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 (Organization)
Decision number (file number)	P2021-ND-118 (File #009390)
Date notice received by OIPC	August 3, 2018
Date Organization last provided information	August 3, 2018
Date of decision	April 27, 2021
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 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: • name, • address, • account number, • fee charged, • account manager information and date of next review, • the member's financial ratio information, • covenants which apply to the member, and • advisement of a breach of covenant. 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 May 25, 2018, the Organization inadvertently mailed an annual post-review letter and a non-compliance letter to the wrong address. • The breach was discovered on June 4, 2018, when the unintended recipient attended the branch to report the error and return the documents.
Affected individuals	The incident affected 2 individuals residing in Alberta
Steps taken to reduce risk of harm to individuals	Revised procedures to verify correspondence is addressed to the correct member.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone and email on June 4, 2018.
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 incident gave rise to a "'Mid-High level' risk of financial fraud and 'Low-Mid level' risk of identity theft". In my view, a reasonable person would consider that the contact and financial information at issue could be used for the purposes of identity theft and fraud. Information about non-compliance could be used to cause embarrassment and damage to reputation. 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 considered a number of factors in assessing the likelihood of significant harm resulting from this breach, including: • "Only one individual obtained the letters. He is also a member of the [Organization]", • " ... maximum days exposed would be 8 days", • "The [affected individuals] are well known to the branch and so anyone trying to impersonate or use their account would be known immediately", • "The individual who received the information is also known to the branch and is well respected". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is decreased because the personal information was not compromised due to any malicious intent. The breach was reported by the unintended recipient who is a known and trusted member of the Organization and returned the documents, making it unlikely the information would be used for identity theft or fraud. However, the fact the affected individuals are well known to the Organization, and possibly to the unintended recipient, increases the likelihood of

	personal/professional relationships between the affected individuals and the unintended recipient, making the harms of embarrassment and damage to reputation more likely.

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 and financial information at issue could be used for the purposes of identity theft and fraud. Information about non-compliance could be used to cause embarrassment and damage to reputation. These are significant harms.

The likelihood of harm resulting from this incident is decreased because the personal information was not compromised due to any malicious intent. The breach was reported by the unintended recipient who is a known and trusted member of the Organization and returned the documents, making it unlikely the information would be used for identity theft or fraud. However, the fact the affected individuals are well known to the Organization, and possibly to the unintended recipient, increases the likelihood of personal/professional relationships between the affected individuals and the unintended recipient, making the harms of embarrassment and damage to reputation more likely.

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 affected individuals were notified by telephone and email on June 4, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner