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-139 (File #016077)
Date notice received by OIPC	June 8, 2020
Date Organization last provided information	June 8, 2020
Date of decision	November 3, 2020
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: • first and last name, • organization credit card number, • CVV security number, and • date of birth. This information is about an identifiable individual 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 December 13, 2018, a fraudulent impersonator with knowledge of personal information and credit card information was able to successfully update the contact information on the credit card account for a single individual.

	• Once the changes were made, the impersonator was able to conduct fraudulent transactions on the credit card, update information on the membership account, and authorize a payment from the account over the telephone. • The Organization confirmed that no direct access was granted to either credit card or membership accounts. • The Organization discovered the breach on January 7, 2019, when the impersonator failed to correctly respond to an authentication question. • The Organization reported that it was unsure if the breach was caused by the Organization or its credit card service provider and are providing notification as a precautionary measure.
Affected individuals	The incident affected one (1) individual.
Steps taken to reduce risk of harm to individuals	• Met with affected individual. • Provided an identity theft kit. • Updated security questions on account. • Prohibited telephone transactions on account messaging. • Closed and destroyed existing credit card and issued new card. • Filed fraudulent charge claim with credit card provider. • Reimbursed all transactions. • Provided 24 month credit monitoring free of charge.
Steps taken to notify individuals of the incident	The affected individual was notified verbally on January 8, 2019 and by letter on February 12, 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 the impersonator had information about an individual's MasterCard, he was able to successfully conduct fraudulent transactions."* In my view, a reasonable person would consider that the financial information at issue could be used to cause the significant harms of 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 "As an impersonator was able to successfully conduct transactions on a MasterCard, we have determined that harm has occurred." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach appears to be the result of malicious intent (deliberate action, impersonation) and actual harm resulted.

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 significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach appears to be the result of malicious intent (deliberate action, impersonation) and actual harm resulted. 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 Organization notified the affected individual verbally on January 8, 2019 and by letter on February 12, 2019, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner