ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-21

Invis Inc.

May 30, 2013

(Case File #P2308)

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 April 10, 2013, Invis Inc. (the 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 in Ontario and operating in Alberta. 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 the following information of 108 of its clients:

- first and last name,
- address,
- social insurance number (SIN),
- dollar amount in investment account,
- yearly salary,
- bank statements (bank account number, direct debit and deposit information),
- copy of a void cheque, and
- photocopy of driver's license.

Additional information for some of the clients included the following:

- working visa for new Canadian immigrants (name and address)
- passport, and
- divorce or separation documentation (dates of marriage, separation, divorce; birth date; child support and alimony payment amounts, if applicable; occupation and length of tenure; scheduled dates of custody and visitation rights; division of assets information; personal custody issues, if applicable).

[7] This information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] On April 10, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization between April 10, and May 29, 2013.

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

- On April 10, 2013, a vehicle belonging to an employee of the Organization (the Mortgage Broker) was broken into while it was parked at a restaurant in Edmonton, Alberta. The Mortgage Broker's laptop was stolen from the vehicle.
- The laptop contained client files for 108 clients.
- The laptop was not password protected and unencrypted.
- The incident was reported to the Edmonton Police Service on April 10, 2013.
- The laptop has not been recovered.
- The Organization has not notified the affected individuals.

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] The Organization reported the personal information involved in the incident as highly sensitive. The Organization further noted the incident did pose a risk of significant harm to the individuals affected by the incident.

[14] In my view, the personal information at issue is highly sensitive. As noted above in section [6], it includes the names, addresses, SINs, copy of driver's license, and banking information, of the affected individuals as well as divorce and separation documentation, where applicable. The type of harm that could result from unauthorized access to the personal information in this instance is identity theft or fraud and reputational harm for those with divorce and separation documentation. In my view, these are significant harms.

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

[16] P2010-ND-006 and 008; P2011-ND-014, 025, 028, 029, 040, and 043; P2012-ND-01, 08, 19; and P2013-ND-01 involved incidents of similar circumstances in which highly sensitive personal information of a similar nature to this incident was stolen and not recovered. In each of those 12 cases, it was decided there was a real risk of significant harm to the individuals affected.

[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 the affected individuals as a result of this incident. The fact that the information is highly sensitive, could be used to commit identity theft and fraud and reputational damage, have contributed to my decision fo a real risk of significant harm. In addition, the personal information at issue has been stolen and not recovered and was on a laptop that was not password protected and unencrypted leaving it easily accessible.

V. Decision

[18] I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation").

[19] The Organization must confirm to me in writing by June 28, 2013 that notification to the affected individuals has been done.

Jill Clayton
Information and Privacy Commissioner