ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-01

SERVUS CREDIT UNION

February 6, 2012

(Case File #P2055)

I. Introduction

[1] On January 17, 2012, my Office received a report from Servus Credit Union ("Servus" or the "Organization") of an incident involving the loss of and unauthorized access to personal information. Based on the information reported to my Office, I have decided that there is a real risk of significant harm to individuals as a result of the incident, and therefore I require that Servus notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] 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.

[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] I have jurisdiction in this matter because Servus is an "organization" as defined in section 1(1)(i) of PIPA, and the information at issue in this incident qualifies as "personal information" as defined in section 1(1)(k).

[6] In considering whether to require Servus to notify affected individuals, I am mindful of PIPA's purpose and legislative principles and the relevant circumstances surrounding the reported incident.

III. Background

[7] On January 17, 2012, my Office received a written report from Servus describing an incident involving the loss of and unauthorized access to personal information. The incident resulted from the theft of a laptop and paper documents from a Servus employee's vehicle that was parked at the employee's residence.

[8] On January 18, 2012, my Office contacted Servus to request that it provide additional information concerning the incident, in order for me to determine whether to require Servus to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided via telephone calls, e-mails, and fax between January 18 and January 31, 2012.

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

- On January 5, 2012, a Servus employee ("the Employee") took work home at the end of the day. The Employee left a bag, containing a work issued laptop and paper documents containing the personal information of five (5) Servus members (customers) and one (1) Servus employee ("the Affected Employee") in her car parked outside her residence in Edmonton, Alberta. When she went to retrieve her bag the next day, it had been stolen.
- Servus reported the theft to the Edmonton Police Service (EPS). Servus reported that EPS told them it had several other reports of thefts from vehicles in the area on the same day.
- The personal information of the Affected Employee included the following:
    - Name;

    - Social Insurance Number;
    - Date of birth;
    - Home address; and,
    - Account number.
- The personal information of the five affected members included the following:
    - Name;
    - Member number;
    - Address (home and business);
    - Social Insurance Number;
    - Operator's License number;
    - Membership Number; and,
    - Transaction information for their account. This included wires and money transfer information for automated fund transfers.
- The laptop was encrypted and the Employee did not store any personal information on the hard drive. The Employee was required to use VPN to access the Servus network drives. The paper documents stolen contained all of the above noted member and employee personal information.
- The files containing the paper documents with the personal information of the 6 affected individuals were returned to Servus via an Edmonton newspaper reporter. Servus confirmed that the documents were viewed, but it is unknown at this time if the paper documents were copied.
- Servus has a policy where employees are not to leave personal information in their vehicles. The Employee who had the personal information stolen out of her car was in contravention of that policy.
- Following the break in, Servus notified the EPS. In addition, the affected members were notified of the incident via telephone, and a follow up letter was mailed to each affected member alerting them of the incident. Servus is currently attempting to contact the Affected Employee to inform them of the loss of their personal information.
- It appears that the laptop was the target of the theft as the paper documents were discarded and subsequently recovered.
- Servus placed messages on the banking system about the loss of the members' information to alert staff and ensure they verify the identity of anyone accessing the members' accounts. Members have also been asked to go to their branches and change their account numbers to remove the risk of fraudulent items passing through the compromised accounts.

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

[10] Pursuant to section 37.1 of PIPA, I have the power to require Servus to "notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure" of personal information. In determining whether or not to require Servus to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

[11] In order for me to require that Servus notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the members as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

[12] In this case, the personal information at issue is of high sensitivity as it includes name, address, social insurance number, and transaction information for the member and name, social insurance number, and date of birth of the Affected Employee. In addition, Servus confirmed that the files were viewed by individuals not authorized to have access as a result of the theft.

[13] Servus also noted that the type of harm that could result from the unauthorized access to or disclosure of this information is identity theft, which, in my view, is a significant harm. I agree that the personal information at issue in this case could be used to cause identity theft. In addition, Servus reported that one of the members had concerns regarding inquiries that were made to the member from VISA, but it is unknown if that inquiry is related to the theft of the documents in this case.

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

[15] Given the information reported by Servus, I have decided that there is a real risk of significant harm to individuals as a result of this incident. I have based my decision on the following factors: the type of information involved could be used to commit identity theft, which is a significant harm, and that the information was stolen and viewed by individuals not authorized to have access to the personal information.

V. Decision

[16] Based on the information reported to me by Servus, I have concluded that there is a real risk of significant harm to individuals as a result of this incident and I require Servus to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation*.

[17] While Servus reports it has attempted to contact the Affected Employee, Servus has not been able to reach that individual at this time. Notification to this affected individual will need to be done in accordance with section 19.1 of PIPA as noted above. I understand Servus has already notified the five affected members in a letter sent following the incident. However, the letter sent to all five affected members does not contain the requirement pursuant to 19.1(1)(b) and Servus will need to provide a more robust description of the loss (as per section 19.1(1)(b)(i)), the date the incident occurred (section 19.1(1)(b)(ii)), and the steps taken by Servus to reduce the risk of harm (section

19.1(1)(b)(iv). I require that Servus confirm in writing to my Office that it has done so on or before February 27, 2012, or such other date as I may specify.

Jill Clayton
Information and Privacy Commissioner