**ALBERTA**

**OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER**

**P2011-ND-041**

**Travers Food Service Ltd.**

December 14, 2011

(Case File #P1952)

## I. Introduction

[1] On August 3, 2011, I received a report from Travers Food Service Ltd. ("Travers") of an incident involving the 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 Travers 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 Travers 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).

[6] In considering whether to require Travers 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 3, 2011, I received a written report from Travers describing an incident involving the disclosure of personal information.

[8] On August 8, 2011, my Office contacted Travers to request that it provide additional information concerning the incident, in order for me to determine whether to require Travers 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 8 and December 9, 2011.

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

- Travers provides food services to numerous organizations. One of its clients operates at a remote site north of Fort McMurray, Alberta. Travers operates a cafeteria at this remote site.

- In January 2011, Travers installed a Point of Sale (POS) terminal in the cafeteria for credit card transactions and a second POS terminal was installed in March 2011. As a result of the remote location, Travers does not have its own external networking infrastructure, but uses its client's network at this particular remote site.

- On July 20, 2011, a security scan of the external facing network discovered that network share folders on Travers' computers held data about credit card transactions that had occurred that day. These computers were connected to the

client's external networking infrastructure. Although the folders were hidden, they could be located and accessed by users of the network and the internet. Upon discovery the system was immediately shut down and investigated, but prior to discovery, the credit card data had been disclosed for approximately 6 months, from January to July 2011.

- The credit card data in the shared folder was not encrypted.

- The type of personal information that was disclosed included:
    - Cardholder name;
    - Credit card number;
    - Expiration date;
    - Card type;
    - Authorization code;
    - Authorized amount;
    - Batch code; and
    - Transaction code.

- Upon investigation of the security breach, Travers determined that the credit card information was deleted every day, so only transactions that occurred on a particular date were disclosed on that date. Travers reported that on any given day there were likely to be anywhere from 50 – 100 transactions on the POS terminals. It is difficult to estimate the number of affected individuals. Over approximately six months, credit card transactions for that particular day were disclosed. Given the remote facility, it is likely that many of the transactions were repeat customers, so the number of affected individuals could range anywhere between 2000 – 18,000 individuals.

- Travers explained that the credit card data was stored in an unencrypted format in the folders, but was sent for processing in an encrypted form at the end of each day.

- After investigating the breach, it was determined that the operating software was out of date and had not been upgraded. As a result of the breach, the software was upgraded and all credit card information was stored in an encrypted form which was not accessible to users of the client's network or the Internet.

- Travers indirectly notified affected individuals by posting a notice about the breach in the cafeteria where the information was collected shortly after discovery of the breach.

## 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 Travers 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 Travers 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 Travers notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to those individuals 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 it includes a combination of credit card information such as cardholder name, card number and expiry date.

[13] Travers also noted that there was a high risk of credit card fraud that could result from the disclosure of this information, which, in my view, is a significant harm.

[14] In order for me to require Travers to notify the affected individuals, however, there must also be a "real risk" of significant harm to those 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. Further, there must be a cause and effect relationship between the incident and the possible harm.

[15] Travers stated there was no evidence that the credit card information had actually been accessed by anyone other than the security professionals who had been hired to find system vulnerabilities; however, there was no audit capability to determine whether the credit card information had been accessed. I note that although Travers acted quickly to secure the information once the breach had been discovered, daily credit card transaction data had been available on the Internet and through the network for approximately six months.

[16] In deciding whether there exists a "real risk" of significant harm in this case, I considered that the personal information was unencrypted in a hidden folder and was disclosed not only to those on the network at the remote facility, but by any user of the internet who knew to look for this sort of information. Viewing "hidden" folders does not require sophisticated computer skills. Further, the incidence of system breaches is rapidly increasing and there are many "hackers" who do little but sniff around network systems looking for vulnerabilities such as this. The personal information at risk in this case was disclosed to any person online who looked for it that it could have been accessed.

[17] Given the information reported by Travers, 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 credit card fraud, which is a significant harm; and given the disclosure of the personal information on the Internet, there is a real risk.

## V. Decision

[18] Based on the information reported to me by Travers, I have concluded that there is a real risk of significant harm to individuals as a result of this incident and I require Travers to notify affected individuals.

[19] Section 19.1(2) of the *PIPA Regulation* gives me the discretion to decide whether the notification may be given to the affected individuals indirectly if I determine that direct notification would be unreasonable in the circumstances. In exercising my discretion, I reviewed persuasive evidence from Travers that direct notification would not be possible because neither Travers nor its third party payment processor had contact information for the affected individuals. I am satisfied that direct notification of the affected individuals would be unreasonable in these circumstances and, therefore, I require that indirect notification be given to the affected individuals.

[20] Travers has already provided some level of indirect notification by posting a notice in the cafeteria where the breach occurred. However, given the transitory nature of the remote workplace, I am not satisfied that this notice is sufficient. Therefore, I require in accordance with my authority under section 37.1(2) that Travers indirectly notify the affected individuals by posting a general notification about the breach containing the information set out in section 19.1(1)(b) of the *PIPA Regulation* on its website for a period of 30 calendar days and placing said notification for a reasonable period in two major daily newspapers in the cities of Edmonton and Calgary, Alberta.

Marylin Mun
Assistant Commissioner