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)	P2019-ND-066 (File #011739)
Date notice received by OIPC	December 21, 2018
Date Organization last provided information	December 21, 2018
Date of decision	May 17, 2019
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 incident involved the following information: • full name, • account information (number, type, balance, history), • transaction history and patterns, and • bill payees and associated account number (excluding credit card number which only discloses the last 4 digits). 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 December 20, 2018, the Organization was notified that an unauthorized individual was able to successfully access a member's account and update information on the account. • The breach occurred as a result of poor authentication practice, contrary to the Organization's policy. • The affected individual suffered a financial loss.

	• The incident was discovered on December 21, 2018, when the Organization contacted the actual member to confirm an outgoing e-transfer.
Affected individuals	The incident affected 3 individuals.
Steps taken to reduce risk of harm to individuals	• Reimbursed the affected individual. • Changed and confirmed information updated by the unauthorized individual. • Revoked online access to the account. • Instructed the affected individuals to file a report with local law enforcement and the Anti-Fraud Centre. • Flagged the account for enhanced authentication. • Cancelled and replaced payment card. • Updated account security. • Offered 24 months credit monitoring to affected individuals. • Reported incident to law enforcement.
Steps taken to notify individuals of the incident	The affected individual was contacted verbally on December 22, 2018 and a formal notification was completed on January 15, 2019. A letter was sent January 17, 2019.
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 highly sensitive as it can be used to commit Identity theft and fraud". Further, "In this case, the members lost funds as a result of access given to fraudulent person". I accept the Organization's assessment that a reasonable person would consider that the financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.
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 the members. It is suspected that this account takeover was conducted by an individual who is familiar with our process and took advantage of human error in our system…As there was malicious intent evident as well as financial harm apparent, the information is considered to be highly sensitive. Online access was revoked once fraudulent access was discovered. The information contained on the online account can be used for further identity theft or fraud. As the information is in an electronic format, we are unable to completely recover it".

	I agree with the Organization's assessment. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to deliberate action (impersonation). 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.

A reasonable person would consider that the financial information at issue could be used to cause the significant harms of identity theft and fraud and financial loss. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to deliberate action (impersonation). 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 accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individuals were notified verbally on December 22, 2018 and a formal notification was completed on January 15, 2019. A letter was sent January 17, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner