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)	P2020-ND-009 (File #013736)
Date notice received by OIPC	October 15, 2019
Date Organization last provided information	October 15, 2019
Date of decision	February 11, 2020
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: • name, • account information (number, type, balance, transaction history and patterns), • bill payees and associated account number (excluding credit card number which only discloses the last 4 digits), • e-transfer details (email addresses and telephone numbers for both member and anyone who has received an e-transfer from member). 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 October 7, 2019, an unauthorized individual was able to successfully access a member's account. • The incident occurred when online banking access was granted over the phone via poor authentication practice by an agent of the Organization, contrary to posted policy. • The incident was discovered the same day, when the unauthorized individual contacted the Organization again and spoke to a different agent who refused access and contacted Corporate Security. • No funds were lost as all e-transfers were able to be blocked before completion.
Affected individuals	The incident affected 2 individuals.
Steps taken to reduce risk of harm to individuals	• Reimbursed funds to the member. • Messaged account to require responses to both challenge questions and the security code set by member at the branch. • Offered 24 months of credit monitoring. • Enhanced policy to require agents to place a return call to any member over the age of 65 requesting on line banking over the telephone. • Conducted training sessions with agents using successful phone calls to highlight "red flag" indicators of an impersonation attempt.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally on October 8, 2019 and by letter on October 15, 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 "There is the risk for identity theft and fraudulent transactions as a result of the unauthorized access". 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 and fraud and financial loss. In addition, email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud.
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 "In this case, harm did occur as there was an unsuccessful attempt to transfer funds from the account". 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, there was an unsuccessful attempt to transfer funds from the account.

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. In addition, email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to deliberate action (impersonation). Further, there was an unsuccessful attempt to transfer funds from the account.

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 affected individuals were notified verbally on October 8, 2019 and by letter on October 15, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner