ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-023

LIFESCAN CANADA LTD.

August 4, 2011

(Case File #P1905)

I. Introduction

[1] On June 9, 2011, I received a report from LifeScan Canada Ltd. ("LifeScan") of an incident involving the unauthorized access to or disclosure of personal information. Based on the information reported to me, I have decided that there is a real risk of significant harm to individuals as a result of the incident, and therefore I require that LifeScan notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] 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.

[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] I have jurisdiction in this matter because LifeScan is an "organization" as defined in section 1(1)(i) of PIPA, and the information at issue in this incident qualifies as "personal information" as defined in section 1(1)(k). LifeScan reported that 4 out of the 78 affected individuals are residents of Alberta.

[6] In considering whether to require LifeScan to notify affected individuals, I am mindful of PIPA's purpose and legislative principles and the relevant circumstances surrounding the reported incident.

III. Background

[7] On June 9, 2011, I received a written report from LifeScan describing an incident involving the unauthorized access to or disclosure of personal information.

[8] On June 21, 2011, my Office contacted LifeScan to request that it provide additional information concerning the incident, in order for me to determine whether to require LifeScan to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls and email correspondence between June 21, 2011 and July 12, 2011.

[9] My Office received LifeScan's response on July 12, 2011.

[10] The circumstances of the incident reported to me are as follows:

- Between October 20, 2010, and November 10, 2010, LifeScan ran a contest entitled the "Breakfast Challenge" (the "Contest"). To enter the Contest, entrants were asked to submit on the Contest website an original diabetes friendly recipe.
- With the entry, the Contest entrants provided the following personal information: name, address, telephone number, email address, date of birth, gender, and connection to diabetes, either their own experience or someone they know.
- On May 10, 2011, LifeScan received an email from an individual who indicated that their personal information in connection with the Contest was visible on the public webpage.
- The Contest website was removed on May 11, 2011. LifeScan worked with various search engine companies to ensure that any personal information in the search engines' cached memory was deleted. By May 13, 2011, personal information of the Contest entrants was no longer available online.
- An investigation by LifeScan revealed that personal information of Contest entrants was stored on web pages that were not intended to be accessible by the public.

- The information was accessible from October 20, 2010 – May 13, 2011.
- There were a total of 78 entrants. Of the 78, 4 were residents of Alberta.
- LifeScan requested an analytic report from one of the search engines to identify if the pages containing the information of the entrants were ever accessed. The analytic report confirmed that 13 Contest entrants' personal information was accessed by at least one person when it was displayed on the webpage. One resident of Alberta was among the 13 Contest entrants whose information was verified as accessed.
- LifeScan sent out two notification letters on June 20, 2011; one letter to the 13 Contest entrants whose personal information was confirmed accessed by the analytic report, and another letter to the balance of the Contest entrants.
- LifeScan has offered all Contest entrants one year of identity theft monitoring services.

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

[11] Pursuant to section 37.1 of PIPA, I have the power to require LifeScan 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 LifeScan to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

[12] In order for me to require that LifeScan notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the Contest entrants as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

[13] In this case, the personal information at issue is of moderate to high sensitivity as it includes name, home address, email address, date of birth, gender and information concerning a medical condition that is either personal to the Contest entrant or an acquaintance.

[14] LifeScan also noted that the type of harm that could result from the unauthorized access to or disclosure of this information is identity theft, which, in my view, is a significant harm.

[15] In order for me to require LifeScan to notify the Contest entrants, however, there must also be a "real risk" of significant harm to the employee 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. Further, 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 harm in this case, I considered that the data elements pose a risk of identity theft, that they were posted on a website for

almost 7 months and that harm may result to reputation or distress from having knowledge of a medical condition posted on web pages that were not intended to be accessible by the public.

[17] Given the information reported by LifeScan, I have decided that there is a real risk of significant harm to individuals as a result of this incident. I have based my decision on the following factors: the type and sensitivity of the information, the length of time the personal information was exposed and the large potential audience it was exposed to on the website.

V. Decision

[18] Based on the information reported to me by LifeScan, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require LifeScan to notify individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation.*

[19] I understand LifeScan has already notified the Contest entrants by way of the letters sent on June 20. 2011. The June 20, 2011, letters, however, do not contain the requirement pursuant to 19.1(1)(b)(ii) with respect to informing the affected individuals of the date on which or time period during which the loss or unauthorized access or disclosure occurred which is significant if the affected individuals need to review their records for any unauthorized activity. I order that LifeScan notify individuals in Alberta of the time period the personal information was available on the public website in accordance with s.19.1(1)(b)(ii) by August 15, 2011.

Frank Work, Q.C.
Information and Privacy Commissioner