Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Servus Credit Union Ltd. (Organization)
Decision number (file number)	P2018-ND-079 (File #008988)
Date notice received by OIPC	June 19, 2018
Date Organization last provided information	July 3, 2018
Date of decision	July 16, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported "The actual breach did not involve personal information. It was the unauthorized access of two bank accounts by an employee." However, the Organization reported "the following information was potentially exposed": • name, • date of birth, • social insurance number, • address, • telephone number, • email address, and • bank account number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On March 2, 2018, one of the Organization's members raised a concern with a Branch Manager regarding a payment made to an unfamiliar credit card. • The Branch Manager engaged the Corporate Security Department to investigate the matter. • The investigation found that an employee of the Organization improperly accessed two unrelated bank accounts for reasons unrelated to his/her job tasks. • In both cases, the members suffered a financial loss. • The unauthorized access occurred between January 18, 2018 and February 7, 2018.
Affected individuals	The incident affected 2 individuals.
Steps taken to reduce risk of harm to individuals	• Notified law enforcement. • Reimbursed funds of the affected individuals. • Terminated the employment of the person involved in the breach.
Steps taken to notify individuals of the incident	I understand that the Organization spoke to the individual who brought the incident to the Organization's attention on or about March 26, 2018. I understand the other affected individual was not notified directly by the Organization as the individual was unavailable due to incarceration; however, the Branch Manager notified this individual about the incident via a police officer working on the file on or about April 26, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to 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.	The Organization reported that "The information can be considered to be highly sensitive as it can be used to commit identity theft and fraud." The Organization also said that "The information potentially exposed could be used for identity theft or fraud; however, we have determined that the information was not the target of the breach so the probability for this use is low and recovery is not required." Nonetheless, "Two members suffered a financial loss as a result of this unauthorized access." In my view, the contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. Email addresses could be used for phishing which I have found to be a significant harm.

Real Risk The likelihood that the significant harm 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.	The Organization reported that "This breach resulted in harm as financial losses were experienced by two individuals. This breach was conducted by a single employee who accessed two accounts for purposes outside his/her normal responsibilities … As there was malicious intent evident as well as financial harm apparent, the information is considered to be highly sensitive. …Two individuals have been affected by this breach. [The Organization] considers one individual to be vulnerable due to his/her incarceration." I agree with the Organization. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a known third party (deliberate unauthorized access by a former employee). Further, the affected individuals already experienced a financial loss as a result of the unauthorized access, which was reimbursed by the Organization.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

The contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. Email addresses could be used for phishing purposes which I have found to be a significant harm. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a known third party (deliberate unauthorized access by a former employee). Further, the affected individuals already experienced a financial loss as a result of the unauthorized access, which was reimbursed by the Organization.

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

I understand the Organization reported that affected individuals were notified of the incident verbally on March 26, 2018, and via law enforcement on or about April 26, 2018.

The onus for notifying affected individuals about this incident rests with the Organization under PIPA, not law enforcement. Further, it is not clear what affected individuals may have been told about the incident, and whether the information provided by law enforcement met the requirements under section 19.1 of the Regulation.

I require the Organization to confirm to my Office, within ten (10) days of the date of this decision, that the two affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

Jill Clayton
Information and Privacy Commissioner