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	Mountain View Credit Union Limited (Organization)
Decision number (file number)	P2017-ND-90 (File #005766)
Date notice received by OIPC	June 5, 2017
Date Organization last provided information	June 5, 2017
Date of decision	July 12, 2017
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the 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: • first and last name, • home address, and • mortgage number and mortgage amount. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On July 14, 2016, two emails that were intended to be sent to a member were inadvertently sent to an incorrect email address. • On October 6, 2016, the member contacted the Organization to discuss another matter and during the conversation it was discovered that the member did not receive the emails sent on July 14. • The emails were not recovered.

Affected individuals	The incident affected two (2) individuals in Alberta (joint mortgagees).
Steps taken to reduce risk of harm to individuals	• An attempt was made to recall the emails but was unsuccessful. • The Organization determined that the incorrect email address was a "live" or valid email address but could not determine whether it was active.
Steps taken to notify individuals of the incident	One of the affected individuals and the Organization representative discovered the inadvertent disclosure at the same time during a conversation together. The matter was also the subject of a complaint made to my office.
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 there is a "Mid level risk of financial fraud. Low or minimal risk of identity theft." In my view, the contact and financial information at issue could be used to cause the harms of 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.	As noted above, the Organization reported there is a "Mid level risk of financial fraud. Low or minimal risk of identity theft." In assessing the likelihood of harm, the Organization considered the following factors: • The type of information at issue, including that no identifiers (e.g. Social Insurance Number or date of birth) were disclosed. • The information at issue does not provide access to online accounts so electronic transfer would not be possible. • The mortgage account number is not necessarily a reflection of a member's overall membership number and an individual coming in with only a mortgage number and not knowing their membership number would be required to produce identification. • The affected individual is well known to the Organization and it would be difficult for someone to impersonate her. • If there were any suspicious activities, identification would be requested before any transaction occurred. • The Organization has not confirmed that the information at issue was actually breached as it has not had any response from the unintended recipient.

	In my view, there is a real risk of harm in this case. Despite the fact the incident did not result from malicious intent but rather human error, the information was exposed for almost three months before the incident was discovered, and has not been recovered. The Organization has not been able to contact the unintended recipient to confirm that the information was destroyed and not further disseminated. Although it is unlikely the information could be used for fraudulent purposes at the Organization (e.g. because the affected individual is known), there is still the potential harm from other forms of identity theft or fraud.

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 contact and financial information at issue could be used to cause the harms of identity theft and fraud. These are significant harms. Despite the fact the incident did not result from malicious intent but rather human error, the information was exposed for almost three months before the incident was discovered, and has not been recovered. The Organization has not been able to contact the unintended recipient to confirm that the information was destroyed and not further disseminated. Although it is unlikely the information could be used for fraudulent purposes at the Organization (e.g. because the affected individual is known), there is still the potential harm from other forms of identity theft or fraud.

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 and one of the affected individuals discovered the incident at the same time, during a telephone conversation, and the matter was also the subject of a complaint made to my office. Given this, the Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner