ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-014

LEXAND ELECTRIC INC.

June 6, 2011

(Case File #P1860)

I. Introduction

[1] On April 21, 2011, I received a report from Lexand Electric Inc. ("Lexand") of an incident involving the loss of and unauthorized access to 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 Lexand 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 Lexand 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 signification 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 Lexand 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 April 21, 2011, I received a written report from Lexand describing an incident involving the loss of and unauthorized access to personal information.

[7] On April 26, 2011, my Office contacted Lexand and spoke with its President requesting additional information concerning the incident and further clarification beyond information contained in Lexand's breach report submitted to this Office, in order for me to determine whether to require that it notify individuals under subsection 37.1(1) of PIPA.

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

- On April 10, 2011, the President of Lexand discovered that his vehicle been burglarized and several items stolen, including one external hard drive (backup of Lexand's server) containing the personal information of current and former employees of Lexand as well as information concerning new home owners. Also stolen from his vehicle was a brief case containing a list of empoyee user IDs and passwords.

- The President of Lexand notified the Edmonton City Police of the incident on April 10, 2011.

- The external hard drive contained personal information of a total of 71 employees (12 current and 59 former employees) in a backup of an accounting file.

- The personal information of the current and former employees on the external hard drive consisted of the following:

    - First and last name
    - Address
    - Phone numbers
    - Date of birth
    - Social Insurance Numbers
    - Pay rate
    - Driver's license numbers (for 9 employees).

- The personal information of new home owners included name, address of new home under construction, and phone number.

- The external hard drive was not encrypted nor was it password protected.

- Lexand has already verbally notified its current employees of the incident, as well as provided them with a letter detailing the incident on April 19, 2011. Telephone calls to former employees began on April 19, 2011. Letters are currently being

drafted to former employees detailing the incident and will be sent out using contact information on file.

- The new homeowners have not been notified by Lexand at this time.

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 Lexand to "notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure of personal information." In determining whether or not to require Lexand 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 Lexand 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 regards to the new home owners' personal information (name, address, phone number), this personal information is of low to medium sensitivity. The new home owners are not connected to the current or former employees of Lexand. It is unlikely that knowledge of the home owners' information could be used to commit fraud or identity theft. Therefore, there is no real risk of significant harm in this case, and I do not require Lexand to notify these individuals.

[12] The current and former employees are another matter. Social insurance numbers are highly sensitive, and coupled with an individual's name, address, telephone number, and driver's license, these numbers could be used to commit identity theft. It is possible that social insurance numbers alone could be used for fraudulent purposes, or to perpetrate identity theft. Adding other personally identifiable information including name and address increases the likelihood of this risk.

[13] In order for me to require Lexand 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.

[14] I note that while Lexand acted quickly to inform the police of this incident, the external hard that was drive stolen was not unencrypted and not password protected. In addition, the hard drive and accompanying user IDs and passwords have not been recovered.

[15] In this case, given the sensitivity of the personal information of the current and former employees at issue, and the fact the information stolen was unencrypted, I believe there is a real risk of significant harm to the current and former employees of Lexand.

[16] The information at issue could be used to cause significant harm to individuals, and provides comprehensive individual profiles that could be used for identity theft and/or fraud. Therefore, in my view, there is a real risk of significant harm and I require Lexand to notify the individuals affected.

V. Decision

[17] Based on the information reported to me by Lexand, I have concluded there is a real risk of significant harm to the current and former employees as a result of this incident, and I require the Lexand to notify these individuals in accordance with the Regulations.

[18] I understand Lexand has already notified its current employees of this incident and is working on communicating the breach to its former employees.

Frank Work, Q.C.
Information and Privacy Commissioner