Canada's new data breach notification rules:
What you need to know

All businesses, big and small, need to be ready for Canada's new mandatory data breach notification rules under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). These changes came into effect on November 1, 2018. Failure to comply with the new rules – including failing to report breaches that pose a real risk of significant harm or deliberately failing to keep records related to such data breaches – may result in fines of up to $100,000.

To comply with the rules and avoid a potential fine, businesses are encouraged to consider the following steps if they believe they have experienced a breach.

Limit the breach: identify, investigate, contain, and assemble a response team.

Potential steps to immediately contain the breach include stopping the unauthorized practice, addressing breached servers, changing passwords, and/or correcting weaknesses in security/completing program updates.

Be sure to retain any evidence that may help determine the cause of the breach while conducting an initial investigation to determine whether a more detailed inquiry is necessary.

Assemble a response team of key people within the organization that have the knowledge, access, and authority to deal with the issue(s) at hand. Members could include:

- Chief Operating Officer or Operations Manager
- Data Privacy Officer
- Senior IT Staff / Chief Technology Officer
- Chief Marketing Officer and/or Communications
- Legal Counsel

Determine if the breach poses a "real risk of significant harm" to any individual whose information was involved.

To determine "real risk," 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
- Other factors that may be set by regulation

"Significant harm" to the individual includes:

- Bodily harm, financial loss, property damage
- Humiliation
- Identity theft, negative effects to credit record
- Damage to reputation or relationships
- Loss of employment or business opportunities

If the breach poses a real risk of significant harm, consult with your response team and notify the following:

The Commissioner

When: As soon as feasible.
What: Information about the breach and steps that have been taken as a result of the breach to reduce the risk of harm to affected individuals.
How: In writing, sent securely.

Affected Individuals

When: As soon as feasible.
What: Information about the breach and steps that have been taken as a result of the breach to reduce the risk of harm to affected individuals.
How: Organizations must generally notify affected individuals directly.

Any other organization that may be able to mitigate harm to affected individuals

Maintain records.

Organizations must keep records of every security safeguard breach involving personal information, even if they do not pose a real risk of significant harm to an individual. These records must be maintained for a period of 24 months after determining that a breach has occurred.

Please contact our Cybersecurity & Privacy group with any questions regarding data breaches:

Matt Saunders, CIPP/C
(902) 491-4221 | msaunders@coxandpalmer.com

Roy Argand
(902) 491-4133 | rargand@coxandpalmer.com

Margaret MacInnis, CIPP/C
(902) 491-4120 | mmacinnis@coxandpalmer.com

Patrick Fitzgerald
(902) 491-4117 | pfitzgerald@coxandpalmer.com