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)	P2015-ND-78 (File #001636)
Date notice received by OIPC	September 25, 2015
Date Organization last provided information	November 3, 2015
Date of decision	December 10, 2015
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 a credit union and qualifies as an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The information at issue includes: • bank account number, transaction history and account balances for a personal account, • account balances for a business account. Information about an identifiable individual qualifies as "personal information" as defined in section 1(1)(k) of PIPA. The personal information in this case was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• On September 21, 2015, an employee of the Organization was contacted via email by an individual pretending to be a member (customer) of the Organization. The individual requested confirmation of his account number and a statement of his account. The Organization's employee disclosed the information, which was then used to complete a fraudulent wire transfer. • The member discovered the fraudulent email and contacted the Organization to report he did not authorize the transaction. • The Organization's policy requires authentication prior to any action on wire transfers. The member must be contacted by telephone to authenticate and confirm a transaction before proceeding. Telephone authentication was not completed in this case.
Affected individuals	Two (2) affected individuals in Alberta (a husband and wife are joint account holders).
Steps taken to reduce risk of harm to individuals	• The Organization reported that it will reimburse the member for lost funds. • The affected individuals were instructed to change their email addresses and have their computer scanned for viruses. Online banking access was restricted pending the computer scan. • Recommended the affected individuals have a notification placed on accounts with credit reporting bureaus. • The affected accounts were closed and new ones opened.
Steps taken to notify individuals of the incident	Notification to be sent by mail on November 3, 2015.
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 information is "highly sensitive as it was the missing piece of information need [sic] to complete the fraudulent wire." I agree with the Organization. The personal information involved could be used to cause 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 "this breach resulted in harm as it permitted an impersonator to commit wire fraud." I agree with the Organization. There is a real risk of harm in this case because the personal information was disclosed to an individual impersonating the affected individuals, indicating malicious intent. The information was used to complete a fraudulent wire transfer.

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 personal information involved could be used to cause the significant harms of identity theft and fraud. The information was disclosed to an individual impersonating the affected individuals, indicating malicious intent, and was used to complete a fraudulent wire transfer.

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 the affected individuals in a letter dated November 3, 2015, in accordance with the Regulation.

Jill Clayton
Information and Privacy Commissioner