ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-13

Servus Credit Union Ltd.

May 22, 2013

(Case File #P2303)

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 10, 2013, Servus 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 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 an organization 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 for 1 of its members and that member's beneficiary:

- name,
- address,
- social insurance number (SIN),
- bank account number and transaction details,
- date of birth,
- signature, and
- beneficiary information (name, address, and SIN).

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

III. Background

[8] On April 15, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization between April 15, and May 1, 2013.

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

- An employee at the Organization sent the member's personal information contained in a tax free savings account (TFSA) document to the wrong email address.
- The Organization does not know the individual to whom the TFSA was sent. The Organization has been unable to reach the individual who received the email in error.

- The Organization notified the affected member by letter on April 9, 2013. The Organization confirmed that the member notified the beneficiary about the incident. In addition, the Organization confirmed it verbally notified the beneficiary.

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 incident involved highly sensitive personal information. The Organization further believed that unauthorized access to the information could be used for identity theft or fraud. While there is no evidence of malicious intent because the incident was the result of human error, the Organization acknowledges that the information could be forwarded infinitely.

[14] I agree with the Organization that the personal information involved in this incident is highly sensitive. It involves names, addresses and SINs for both affected individuals and for 1 affected individual, birth date, account and signature. The type of harm that could occur from unauthorized access to these individuals' personal information as a result of this incident is identity theft and fraud. 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] P2013-ND-06 involved the disclosure of highly sensitive personal information by email where the organization in that case was not able to recover the email. It was

decided that a real risk of significant harm, identity theft and fraud, existed to the individuals affected by that incident.

[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 personal information is highly sensitive, the type of information could be used to commit identity theft and fraud, the information has gone to an unknown recipient and has not been recovered. These are all factors I considered in my decision.

V. Decision

[18] I require the Organization to notify the affected individuals in accordance with section 19.1(1) of the *Personal Information Protection Act Regulation* (the "Regulation").

[19] I understand the Organization notified the member of the incident in a letter dated April 9, 2013. The letter is in accordance with the Regulation. I also understand the beneficiary was directly notified by the Organization. The contents of the letter sent to the member, and the verbal notification to the beneficiary are in accordance with the Regulation. I will not require the Organization to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner