PRIVACY PRESS

A NEWSLETTER BY FIELD LAW'S PRIVACY GROUP

SUMMER 2010

ANNE CÔTÉ

ALBERTA INTRODUCES MANDATORY PRIVACY BREACH NOTIFICATION

Data breaches are like pollution: a preventable byproduct of organizational activities that exposes people to harms. The challenge in both cases is to maximize social welfare while minimizing everyone's costs to optimal levels.[1]

What is the role of an organization in a privacy breach incident? A partial answer comes from the amendments to the *Personal Information Protection Act* ("PIPA"), which were proclaimed in force on May 1, 2010. On that date, Alberta became the first jurisdiction in Canada to require notification in the event of a privacy breach.

Many private-sector organizations are subject to the provisions of PIPA: businesses, certain non-profit organizations, professional regulatory organizations, and others. These organizations must now notify Alberta's Information and Privacy Commissioner (the "Commissioner") if personal information in the organization's control is lost or is accessed or disclosed without authorization, if the incident reaches the required threshold for harm.

What types of privacy breaches would be covered by the amendments? Examples include the following:

- loss of a laptop containing personal information about clients or customers;
- a client database being accessed by hackers;
- theft of a point-of-sale terminal containing customer credit and debit card information; or
- a rogue employee selling customer credit card information.

The Commissioner must be notified without unreasonable delay if a reasonable person would view the incident as presenting a "real risk of significant harm" to the affected individuals. A *real* risk is a genuine risk, not one that is merely theoretical or hypothetical. The organization must consider the likelihood that the information could be accessed or misused by an unauthorized individual. *Significant* harm occurs when there is harm of importance or consequence. Examples include potential financial loss, identity theft, physical harm, embarrassment or harm to reputation.

Where the threshold for harm is reached, the following information must be provided to the Commissioner:

- a description of the circumstances of the breach;
- the date on which, or the time period during which, the breach;
- a description of the personal information involved;
- an assessment of the risk of harm to individuals as a result of the breach;
- an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the breach;
- a description of any steps the organization has taken to reduce the risk of harm to individuals;
- a description of any steps the organization has taken to notify individuals of the breach; and
- the name of and contact information for a person who can answer, on behalf of the organization, questions about the breach.

The Commissioner determines whether, and how, the organization must inform affected individuals. The amendments to PIPA also give the Commissioner the power to require that the organization satisfy additional terms and

---

1 A. Cavoukian, Information and Privacy Commissioner of Ontario, "Privacy Externalities, Security Breach Notification and the Role of Independent Oversight" (May 2010) Canadian Privacy Law Review

conditions that the Commissioner considers appropriate. This may include the requirement that the organization continue to report to the Commissioner regarding the notification process. It is not yet known what other terms or conditions the Commissioner will order in this regard.

Organizations may also notify affected individuals without awaiting a response from the Commissioner's office. This may well be advisable in the event that the risk of significant harm is obvious and immediate (although the amendments require that the Commissioner create an "expedited" process in such a situation). Further, the Commissioner may require that the Organization notify affected individuals when the Commissioner has not received a direct report of a privacy breach from the organization itself but has learned of the incident through media reports or other means.

If the Commissioner requires that the organization notify affected individuals, the notice must include the following information: a description of the incident; the time when the incident occurred; a description of the personal information involved; information about any steps taken to reduce the risk of harm; and contact information for a person who can answer the individual's questions.

Organizations should consider the impact of the mandatory breach notification requirements on their operations. It is an offence to fail to notify the Commissioner of a privacy breach that poses a real risk of significant harm to individuals. It is also an offence to fail to comply with an order of the Commissioner, such as an order to notify affected individuals. Conviction of an offence can result in the organization being fined in an amount up to $100,000. In addition, once an order has been issued by the Commissioner, an affected individual has a cause of action against the organization for any harm resulting from the matter at issue in the order. It remains to be seen if the breach notification amendments lead to actions being filed against organizations.

These amendments serve not merely as a reminder to organizations about the proper response to a privacy breach once it has occurred, but also as a reminder that breaches are better avoided than endured. Because of these and other changes to the private-sector privacy regime in Alberta, this is an excellent time for organizations to review their privacy practices and policies. ▲

	edmonton	
JANE STEBLECKI	PH 780 423 9594	jsteblecki@fieldlaw.com
	calgary	
KELLY NICHOLSON	PH 403 260 8515	knicholson@fieldlaw.com
AYLA AKGUNGOR	PH 780 423 9595	aakgungor@fieldlaw.com
SANDRA ANDERSON	PH 780 423 7602	sanderson@fieldlaw.com
BONNIE BOKENFOHR	PH 780 423 7659	bbokenfohr@fieldlaw.com
ANNE CÔTÉ	PH 780 423 7663	acote@fieldlaw.com
KATRINA HAYMOND	PH 780 423 9584	khaymond@fieldlaw.com
LINDSEY MILLER	PH 780 423 7649	lmiller@@fieldlaw.com
KATIE OVIATT	PH 780 423 7601	koviatt@fieldlaw.com
BRENT WINDWICK	PH 780 423 7696	bwindwick@fieldlaw.com

EDMONTON
2000, 10235 - 101 STREET
EDMONTON AB T5J 3G1
PH 780 423 3003
FX 780 428 9329

CALGARY
400, 604 - 1 STREET
CALGARY AB T2P 1M7
PH 403 260 8500
FX 403 264 7084

YELLOWKNIFE
201, 5120 - 49 STREET
YELLOWKNIFE NT X1A 1P8
PH 867 920 4542
FX 867 873 4790

WWW.FIELDLAW.COM