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 (Organization)
Decision number (file number)	P2020-ND-079 (File #015161)
Date notice received by OIPC	July 18, 2019
Date Organization last provided information	July 18, 2019
Date of decision	July 24, 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 some or all of the following information: • name, • address, • cell phone number, • citizenship, • marital status, • date of birth, • SIN or SSN, • net worth, • employer information, • employer information for spouse, • beneficiary information, • vehicle insurance certificate and registration, • banking information (name of bank, bank account numbers), • tax status self-certification, • signature, • void cheque, and • copy of identification.

	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 June 26, 2019, there was a break-in at a Red Deer branch of the Organization. A briefcase containing documentation for 12 Wealth Management Accounts was stolen. • The breach was discovered the following morning by an employee entering the branch and completing a branch check per corporate policy. • The files and associated documentation were recovered intact on June 27, 2019.
Affected individuals	The incident affected 21 individuals.
Steps taken to reduce risk of harm to individuals	• Offered to change accounts. • Offered 24 months of credit monitoring services. • Offered identity theft brochure to assist in minimizing further harm. • Reviewing security measures of the branch (e.g. alarm system, number and placement of cameras, and how often security company visits the site after hours.)
Steps taken to notify individuals of the incident	Affected individuals were notified verbally on July 10, 2019 and in writing on July 18, 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, "As sensitive personal and financial information is involved, there is the possibility of identity theft and fraud as a result of the breach." I agree with the Organization's assessment. A reasonable person would consider that the contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud, negative effects on credit, 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, "As the files and associated documentation were recovered intact the following morning, we consider the likelihood of the harm to be low." In its "Talking Points for Verbal Notification", the Organization said, *We have reason to believe that the perpetrator of this break and enter was likely looking for cash or items that could be easily exchanged for cash and was not targeting your personal information. However the information they may have potentially been exposed to is sensitive and we do not want to place you at risk to fraud or identity theft.* In my view, although the files and associated documentation were recovered, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in and theft). Although the Organization said the perpetrator was likely looking for cash or items that could easily be exchanged for cash, the Organization can only speculate to the motives of the perpetrator(s). As well, the information was not in the Organization's control for several hours and the Organization cannot confirm the information was not copied or recorded for future use by the perpetrators.

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 contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud, negative effects on credit, and financial loss. Although the files and associated documentation were recovered, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in and theft). Although the Organization said the perpetrator was likely looking for cash or items that could easily be exchanged for cash, the Organization can only speculate to the motives of the perpetrator(s). As well, the information was not in the Organization's control for several hours and the Organization cannot confirm the information was not copied or recorded for future use by the perpetrators.

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 verbally on July 10, 2019 and in writing on July 18, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner