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-069 (File #008664)
Date notice received by OIPC	May 15, 2018
Date Organization last provided information	May 15, 2018
Date of decision	July 4, 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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • first and last name, • account information (number, type, balance, history) • transaction history and patterns, • bill payees and associated account numbers, and • e-transfer details (email address and telephone numbers of sender and third party recipients). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• Between November 27, 2017 and March 28, 2018, the Organization discovered instances whereby "fraudulent impersonators have been successfully able to take over the accounts of…members. These accounts were taken over because online access was granted over the phone via poor authentication practices by several Member Contact Centre Agents contrary to posted policy". • In all instances, members suffered a financial loss.
Affected individuals	The incident affected 14 people, including 4 seniors.
Steps taken to reduce risk of harm to individuals	• Instructed members to report the incident to law enforcement. • Revoked online access, froze/closed accounts and enhanced security/monitoring. • Reimbursed funds. • Offered 24 months of credit monitoring services at the Organization's cost.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally and by mail.
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 used to commit identity theft and fraud" and "In all cases, members lost funds as a result of access given to fraudulent persons". Further, "This harm can be considered significant as the initial breach involved unauthroized [sic] access to the online banking portal". I agree with the Organization's assessment. The financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes. These are all 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 "This breach resulted in harm as financial losses were experienced by all members involved…As there was malicious intent evident as well as financial harm apparent, the information is considered to be highly sensitive…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. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate action and impersonation), actual harm occurred, and the Organization is not able to recover the information.

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 financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes. These are all significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate action and impersonation), actual harm occurred, and the Organization is not able to recover the information. 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 notified affected individuals were notified verbally and by mail in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner