CANADA'S BREACH NOTIFICATION RULES SOON TO BE IN EFFECT

Article by
Roy Argand, Patrick Fitzgerald,
Margaret MacInnis, and Matt Saunders

COX & PALMER
The difference is a great relationship

Local and global data breaches remain headline news. From Facebook's disclosure of its sharing of millions of users' profiles (without their consent) to the recent data breach involving the Nova Scotia government's Internal Services website, awareness is growing about privacy rights, how people share data, and how personal information is protected.

Canadians' interest in these issues will only increase as Canada's new mandatory data breach notification provisions under the Personal Information Protection and Electronic Documents Act (**"PIPEDA"**) come into force on November 1, 2018. Further details of the notification process are set out in the Breach of Security Safeguard Regulations (the "**Regulations**"), which were published in final form on April 18, 2018.

The new data breach notification framework lists the steps an organization must take when it experiences a "breach of security safeguards" (or a breach due to a failure to establish safeguards):

1. Determine if the breach poses a "real risk of significant harm" to any individual whose information was involved in the breach;
2. If the answer is "yes" to (1), notify affected individuals and report to the Privacy Commissioner of Canada (the "**Commissioner**") as soon as feasible after determining the breach has occurred;
3. Notify any other organization that may be able to mitigate harm to affected individuals; and
4. Maintain a record of any data breach the organization becomes aware of (and provide these records to the Commissioner upon request).

"REAL RISK OF SIGNIFICANT HARM"

Under the new framework, "significant harm" is broadly defined to include bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on one's credit record, and damage to or loss of property.

When assessing whether a breach poses a real risk of significant harm to affected individuals, the organization should consider the sensitivity of the personal information involved in the breach, the probability that the personal information has been, is being or will be misused, and other factors that may be set by regulation.

NOTIFICATION TO THE COMMISSIONER

After determining that a data breach has occurred and poses a real risk of significant harm, an organization must report the data breach to the Commissioner as soon as feasible. The Regulations require that any report to the Commissioner must be in writing, sent by any secure means of communication, and include:

- a description of the circumstances of the breach and, if known, the cause;
- 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;

- the number of individuals affected by the breach or, if unknown, the approximate number;
- a description of the steps 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 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 Commissioner's questions about the breach.

Additionally, an organization can submit to the Commissioner any new information referred to above that the organization becomes aware of after the report is made.

NOTICE TO AFFECTED INDIVIDUALS

Organizations must also provide notification to each individual affected by a breach, unless otherwise prohibited by law. Such notifications must include:

- 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 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.

Organizations must **directly** notify affected individuals of a breach in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances.

However, it is acceptable for an organization to **indirectly** notify affected individuals in the following circumstances: (i) direct notification would be likely to cause further harm to the affected individual; (ii) direct notification would be likely to cause undue hardship for the organization; or (iii) the organization does not have contact information for the affected individual. Indirect notification can be given by public communication or similar measure that could reasonably be expected to reach the affected individuals.

NOTICE TO OTHER ORGANIZATIONS

If an organization notifies affected individuals, they must also notify any other organization, government institution, or part of a government institution of the breach if the notifying organization believes that the other organization or government institution may be able to reduce the risk of harm that could result from the breach or mitigate that harm.

RECORD KEEPING

An organization must maintain a record of **every** breach of security safeguards involving personal information, even those that the organization has determined do not pose a real risk of significant harm to an individual, for a period of **24 months** after the day on which the organization determines that the breach has occurred. The record must also contain any information that enables the Commissioner to verify compliance with the provisions requiring reports to the Commissioner and notification to affected individuals.

FINES

Organizations should also be aware that knowingly failing to report to the Commissioner or notify affected individuals of a breach that poses a real risk of significant harm, or knowingly failing to maintain a record of all breaches, can lead to fines of up to $100,000, **or much more.**

The teams at Trisura and Cox & Palmer are happy to assist businesses and organizations looking for more information on how to prepare for the roll-out of Canada's data breach notification requirements. Should you have any questions, please do not hesitate to contact Michael Kalakauskas or Matt Saunders.

ABOUT COX & PALMER

200 lawyers strong, with over a century of experience serving Atlantic Canadians, Cox & Palmer is a full-service regional firm providing advice to individuals and businesses in a broad range of sectors across all major industries.

Proud to be recognized by Canadian Lawyer as a number one Atlantic Canadian law firm, they continue to attract, develop and retain top legal talent. Cox & Palmer is a member of the Nextlaw Global Referral Network, the Law Firm Diversity and Inclusion Network (LFDIN), and Pride at Work Canada.

At Cox & Palmer, they believe that strong client relationships are the foundation for great results. With excellence in client service a number one priority, they deliver timely legal solutions built on a deep understanding of our clients' needs and top quality work.

ABOUT TRISURA

Trisura Guarantee Insurance Company is a Canadian specialty lines insurance and surety company. Through a select network of national and regional brokerage firms, Trisura Guarantee provides innovative solutions and expertise in Contract, Developer and Commercial Surety, Directors' and Officers' Liability, Fidelity, Professional Liability including Media, Technology and Cyber Liability, Property, Casualty and Warranty products. Trisura Guarantee is rated A- (Excellent) by A.M. Best Company.

Trisura Guarantee is a subsidiary of Trisura Group Ltd., a leading international specialty insurance provider operating in the surety, risk solutions, corporate insurance and reinsurance segments of the market. Trisura Group has three principal regulated subsidiaries: Trisura Guarantee Insurance Company, Trisura International Insurance Ltd. and Trisura Specialty Insurance Company. Trisura Group is listed on the Toronto Stock Exchange under the symbol "TSU".