

Strategic Perspectives | Cybersecurity Policy Report

Canada: Preparing For And Responding To Security Breaches

By [Roland Hung](#) of [Torkin Manes LLP](#)

T-Mobile recently discovered that it suffered a massive security breach in or around mid-January 2023. The result of the breach was that the personal information — including names, emails and birthdays — of more than 37 million customers were stolen. The security breach cost the company more than \$350 million. For more information about the T-Mobile security breach, read [Reuters' January 20, 2023](#), article.

Similarly, SevenRooms, a popular “guest experience and retention platform” for food establishments and hospitality organizations, has confirmed it has fallen victim to a third-party vendor data breach. SevenRooms discovered that, from December 11 to December 15, 2022, an unauthorized individual was able to gain access to a third-party file transfer system used to share reservation information with SevenRooms.

The T-Mobile and SevenRooms breaches are just two examples of recent breaches. In the 2022 [Cost of a Data Breach Report](#) (the “**Report**”) based on IBM Security analysis of research data compiled by Ponemon Institute, IBM found that for 83% of companies, it’s not if, but rather when a security breach will happen. Not only are security breaches happening more often, but security breaches are also costly. According to the Report, the average total cost of a data breach in Canada in 2022 was US\$5.64 million.

In the wake of security breaches reported by T-Mobile and SevenRooms, now may be a good time for businesses to re-acquaint

themselves with the applicable Canadian statutory framework for the protection of personal information, as well as implement or update policies and procedures around breach detection and notification.

Statutory Breach Notification Requirements

Alberta’s [Personal Information Protection Act](#) (“**PIPA**”) was the first piece of Canadian legislation to require mandatory security breach notification in the private (non-health) sector. Under PIPA, businesses are required to notify the Alberta Privacy Commissioner whenever a “real risk of significant harm” to an individual as a result of a breach exists. The Alberta Privacy Commissioner may direct the business to notify the affected individuals.

Recently, Québec enacted the *Act to Modernize Legislative Provisions respecting the Protection of Personal Information* (“**Bill 64**”), which made significant amendments to Québec’s private sector law, the *Act Respecting the Protection of Personal Information in the Private Sector* (the “**New Québec Privacy Law**”). On September 22, 2022, the first set of privacy requirements (which include the appointment of a privacy officer and mandatory breach reporting) under the New Québec Privacy Law came into force.

Among other things, the New Québec Privacy Law imposes new requirements on companies to “promptly” notify the

Commission d’accès à l’information (the “**CAI**”) and affected individuals of any security breaches, called “confidentiality incidents”, that present a “risk of serious injury.” Section 3.6 of the New Québec Privacy Law defines a “confidentiality incident” broadly as unauthorized access, use or communication of personal information, loss of personal information, or other breach in the protection of such information.

Further, according to the *Quebec’s Regulation Respecting Confidentiality Incidents*, which came into force on December 29, 2022, companies will be required to maintain records of confidentiality incidents for five years after the date on which the company became aware of the violation.

The mandatory breach requirements under the New Québec Privacy Law resemble the mandatory breach requirements set out under the federal privacy legislation, the *Personal Information Protection and Electronic Documents Act* (“**PIPEDA**”).

Under PIPEDA, businesses must notify the federal Privacy Commissioner of any breach of “security safeguards” that creates a “real risk of significant harm” to an individual, “as soon as feasible”. Further, businesses are required to directly notify individuals who may reasonably face a “real risk of significant harm” from the breach as soon as feasible following the breach. This notification must allow the individual

to understand how the breach may impact them and what steps they can take to reduce or mitigate the risk.

An important difference between PIPA, and the New Québec Privacy Law and PIPEDA, is that under PIPA, the Alberta Privacy Commissioner determines whether notification to the affected individuals is required, whereas under the New Québec Privacy Law and PIPEDA, businesses are automatically required to notify the affected individuals once the respective applicable notification thresholds of risk have been met.

Penalties and Fines

Under PIPA and PIPEDA, businesses can be fined up to CA\$100,000 for failing to adhere to the mandatory breach notification provisions, a relatively low penalty compared to the New Québec Privacy Law, where administrative monetary penalties of up to CA\$10 million or 2% of worldwide turnover of the preceding year, and fines of up to CA\$25 million or 4% of worldwide turnover of the preceding year may be imposed on businesses that fail to report a confidentiality incident to the CAI or the affected individuals.

If Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, also known as the *Digital Charter Implementation Act, 2022* ("Bill C-27" or the "Bill"), modernizes PIPEDA, the penalties will be brought in line with the New Québec Privacy Law. Businesses that are found guilty of an indictable offence are liable to a fine of up to 5% of global revenue or CA\$25 million, whichever is greater. In

addition, there are administrative monetary penalties of up to 3% of global revenue or CA\$10 million for other select violations of the *Consumer Privacy Protection Act* ("CPPA"), including the failure to adhere to the mandatory breach notification provisions. Given the fines and penalties, businesses should ensure they are prepared for security breaches.

Guidelines for Protecting Personal Information

As legislative amendments are undertaken to address privacy issues, businesses will encounter increased compliance requirements. Here are some guidelines that may assist businesses in protecting data containing personal information and limit privacy liability:

- Develop a breach protocol that is amended periodically to account for improvements in technology.
- Incorporate a notification procedure in the breach protocol to report breaches to the applicable privacy regulator. Even in jurisdictions where such notification is not strictly required by law, it may be advisable to notify the privacy regulator (or affected individuals) of data breaches where such notification to the privacy regulator or individuals would help mitigate the harm arising from the breach.
- Ensure that all contracts with third parties include provisions that require the third-party contractor to immediately inform the organization of any breach or suspected breach. Inform third parties of the breach protocol once it is developed.
- Ensure that record retention and destruction policies comply with existing privacy law requirements. To ensure compliance, destroy or 'anonymize' all personal

information once it is no longer needed or legally required to be retained.

- Undertake employee training initiatives to ensure familiarity and compliance with all policies and practices.

For businesses seeking to develop policies and procedures, the following guidelines may be helpful:

- Build a security program that protects the confidentiality, integrity and availability of all information, not just personal information.
- Develop classification standards so that personal information can be easily identified.
- Ensure that proper security controls are in place and conduct risk assessments of all personal information.

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

Mr. Roland Hung
Torkin Manes LLP
151 Yonge Street
Suite 1500
M5C 2W7
Toronto
Ontario
CANADA
Tel: 4168631188
Fax: 4168630305
E-mail: publications@torkinmanes.com
URL: www.torkinmanes.com

(c) Mondaq Ltd, 2023 - Tel. +44 (0)20 8544 8300 - <http://www.mondaq.com>