ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-002

MINI MALL SELF STORAGE LTD.

January 14, 2011

(Case File #P1726)

I. Introduction

[1] On November 17, 2010, I received a report from Mini Mall Self Storage Ltd. (Mini Mall) 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 Mini Mall notify those individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] PIPA applies to provincially-regulated private sector organizations in Alberta. I have jurisdiction in this case because Mini Mall is an "organization", as defined in section 1(1)(i) of the Act, operating in the province of Alberta.

[3] 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.

[4] 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.

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

III. Background

[6] On November 17, 2010, I received a written report from Mini Mall describing an incident involving the loss of personal information.

[7] On November 18 and 19, 2010 my Office contacted Mini Mall to request that it provide additional information concerning the incident, in order for me to determine whether to require that it notify individuals under subsection 37.1(1) of PIPA. My Office received Mini Mall's responses on November 18 and December 14, 2010.

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

- Sometime between midnight and 12:30 am on November 8, 2010, individuals broke into the Mini Mall premises and stole among other items, computer towers. The break and enter and loss was discovered the morning of November 8, 2010 by a Mini Mall employee.
- The following personal information was on the hard drives of the computer towers that were stolen:
    - Customer Information: For all customers: name, address, home phone number, workplace and phone number, driver's license number, next of kin name and their address and phone numbers. For about 40 customers: names and credit card number with expiry date. For about 20 customers: names and bank account information (including branch, transit number, and account number)
    - Employee Information: name, address, phone numbers, SINs and birth dates.
- In addition, certain paper records were also stolen. The following personal information was on the paper records:
    - Customer Information: Credit card receipts from Nov. 1-6, 2010 of those approximately 40 customers mentioned above who had already paid, and those that had come in to use their credit card to make a payment for that month. Mini Mall estimates that there were about 5 people who had used their cards (either credit card or debit card) over and above those on the lists.
- Approximately 208 customers of Mini Mall were affected by this incident as well as 3 current employees and 2 former employees.
- The computers and the programs were both password protected but the information was not encrypted.
- Mini Mall believes the information from the computers was stolen for the purpose of committing fraud and identity theft and that there is a real risk of significant harm to the individuals affected by this incident.
- In addition to reporting the incident to the police, Mini Mall has taken a number of steps to reduce the possible harm to customers and employees.
- Mini Mall has verbally notified its current employees and the customers who have come into the premises since the incident and sent a letter on December

15, 2010 to all customers and the former employees affected by the incident notifying them of the incident.

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

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

[10] In order for me to require that Mini Mall notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to 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.

[11] In my view, the personal information of the customers contained on the computer hard drives which included their name, address, home phone number, workplace and phone number, driver's license number, next of kin name and their address and phone numbers is of moderate to high sensitivity.

[12] In my view, the personal information of those customers contained on the computer hard drives and in the paper records which included their names, credit card numbers with expiry date or specific banking information is of high sensitivity.

[13] Similarly, in my view, the personal information of the employees, which included name, address, phone numbers, SINs and birth dates is of high sensitivity.

[14] In all three instances, this is information that could be used to cause significant harm to individuals, and provides partial or comprehensive individual profiles that could be used for identity theft and/or fraud.

[15] In order for me to require Mini Mall to notify individuals, however, there must also be a "real risk" of harm to individuals as a result of the incident. This standard does not require that 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] I note that while Mini Mall acted quickly to inform the police of this incident and take other steps to reduce the chance of fraud and identity theft, the computer hard drives were stolen, were unencrypted and along with the paper records, have not been recovered.

[17] Given the sensitivity of the personal information and the fact the information was stolen and in the case of the computer files was unencrypted, I believe there is a real risk of significant harm to these particular customers and employees of Mini Mall.

V. Decision

[18] Based on the information reported to me by Mini Mall, I have concluded there is a real risk of significant harm to the Mini Mall customers and employees whose information was located on the computer hard drives or in the paper files as a result of this incident and I require the Mini Mall to notify these individuals in accordance with the Regulations.

[19] I understand Mini Mall has already notified the affected individuals.

Frank Work, Q.C.
Information and Privacy Commissioner