ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-030

Devonian Properties Inc.

September 9, 2011

(Case File #P1968)

I. Introduction

[1] On August 23, 2011, I received a report from Devonian Properties Inc. ("DPI") of an incident involving the 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 DPI 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 DPI 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 DPI 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 23, 2011, I received a written report from DPI describing an incident involving the unauthorized access to personal information.

[8] On August 26, 2011, my Office contacted DPI to request that it provide additional information concerning the incident, in order for me to determine whether to require DPI 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 26 and August 31, 2011.

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

- DPI is a property development organization. On August 9, 2011, it discovered there had been unauthorized access to its servers. An unknown intruder had created several user profiles with administrative rights on both of DPI's servers.

- The incident was discovered by an authorized user who noticed that when logging onto DPI's server for an update, the internet browser was open to an unfamiliar site with Korean writing. DPI determined that a program had been downloaded to the server at a time when no employees with authorization had done so. This indicated an unauthorized person had been accessing the server.

- DPI's IT consultants determined that there had been unauthorized access from August 5 – August 10, and that some suspicious files may have been created as early as May 2011.

- The servers contained the personal information of 45 individuals, both clients and employees of DPI.

- DPI outlined the personal information at risk as follows:

  Purchaser information required for FINTRAC records (30 individuals) stored in electronic pdf files:
  - Name;
  - Address;
  - Date of birth;
  - Bank account number and financial institution name; and
  - One of following identification numbers: driver's license, passport, or birth certificate.

  Tenant information required for personal guarantees (2 individuals) stored in electronic pdf files:
  - Name;
  - Address;
  - Date of birth; and
  - Social insurance number.

  Employee information for signing authority purposes (5 individuals) stored in electronic pdf files:
  - Name;
  - Address;
  - Date of Birth;
  - Driver's license number;
  - Scanned copy of driver's license;
  - Scanned copy of Alberta Health Care card;
  - Copies of signatures; and
  - Social insurance number.

  Investor information for T5 reporting (8 individuals) stored in an electronic file accessible only by licensed users of the particular program.
  - Name;
  - Address; and
  - Social insurance number.

- DPI provided a description of the various physical, technical and administrative safeguards it had in place at the time of the breach. After discovering the breach, DPI "locked down" its servers.

- DPI also reported the breach to the Canadian Anti-Fraud Centre and the Office of the Privacy Commissioner of Canada.

- DPI plans to notify affected individuals and is currently drafting a notification letter.

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 DPI 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 DPI 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 DPI notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the affected 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 numerous data elements which can be used in identity theft such as dates of birth, social insurance numbers, government identification numbers, and for 5 affected individuals, even their signatures and scanned copies of their driver's licenses and Alberta health care cards were accessible by the system hacker.

[13] DPI 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 DPI 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 an unauthorized user had accessed DPI's servers for at least five days in August 2011, and had possibly had access since May 2011. The discovery of the internet browser in a foreign language could be another indication of real risk because identity theft is known as an international crime. The personal information of DPI's purchasers, tenants and employees was all easily accessible in pdf documents which increase the likelihood that the intruder obtained access to it.

[16] The personal information collected from the 8 investors for their T5s included a sensitive data element of a social insurance number; however, this information could be accessed in a usable format only by someone who has the same licensing program used by DPI. DPI pointed out that although the information was not encrypted, the

requirement for the licensing program is likely to make this personal information more difficult to access. I agree that the information does not appear to be as accessible as a pdf document; however, there is insufficient information before me regarding the accessibility of the tax licensing software, the format in which the personal information was stored, the steps that would be required to access the information or other relevant considerations which might allow me to determine there is no real risk to the affected investors. The facts are clear that DPI's servers were targeted by a hacker who created user profiles with administrative rights and that a great deal of sensitive personal information was accessible. In this case, I am not satisfied that a license requirement is sufficient protection to alleviate the real risk to the individuals who were affected by this breach.

[17] Given the information reported by DPI, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident. In particular, there is a real risk of significant harm to the personal information of DPI's purchasers, tenants and employees who had their personal information stored in pdf on the accessed servers, but I am also satisfied on the facts before me that there is a real risk to DPI's investors as well. I have based my decision on the fact that the type of information involved could be used to commit identity theft, which is a significant harm, and the manner of the intruder's access to DPI's servers indicates nefarious purposes.

V. Decision

[18] Based on the information reported to me by DPI, I have concluded that there is a real risk of significant harm to individuals as a result of this incident and I require DPI to notify affected individuals to whom I have determined there is a real risk of significant harm in accordance with section 19.1 of the *Personal Information Protection Act Regulation*. I require DPI to confirm in writing to my Office that it has done so on or before September 30, 2011 or such other date as I may specify.

Frank Work, Q.C.
Information and Privacy Commissioner