ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-19

PFSL Investments Canada Ltd.

May 22, 2013

(Case File #P2316)

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 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 23, 2013, PFSL Investments Canada Ltd. (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 a Federal corporation registered 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 4 of its clients (the Client Information):

- Client A: name, address, date of birth, social insurance number (SIN), and RRSP account number,
- Client B: name, address, date of birth, SIN, RRSP and RESP account numbers,
- Client C: name, address, SIN, driver's license number, income, life insurance policy number; and,
- Client D: name and life insurance policy number.

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

III. Background

[8] On April 29, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization between April 29 and 30, 2013.

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

- On January 21, 2013, an agent for the Organization (the Agent) had a bag containing the Client Information stolen out of her rental vehicle in Costa Rica.
- The Agent's personal belongings were also stolen from the vehicle.
- The Client Information has not been recovered.
- The Organization issued new account numbers for Clients A, B, and C.
- The Organization verbally notified Clients A, B, and C on January 24 and 25, 2013. Each of these individuals was further notified of the incident by letter dated March 19, 2013.

- Client D was not notified of the incident.

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 at issue is sensitive from a financial perspective. The Organization believed the incident did pose a risk of significant harm to Clients A, B, and C. It stated the harm that could occur as a result of the loss of personal information for Clients A, B, and C are identity theft and fraud. The Organization believed the personal information of Client D was of low sensitivity and there was no risk of harm to this individual.

[14] In my view, the personal information for Client D is of low sensitivity as it includes name and life insurance policy number. The personal information at issue for Client D could not be used to cause significant harm to this individual. As there is no risk of significant harm, real or otherwise, to Client D I have decided the Organization is not required to notify Client D of this incident.

[15] In my view, the personal information at issue is highly sensitive for Clients A, B, and C. The personal information for these individuals includes names, addresses, SIN, dates of birth, and a driver's license number for Client C. The type of harm that could result from unauthorized access to personal information for these individuals is identity theft or fraud. In my view, these are significant harms.

[16] In order for me to require the Organization to notify these affected individuals, there must also be a "real risk" of significant harm to these 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.

[17] P2011-ND-004, P2011-ND-007, P2012-ND-08, and P2013-ND-01 all involved the theft of highly sensitive personal information from vehicles. In each of these cases, the information was in paper form and not recovered. It was determined a real risk of significant harm, identity theft and fraud, existed in those cases.

[18] Based on the above and given the circumstances, I have decided that there is a real risk of significant harm to the Clients A, B and C as a result of this incident. The personal information at issue for these individuals is highly sensitive. The personal information was stolen and has not been recovered. In my view, these factors indicate there is a real risk of significant harm to the affected individuals as a result of this incident.

V. Decision

[19] I require the Organization to notify Clients A, B and C in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation").

[20] I understand that the Organization has notified these individuals in accordance with the Regulation in a letter sent on March 19, 2013. Therefore, I will not require the Organization to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner