requirements prevents the publication of a BND (which would include the organization's name and the details of the privacy breach).

As a further reason to proactively provide notice, if the result of a BND is that the RROSH test was met for that privacy breach, the AB OIPC will require the organization to notify the affected individuals as part of that decision, so notification will be required in addition to having a published BND. It generally makes the most sense for an organization to notify the affected individuals itself, rather than having a published BND and the Privacy Commissioner then directing it to do so.

Conclusion

If your organization is based in, or operates in, any of the Canadian jurisdictions that have mandatory privacy breach notification requirements, and the organization suffers a privacy breach, it is important to analyze the situation promptly. The organization should use available guidance, including from legal counsel, to determine whether organization believes the breach meets the RROSH test. If so, it must seek further guidance, from government materials and from legal counsel, to provide appropriate notice to both the applicable Privacy Commissioner and the affected individuals.

If you have questions or would like assistance, please reach out to any member of our **Cybersecurity team**.

[11] AB OIPC, *Changes to Processing of PIPA Privacy Breach Notifications* (1 April 2024), online: <**oipc.ab.ca/wp-content/uploads/2024/04/Changes-to-Processing-of-PIPA-Privacy-Breach-Notifications-April-2024.pdf**>.