ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-029

Liquor Stores Limited Partnership

September 9, 2011

(Case File #P1961)

I. Introduction

[1] On August 18, 2011, I received a report from Liquor Stores Limited Partnership ("LSLP") of an incident involving the loss 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 LSLP 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 LSLP 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). Although the personal information at issue is that of U.S. employees and the information was lost in the U.S., LSLP is an Alberta based corporation which had control over the personal information at issue. Therefore, LSLP is subject to PIPA.

[6] In considering whether to require LSLP 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 August 18, 2011, I received a written report from LSLP describing an incident involving the loss of personal information.

[8] On August 18, 2011, my Office contacted LSLP to request that it provide additional information concerning the incident, in order for me to determine whether to require LSLP 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 August 18, 2011 and August 26, 2011.

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

- LSLP has a number of subsidiary Canadian and US corporations. LSLP entered into an agreement with an IT service provider to transfer information from a subsidiary organization's Alaskan database into its main database. The Alaskan database included the personal information of employees.

- LSLP's IT service provider entered into a subcontract with another IT service provider, Microsoft Business Solutions ("Microsoft") to assist with the database transfer and subsequently provided the Alaskan database information in a secure format to Microsoft.

- According to Microsoft, several hard drives, including a hard drive containing information from the Alaskan database was reported missing from the work area in its secured facility in Fargo, North Dakota on July 26, 2011. Microsoft investigated the matter as a potential theft and reported the lost hard drives to local police. On August 2, 2011 LSLP was notified of the potential theft.

- Microsoft advised LSLP that the information on the hard drives was neither encrypted nor password protected at the time it was lost.

- Personal information on the lost or potentially stolen hard drive included personal information of 386 past and present U.S. employees of a subsidiary of LSLP. No Canadians were affected by the breach. The personal information of the 386 affected US employees includes the following:

    - Names;
    - Addresses;
    - Dates of Birth and
    - Social Security Numbers.

- Since learning of the breach, at the direction of LSLP, LSLP's US subsidiary has taken the following proactive steps:

    i) The subsidiary sent out written notices to all current and past affected employees. The notification explains the circumstances surrounding the lost hard drive, steps that can be taken by the employees to avoid identity theft, and offers them a free third party service (at the expense of the subsidiary) to monitor their credit and assist in preventing identity theft over the next two years. Many of the affected employees have accepted the credit monitoring service.

    ii) The Director of Operations of the subsidiary has held informal meetings with many affected employees to further explain the facts surrounding the breach and to answer and respond to employee questions and concerns.

    iii) LSLP has engaged in weekly discussions with Microsoft to monitor the status of the Microsoft internal investigation.

- Regulatory authorities in the United States have also been informed of the breach, and to date no authority has expressed concern respecting this breach or the steps taken to mitigate the effect of same.

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

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

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

[12] In this case, the personal information at issue is of high sensitivity as, in addition to names and addresses, it includes date of birth and social security numbers of affected employees.

[13] LSLP 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.

[14] In order for me to require LSLP to notify the affected individuals, 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.

[15] In deciding whether there exists a "real risk" of harm in this case, I considered that the circumstances surrounding the incident indicate that several hard drives may have not just been lost, but stolen from Microsoft's secure facility. The possibility of theft greatly increases the "real risk".

[16] Given the information reported by LSLP, 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 of information involved could be used to commit identity theft, which is a significant harm, and the circumstances indicate the hard drive may have been stolen from Microsoft's secure facility.

V. Decision

[17] Based on the information reported to me by LSLP, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require LSLP to notify the affected individuals. I understand LSLP has already notified the individuals in

accordance with section 19.1 of the *Personal Information Protection Act Regulation* by way of letters sent on August 5, 2011; therefore I will not require LSLP to notify again.

Frank Work, Q.C.
Information and Privacy Commissioner