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-186 (File #013652)
Date notice received by OIPC	August 12, 2019
Date Organization last provided information	August 12, 2019
Date of decision	December 13, 2019
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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 address and telephone number for member and anyone who received an e-transfer). 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 August 1, 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 on August 2, 2019 when the unauthorized individual contacted the Organization again and spoke to a different agent who refused access, cancelled online banking, and contacted Corporate Security. The breach was discovered during a subsequent investigation.
Affected individuals	The incident affected 1 individual.
Steps taken to reduce risk of harm to individuals	• Funds have been reimbursed to the member. • Previous account closed and a new one opened preventing further access. • Member instructed to file a report with local law enforcement and the Anti-Fraud Centre. • Account has been messaged requiring responses to both challenge questions and the security code set by member at the branch. An incorrect response requires in-person authentication before access can be given. • Offered 24 months credit monitoring services to affected individuals. • Conducted a series of training sessions with agents to highlight "red flag" indicators of an impersonation attempt.
Steps taken to notify individuals of the incident	The affected individual was notified in person on August 2, 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 harms of identity theft and fraud and financial loss. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.
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". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to deliberate action (impersonation) and the unauthorized individual did attempt to use the information for fraudulent purposes. The Organization cannot confirm that the information will not be used for other fraudulent activities.

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 individual. A reasonable person would consider that the financial information at issue could be used to cause the harms of identity theft and fraud and financial loss. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to deliberate action (impersonation) and the unauthorized individual did attempt to use the information for fraudulent purposes. The Organization cannot confirm that the information will not be used for other fraudulent activities. I require the Organization to notify the affected individual in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the affected individual was notified in person on August 2, 2019. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner