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)	P2021-ND-280 (File #020252)
Date notice received by OIPC	March 23, 2021
Date Organization last provided information	March 23, 2021
Date of decision	February 18, 2022
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: • name, • gender, • date of birth, • address, • identification details, • social insurance number, • social security number, • tax identification number, • email address, • employment information, and • account information (joint member name, balances, interest rate, transaction history, etc.) 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 January 20, 2021, the Organization's Internal Audit department identified numerous instances where four employees of the organization had accessed account information of other employees and members without an authorized purpose. The accesses were discovered during a review into system access conducted in January. • The Organization reported the unauthorized accesses occurred between November 2020 and February 2021.
Affected individuals	The incident affected 78 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified affected individuals and offered them 24 months of complimentary credit monitoring. • Disciplined employees who conducted the accesses. • Sent communications to all employees reminding them about the existence of the audit tool, the importance of maintaining member and employee privacy, and the consequences of failure to do so, up to and including termination. • Developing a process for frequent spot checks of employee accesses.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally throughout February and March. A follow-up letter was sent to affected individuals on March 23, 2021
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 the possible harms that might result from this incident include identity theft and fraud. 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 harms of identity theft and fraud. Employment information could be used to cause the harms of hurt, humiliation and embarrassment, as well as damage to personal/professional relationships. Email addresses could be used for phishing purposes, increasing affected individuals' vulnerability to identity theft and fraud. 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: *There is a low likelihood for harm as the reason for access was curiosity and not malicious intent. In addition, we have confirmed that no information was transferred to personal devices.* In my view, a reasonable person would consider that the likelihood of significant harm resulting from this incident is increased

	because it resulted from deliberate action (access without authorization). Although the Organization has confirmed that information was not transferred to personal devices, there is no evidence the information has not been further disseminated or disclosed. Because the affected individuals and the perpetrators are known to each other, there is an increased likelihood of damage to personal/professional relationships resulting from this incident.

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 harms of identity theft and fraud. Employment information could be used to cause the harms of hurt, humiliation and embarrassment, as well as damage to personal/professional relationships. Email addresses could be used for phishing purposes, increasing affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of significant harm resulting from this incident is increased because it resulted from deliberate action (access without authorization). Although the Organization has confirmed that information was not transferred to personal devices, there is no evidence the information has not been further disseminated or disclosed. Because the affected individuals and the perpetrators are known to each other, there is an increased likelihood of damage to personal/professional relationships resulting from this incident.

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 Organization notified affected individuals verbally, and in a letter sent on March 23, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner