Advisory for

Notifying Affected Individuals under PIPA

The *Personal Information Protection Act* (PIPA) requires organizations to make reasonable security arrangements to protect personal information in their custody or control from such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

Section 34.1 of PIPA requires organizations to notify the Information and Privacy Commissioner of Alberta (Commissioner) of certain breaches involving personal information.[1] Where an organization suffers a breach that the organization is required to provide notice of under section 34.1, the Commissioner has authority under Section 37.1 of PIPA **to require organizations to notify individuals affected by a reportable breach.**

Section 37.1 of PIPA states:

> **Power to require notification**
>
> 37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
>
> (a) in a form and manner prescribed by the regulations, and
> (b) within a time period determined by the Commissioner.
>
> (2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).
>
> (3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.
>
> (4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization
>
> (a) in a form and manner prescribed by the regulations, and
> (b) within a time period determined by the Commissioner.

[1] Section 34.1 of PIPA states, "An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure".

Office of the Information and Privacy Commissioner of Alberta

Issued June 2012; last updated August 2018

(5) An organization must comply with a requirement

(a) to provide additional information under subsection (4),
(b) to notify individuals under subsection (1), or
(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),
(b) to notify individuals under subsection (1), or
(c) to satisfy terms or conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

When the Commissioner requires an organization to notify individuals in accordance with section 37.1, section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) specifies what must be included in the notification.

Section 19.1 of the Regulation states:

Notification to individuals

19.1(1) Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must

(a) be given directly to the individual, and
(b) include

(i) a description of the circumstances of the loss or unauthorized access or disclosure,
(ii) the date on which or time period during which the loss or unauthorized access or disclosure occurred,
(iii) a description of the personal information involved in the loss or unauthorized access or disclosure,
(iv) a description of any steps the organization has taken to reduce the risk of harm, and
(v) contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure.

(2) Notwithstanding subsection (1)(a), where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances.

Section 37.1(7) of PIPA clearly states that **an organization is not prohibited or restricted from notifying individuals on its own initiative**. When notifying individuals on their own accord, **organizations are encouraged to notify individuals in the form prescribed by the Regulation to avoid the potential of having to re-notify affected individuals** should the Commissioner require notification under section 37.1. The Commissioner will (and has) require(d) organizations to re-notify affected individuals where the prior notification issued by the organization did not meet the requirements of the Regulation.

Other Resources

Additional resources are available at **www.oipc.ab.ca**.

You may also contact the OIPC for general information about responding to a privacy breach, by calling (780) 422-6860 or toll free at 1-888-878-4044. Information provided does not constitute legal advice, is not binding on the Commissioner, and does not mean an organization or custodian has fulfilled its legal obligation to report a privacy breach to the Commissioner.