ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-023

1st Choice Savings and Credit Union Ltd.

August 27, 2012

(Case File #P2132)

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 July 12, 2012, 1st Choice Savings and Credit Union Ltd. (the "Organization") provided notice of an incident involving the unauthorized disclosure of personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to the Affected Members 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 corporation that is registered in Alberta and is 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 its members:

- name,
- designated beneficiary,
- Tax Free Savings Account ("TFSA") number,
- TFSA balance, and
- TFSA transactions.

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

III. Background

[8] On July 20, 2012, and August 13, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between July 20, 2012, and August 13, 2012.

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

- The Organization serves the Lethbridge community as well as other smaller communities in southern Alberta.
- The Organization printed the TFSA statements at the end of June, 2012, and mailed them the week of July 2, 2012.
- On July 9, 2012, a member of the Organization reported to the Organization that he or she received another member's TFSA statement printed on the back of his or her TFSA statement.
- The breach affected 293 members.
- A printing error caused by human error resulted in one page of a member's statement appearing on the back of another member's statement.

- All affected individuals were notified of the breach by letter on July 16, 2012. The letter, which was also sent to the members who received TFSA statements in error, requested the TFSA statement received in error be destroyed.
- Correct TFSA statements were mailed.
- The Organization disabled the ability to print statements in reverse order. If anything is flagged as an error in the printing system, the operator must obtain sign-off from a supervisor before the printing is resumed.

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 whether 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 the Organization to 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 be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[13] The Organization identified that the type of harm which could result from the unauthorized disclosure of the affected individual's beneficiary is hurt, humiliation, and damage to reputation. The Organization reported that this is because the affected individuals live in several small communities in southern Alberta and may know each other.

[14] The personal information at issue is highly sensitive for the Organization's members as it includes name, TFSA number, balance, transactions, and the members' beneficiary.

[15] The type of harm that could occur to the affected individuals from unauthorized access to the members' name and TFSA number, balance, and transactions is identity fraud. In addition, the affected individuals could also suffer hurt, humiliation, or damage to reputation as a result of unauthorized access to their beneficiary information. 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 indicated that there is a significant risk of harm to the affected individuals with regards to the members' beneficiary information for the reasons noted above.

[18] With respect to the TFSA number, balance, and transactions, the Organization informed my staff that members must provide photo identification in order to access their accounts. As a result, this information cannot be used to fraudulently access an affected individual's account. Therefore, there is no real risk of significant harm that will occur to an affected individual as a result of the unauthorized access to this information.

[19] In deciding whether there exists a "real risk" of significant harm in this case to the affected individuals with respect to the beneficiary information, I considered the following factors:

- The beneficiary information is highly sensitive.
- The affected individuals live in small communities in southern Alberta, increasing the likelihood that they know each other.
- There were 293 individuals affected by the breach.
- The letter sent by the Organization instructed the members who received another member's information to destroy the information.
- The Organization did not confirm the information was destroyed and did not recover the information.

[20] 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 the unauthorized access to the beneficiary information.

V. Decision

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

[22] I understand that the Organization has notified the affected individuals in accordance with the Regulation in a letter sent on July 16, 2012. Therefore, I will not require the Organization to notify the affected individuals again.

Jill Clayton

Information and Privacy Commissioner