ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-06

Boehringer-Ingelheim (Canada) Ltd.

February 14, 2013

(Case File #P2195)

I. Introduction

[1] Under s. 34.1 of the *Personal Information Protection Act* ("PIPA"), an organization having personal information under its control must, without unreasonable delay, notify me 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.

[2] On November 16, 2012, Boehringer-Ingelheim (Canada) Ltd. (the "Organization") provided notice of an incident involving the unauthorized disclosure of personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to the individuals as a result of the incident. I require that the Organization notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[3] Section 37.1 of PIPA authorizes me to require an organization to notify individuals to whom there is a real risk of significant harm as a result of an incident. It states:

> 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) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

(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), and

(c) to satisfy terms and 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.

[4] PIPA applies to organizations, defined in section 1(1)(i) of PIPA as follows:

1(1) (i) "organization" includes

(i) a corporation,

(ii) an unincorporated association,

(iii) a trade union as defined in the *Labour Relations Code*,

(iv) a partnership as defined in the *Partnership Act*, and

(v) an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity;

[5] The Organization is registered as an extra-provincial federal corporation operating in Alberta. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA.

[6] The Organization reported that the incident involved the following information of 275 customers, 26 of whom are from Alberta ("the Affected Individuals"):

- name,
- work email address,
- home address, and
- driver's licence number.

[7] This information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] On November 26, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between November 28, 2012, and January 14, 2013.

[9] The circumstances of the incident as reported to me by the Organization are as follows:

- On October 17, 2012, a service provider sent an email to 182 individuals (the "Recipients"). 172 of the Recipients were employees of the Organization. Inadvertently attached to the email was a spreadsheet containing the personal information.
- The Organization is in the process of obtaining undertakings from the Recipients that they deleted the spreadsheet, did not retain a copy, and would not use the contents of the spreadsheet for any purpose. It has only been able to obtain an undertaking from 73 Recipients.
- The Affected Individuals were notified of the incident by email on October 25, 2012.

- The Organization offered credit monitoring for the Affected Individuals.

IV. Is there a real risk of significant harm to individuals as a result of the incident?

[10] In considering whether to require the Organization to notify the Affected Individuals, I am mindful of PIPA's purpose, legislative principles, and the relevant circumstances surrounding the reported incident.

[11] Pursuant to section 37.1 of PIPA, I have the power to 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." In determining whether or not to require the Organization to notify the Affected Individuals, I must consider if there is a "real risk of significant harm" to the Affected Individuals as a result of the incident.

[12] In order for me to require that the Organization notify the Affected Individuals, there must be some harm – some damage or detriment or injury – that could be caused to those Affected Individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[13] The Organization reported that the incident did pose a low risk of significant harm to the Affected Individuals due to the sensitivity of the personal information involved. The Organization stated that the incident may result in identity theft or fraud.

[14] In my view, the personal information at issue is moderate to highly sensitive. It includes the name, home address, driver's licence number, and work email of the Affected Individuals. The type of harm that could result to the Affected Individuals as a result of unauthorized access to the personal information in this incident is identity theft and fraud. In my view, these are significant harms.

[15] In order for me to require the Organization to notify the Affected Individuals, there must also be a "real risk" of significant harm to the Affected Individuals as a result of the incident. This standard does not require that significant harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.

[16] In deciding whether there exists a "real risk" of significant harm in this incident to the Affected Individuals, I considered the following factors:

- The personal information is moderate to highly sensitive.
- The type of information involved could be used to commit identity theft and fraud.
- The number of unauthorized recipients is considerable.

- The Organization has been unable to obtain an undertaking from all the Recipients that the personal information would be deleted, has not been copied, and would not be used for any purpose.

[17] In P2011-ND-014, P2011-ND-022, and P2012-ND-01 it was decided that the unauthorized disclosure of name, home address, and driver's licence number posed a real risk of significant harm, identity theft and fraud, to the affected individuals involved in those incidents.

[18] Based on the above and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the Affected Individuals as a result of this incident.

V. Decision

[19] I require the Organization to notify the Affected Individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation").

[20] I understand that the Organization has notified the Affected Individuals in accordance with the Regulation in an email on October 25, 2012. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner