ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-24

VANCOUVER ISLAND INSURANCECENTRES INC. operating as H & D INSURANCE BROKERS

June 13, 2013

(Case File #P2252)

I. Introduction

[1] 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.

[2] On February 11, 2013, Vancouver Insurancecentres Inc. operating as H & D Insurance Brokers (Organization) provided notice of an incident involving the loss of personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to individuals as a result of the incident. I require that the Organization notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[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] The Organization is registered as an extra provincial corporation and is licensed to operate in Alberta under the *Insurance Act*. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA.

[6] The Organization reported the incident involved forms associated with the application or underwriting of residential property insurance. There were 42 Alberta clients affected by this incident. In addition to information about the residential properties, the forms contained all or a combination of the following information about the Organization's clients:

- insurance application forms (name, address, date of birth, marital status, years of residency in Canada, and occupation),
- property appraisals and inspection forms (name, address, photographs of the interior of residences),
- common declaration forms (name, address, and insurance premiums), and
- vacant risk program application forms (name, address, phone number or email address (or both), reason for vacancy, and signature of applicant).

[7] The information about the clients in paragraph [6] is "personal information" as defined by section 1(1)(k) of PIPA.

III. Background

[8] On February 25, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization between February 28, 2013, and May 13, 2013.

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

- A USB drive containing the personal information was mailed in an envelope from London, England, on January 17, 2013, to the Organization's office in Nanaimo, British Columbia.

- The Organization received the envelope on January 21, 2013. The USB drive was missing. There was a hole in the envelope.
- The USB drive was not password protected or encrypted.
- The loss was reported to Canada Post.
- The USB drive has not been recovered.
- The electronic data handling and security protocol was updated to include the requirement to encrypt data prior to transmission.
- The Organization notified 8 of the 42 clients. The Organization notified clients if their personal information involved name, contact information (address, phone number, email address), photographs of the interior of residences and date of birth or signature(s) or both.
- The Organization notified the clients by telephone shortly after the incident. It also sent a notification letter between March 11 and 18, 2013.
- The Organization offered one year of credit monitoring service to the clients and advised credit bureaus to place a fraud warning on client files.

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

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

[11] Pursuant to section 37.1 of PIPA, I have the power to 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." In determining whether or not to require the Organization to notify the affected individuals, I must consider if there is a "real risk of significant harm" to the affected individuals as a result of the incident.

[12] In order for me to require that the Organization notify the affected individuals, there must be some harm – some damage or detriment or injury – that could be caused to those affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[13] For 8 clients, the Organization recognized that if sensitive personal information, such as dates of birth or applicant signatures, in combination with the other information fell into the hands of the wrong individual, the incident may pose a risk of significant harm with respect to fraud. The Organization did not notify 34 clients as the personal information of those clients involved name, address and insurance premiums only.

[14] In my view, the personal information of the 34 clients could not be used to cause significant harm to those clients as a result of this incident. Accordingly, the first part of the test of requiring notification – that the incident could result in significant harm to individuals – is not met for these 34 clients.

[15] However, in my view, for the 8 clients whose personal information included name and contact information, in addition to a date of birth or signature, this information in combination is of moderate sensitivity. The type of harm that could result from unauthorized access to the personal information of these clients in this instance is identity theft or fraud. In my view, these are significant harms.

[16] In order for me to require the Organization to notify these clients there must also be a "real risk" of significant harm to these clients 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. There must be a cause and effect relationship between the incident and the possible harm.

[17] Based on the above and given the circumstances of the incident, I have decided that there is a real risk of significant harm to these clients as a result of this incident. The USB drive was not protected by a password or encryption. This factor, in addition to the nature and amount of personal information lost together with the Organization's inability to confirm how the information was lost contributed significantly to my decision.

V. Decision

[18] I require the Organization to notify the 8 clients referred to in paragraph 13 in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation").

[19] I understand that the Organization notified these clients in accordance with the Regulation in a letter sent between March 11 and 18, 2013. Therefore, I will not require the Organization to notify these clients again.

Jill Clayton
Information and Privacy Commissioner