June 8, 2017

Data Breach Reporting Obligations

In Canada, breach reporting to the appropriate regulatory bodies is currently only mandatory for private sector organizations in Alberta under the provincial *Personal Information Protection Act* (PIPA), as well as organizations subject to provincial health-specific legislation in Ontario, New Brunswick, and Newfoundland & Labrador. These organizations are required to report a breach to provincial information and privacy commissioners if personal information under the organization's control is lost, accessed or disclosed without authorization, and where the threshold for notification to the individual is met (normally in the event of a "real risk of significant harm" to an individual). Failure to report a breach to the commissioner or notify individuals of a breach in such where required by law constitutes an offence under the applicable legislation.

The commissioners have interpreted "significant harm" to mean a material harm having non-trivial consequences or effects. Examples include potential financial loss, damage to property identity theft, physical harm, humiliation, or damage to one's professional or personal reputation. Some commissioners have set a low threshold. For example, decisions in Alberta have concluded that unauthorized access to email addresses along with information about the organization with whom the affected individual does business could lead to significant harm because of a risk of phishing schemes. Generally, significant harm is certain to be considered to exist where there is unauthorized access to or loss of sensitive personal information, such as financial or medical information. The commissioner will review the information provided by the organization to determine whether affected individuals need to be notified of the data breach, and may direct the organization to notify individuals in the form and manner prescribed by applicable regulations, or where a breach notification has already been made to affected individuals, may review the adequacy of that notification.

It should be noted that many organizations will notify affected individuals and voluntarily report breaches to the relevant commissioners. Even where there is no mandatory reporting and notification, a failure to notify may lead to an investigation by the relevant commissioner and a determination that the organizations failed to discharge its obligation to adequately safeguard personal information. It is therefore essential to consider the need to make notifications and reports even where these requirements are not specifically legislated.

A new provision of the federal private sector law *Protection of Personal Information and Electronic Documents Act* (PIPEDA) that will require mandatory breach notification is expected

to come into force by the end of 2017. PIPEDA applies to private sector organizations throughout Canada, with the exception of Alberta, British Columbia and Quebec that have enacted "substantially similar" provincial legislation. Once PIPEDA's mandatory notification provision comes into force, organizations that suffer a data breach that creates a "real risk of significant harm" will be required to undertake specified breach reporting and notification measures. In addition, there will be a requirement to maintain detailed records of breach incidents, even where these incidents do not reach the threshold for reporting and notification.

PIPEDA's offence provisions will also be modified to create offences for non-compliance with data security breach obligations. Organizations may face fines per violation of up to $10,000 for a summary offence, or up to $100,000 for an indictable offence for failure to report and record a breach or hindering the commissioner's efforts to investigate a complaint or perform an audit.

Data Breach Class Actions

Although Canadian jurisprudence has yet to consider issues of insurance coverage in the context of privacy breaches, a growing number of privacy class actions arising out of data breaches have been commenced over the last several years. This is due in part to the active enforcement activities of Canadian privacy regulators, as well as the recognition by Ontario courts of privacy torts such as "intrusion upon seclusion" (see *Jones v Tsige*) and "public disclosure of embarrassing private facts" (see *Doe 464533 v N.D.*).

For example, a class action for "publicity given to private life" was certified in the Federal Court (see *John Doe and Suzie Jones v. Her Majesty the Queen*), in a case where a number of individuals received correspondence from Health Canada in envelopes that identified them as participants of the medical marijuana access program. The Federal Court of Appeal reversed the certification of this cause of action (see *Canada v John Doe*) on the facts of that case, but affirmed the existence of the cause of action for invasion of privacy, which could be established where the matter publicized was highly offensive to a reasonable person and not of legitimate concern to the public.

Recent jurisprudence also suggests that the way in which organizations respond to data breaches can have a significant impact on reducing the risk of a successful class action lawsuit. Organizations may mitigate their potential liability for a data breach by adopting proactive breach prevention and management measures.

Data Breach Management

Every organization should have a breach management policy and procedure in order to be able to take timely action in response to a breach event. At minimum, policies and procedures should include the follow key breach reaction steps:

1. **Breach containment and preliminary assessment:** take immediate steps to limit the breach, including stopping the unauthorized practice; recovering the compromised records; shutting down the system that was breached; revoking or changing computer access codes; and correcting weaknesses in physical or electronic security;
2. **Evaluation of the risks associated with the breach:** determine what steps are immediately necessary and the severity of the breach, and assess the risks associated with the breach, by considering the following factors: type of incident, type of personal information in issue, security measures in place, cause and extent of the breach, the number of affected individuals, and the extent of foreseeable harm from the breach;
3. **Notification and Reporting:** determine whether notification/reporting must be made to appropriate regulatory authorities, affected individuals and any other organizations, institutions or law enforcement agencies, by considering whether there is a real risk of significant harm to the individual, as well as the organization's legal and contractual obligations; and
4. **Prevention of future breaches:** develop a prevention plan, which may include a security audit, as well as reviews of policies and procedures, staff or volunteer training practices, and third party service providers.

Authors

Anastasia Semenova, LLB, LLL

Associate

/en/canada/people/anastasia-semenova

Email Anastasia Semenova, LLB, LLL
(613) 786-0207

Wendy J. Wagner

Partner

/en/canada/people/wendy-wagner
Email Wendy J. Wagner
613-786-0213