ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-17

TD FINANCING SERVICES INC.

May 9, 2013

(Case File #P2291)

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 March 11, 2013, TD Financing Services Inc. (Organization) provided notice of an incident involving the unauthorized access to and disclosure 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 and operates in Alberta as an extra-provincial corporation. 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 home improvement loan applications (Applications) for 11 individuals (Affected Individuals) that contained the following information:

- name,
- address,
- date of birth,
- phone number,
- occupation,
- annual salary,
- place of employment,
- mortgage payments and balance.

[7] In addition to the above list, Applications for the following number of Affected Individuals also contained:

- For 2, a driver's licence number.
- For 4, a social insurance number.
- For 1, both a driver's licence number and a social insurance number.

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

III. Background

[9] On March 11, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization March 18, 2013.

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

- On January 25, 2013, the police advised the Organization a person had been apprehended with photos of full and partial Applications on his or her cell phone.
- The Applications were dated from 2011. The Applications appeared to have originated from a hot tub vendor who is a dealer for the Organization. The Organization offers financing for customers of the vendor.
- It is unknown how the person obtained access to the Applications.
- The Organization notified the Affected Individuals of the incident by telephone on February 8, 2013, and by a letter dated March 1, 2013.
- The Organization offered the Affected Individuals a credit monitoring service. The Organization placed an alert on the Affected Individual's profiles.

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

[11] 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.

[12] 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.

[13] 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.

[14] The Organization reported the incident posed a risk of significant harm for identity theft based on the nature of the personal information and the circumstances.

[15] The personal information of the Affected Individuals is moderate to highly sensitive. For 5 Affected Individuals, the information includes social insurance numbers or driver's license numbers. The type of harm that could occur to these individuals as a result of unauthorized access to their personal information in this case is identity theft and fraud. In my view, these are significant harms.

[16] 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.

[17] The Organization reported the incident did pose a "real risk" of significant harm. The Organization was informed by the police that the person who was apprehended with the photos of the Applications had a history of fraud and identity theft offences.

[18] 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 nature of the personal information, the unknown circumstances surrounding how the unauthorized person obtained access to the Applications, and the information provided to Organization by the police about the person who had the photos of the Applications contributed significantly to my decision.

V. Decision

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

[20] I understand that the Organization has notified the Affected Individuals in accordance with the Regulation in a letter sent on March 1, 2013. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner