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	Connect First Credit Union Ltd. (Organization)
Decision number (file number)	P2021-ND-329 (File #022827)
Date notice received by OIPC	August 17, 2021
Date Organization last provided information	August 17, 2021
Date of decision	March 9, 2022
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 whose personal information was collected in Alberta pursuant to section 37.1 of *the Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is headquartered in Calgary, Alberta, and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • account number, • banking information, and • physical address. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On August 6, 2021, a member of the credit union unintentionally logged into another member's account. • The Organization explained that "The impacted member did not change [their] default password, which was originally the same as the username… The [other] member coincidentally used the same username and password when accessing [their] own online account." • The incident was discovered the same day when the member contacted the bank and reported that they were "viewing the account profile of another individual."
Affected individuals	The incident affected 1 individual in Alberta.
Steps taken to reduce risk of harm to individuals	• Temporarily disabled the affected member's account. • Advised the other member to change their password. • Advised the affected member to change their password.
Steps taken to notify individuals of the incident	The affected individual was notified verbally on August 10, 2021.
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 risk of identity theft to the impacted member, due to the compromise of account information and possibly, physical address.* I agree with the Organization's assessment. A reasonable person would consider 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.	The Organization reported: *The likelihood of harm is considered medium. This is conditional on presumption that the member who wrongly accessed onling [sic] banking of another, would have viewed the electronic bank statement and seen the address.* I accept the Organization's assessment. A reasonable person would consider the likelihood of harm resulting from this incident decreased because the personal information was compromised due to human error and insufficient technical and administrative safeguards with respect to managing user credentials.

	Despite this, the Organization reported **advising** both members to change their passwords as opposed to forcing a reset, which may not mitigate the risk of harm. The Organization also did not report taking steps that would prevent reoccurrence of a similar incident.

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 the contact and financial information at issue could be used to cause the harms of identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident decreased because the personal information was compromised due to human error and insufficient technical and administrative safeguards with respect to managing user credentials.

Despite this, the Organization reported **advising** both members to change their passwords as opposed to forcing a reset, which may not mitigate the risk of harm. The Organization also did not report taking steps that would prevent reoccurrence of a similar incident.

I require the Organization to notify the affected individual whose personal information was collected 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 August 10, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner