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	1st Choice Savings and Credit Union Ltd. (Organization)
Decision number (file number)	P2018-ND-143 (File #010200)
Date notice received by OIPC	October 23, 2018
Date Organization last provided information	October 23, 2018
Date of decision	November 14, 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 is incorporated in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved scanned copies of cheques which included the following information: • name of individual/company (to whom the cheques were payable), • address, • account number, and • name and address of financial institution where accounts are held. This information is, in part, 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 July 4, 2018, an employee of the Organization intended to send an email with three PDF attachments to the Compliance department to verify ATM deposits. Inadvertently, the email was sent to a non-employee, along with other staff members.

	• The email was not encrypted or password protected. • Attempts were made to recall the message through Outlook, but were not successful. • The Organization made multiple attempts (through email, telephone and facebook) to contact the unintended recipient. • The unintended recipient eventually did respond and advised that she does not use the email account any longer, and does not have access to it. • The incident was discovered on July 5, 2018.
Affected individuals	The incident affected 28 individuals and companies (parties whose information was included on the cheques that were part of the deposit).
Steps taken to reduce risk of harm to individuals	Contacted the unauthorized recipient who has accounts with the branch and is known to the Organization as an ex-staff member. The unauthorized recipient was cooperative and advised that she does not have access to the account as it is an old account that hasn't been used in years and she no longer has the password.
Steps taken to notify individuals of the incident	The Organization reported that "All individuals and businesses affected by the breach have been contacted by the branch manager by telephone and advised of the breach and the risks outstanding and assisted in advising of what protective measures they should take."
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 there is a ""Mid-High level" risk of financial loss through fraudulent activities such as remote deposit capture fraud and/or counterfeit cheques by knowing the individual/company's account information." I agree with the Organization's assessment that the financial information at issue could be used to cause the significant harms of identity theft or 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: *Although there is still the potential for all 28 Individuals & companies to suffer a financial loss through fraudulent activities in the future due to the reasons mentioned, the likelihood of this happening at this time would be minimal due to the following:* *• The branch manager immediately contacting all affected parties and advising them of the breach and having them*

	take proper corrective and preventative measures on their accounts (stop all, review all transactions, ordering of new cheques or different account numbers). *• Financial institutions have adequate security measures in place to obtain the identity of individuals trying to access accounts and sophisticated fraud detection software for remote deposit capture and cheque fraud* *• The Individual who would possibly have access to the information is known to the branch, is an ex-staff member and is a reputable person.* I agree with the Organization that these factors reduce the likelihood of significant harm resulting from this incident. The breach did not result from malicious intent, but rather human error, and the unauthorized recipient is known to the Organization. Despite this, the Organization reported that the information was not recovered and is still in the unauthorized recipient's email account as the account holder does not have access to the account any longer and hasn't for years as she cannot remember the password. The information has not been recovered, and the Organization is therefore unable to confirm it has not and will not be used or disclosed in the future.

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 significant harms of identity theft or fraud. The breach did not result from malicious intent, but rather human error, and the unauthorized recipient is known to the Organization. Despite this, the Organization reported that the information was not recovered and is still in the unauthorized recipient's email account as the account holder does not have access to the account any longer and hasn't for years as she cannot remember the password. The information has not been recovered, and the Organization is therefore unable to confirm it has not and will not be used or disclosed in the future.

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 that all individuals and businesses affected by the breach were contacted by the branch manager by telephone and advised of the breach and the risks outstanding and assisted in advising of what protective measures they should take. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner